Détection d'attaques dans un système WBAN de surveillance médicale à distance

Ali Makke

Université Paris Descartes

Laboratoire LIPADE

Ecole Doctorale Informatique, Télécommunications et Electronique (ED 130)

Thèse

Présentée par

Ali MAKKE

pour obtenir le grade de docteur

de l'Université Paris Descartes

Spécialité: Informatique et Réseaux

Détection d'attaques dans un système WBAN de surveillance médicale à distance

Soutenue le 30 Mai 2014 devant le jury composé de

Rapporteurs:	
M. Ahmed Karmouch	Professeur, Université d'Ottawa
M. Yacine Ghamri-Doudane	Professeur, Université de la Rochelle
Examinateurs:	
M. Farid Naït-Abdesselam	Professeur, Université Paris Descartes
M. Yassine Hadjadj-Aoul	MCF, Université de Rennes 1
Directeurs de thèse:	
M. Ahmed Mehaoua	Professeur, Université Paris Descartes
M. Osman Salem	MCF, Université Paris Descartes

Résumé

L'un des défis majeurs du monde de ces dernières décennies a été l'augmentation continue de la population des personnes âgées dans les pays développés. D'où la nécessité de fournir des soins de qualité à une population en croissance rapide, tout en réduisant les coûts des soins de santé. Dans ce contexte, de nombreux travaux de recherche portent sur l'utilisation des réseaux de capteurs sans fil dans les systèmes WBAN (Wireless Body Area Network), pour faciliter et améliorer la qualité du soin et de surveillance médicale à distance.

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

En effet les vulnérabilités dans un système WBAN se décomposent en deux parties principales. La première partie se compose des attaques possibles sur le réseau des capteurs médicaux et sur le médium de communications sans fils entre ces capteurs et l'unité de traitement. La deuxième partie se compose des attaques possibles sur les communications à haut débit entre le système WBAN et le serveur médical.

L'objectif de cette thèse est de répondre en partie aux problèmes de détection des attaques dans un système WBAN de surveillance médicale à distance. Pour atteindre cet objectif, nous avons proposé un algorithme pour détecter les attaques de brouillage radio (*jamming attack*) qui visent le médium de communications sans fils entre les capteurs et l'unité de traitement. Ainsi nous avons proposé une méthode de mesure de divergence pour détecter les attaques de type *flooding* qui visent les communications à haut débit entre le système WBAN et le serveur médical.

Mots clés: réseaux de capteurs médicaux sans fil, systèmes WBAN, détection des attaques, *jamming*, *flooding*, mesure de divergence, taux de détection, taux de fausses détections.

Abstract

One of the major challenges of the world in recent decades is the continued increase in the elderly population in developed countries. Hence the need to provide quality care to a rapidly growing population while reducing the costs of health care is becoming a strategic challenge. In this context, many researches focus on the use of wireless sensor networks in WBAN (Wireless Body Area Network) systems to facilitate and improve the quality of medical care and remote monitoring.

These WBAN systems pose new technological challenges in terms of security and protection against faults and attacks. The wireless communication mode used between the sensors and the collection node accentuates these vulnerabilities.

Indeed vulnerabilities in a WBAN system are divided into two main parts. The first part consists of the possible attacks on the network of medical sensors and on the wireless communications medium between the sensors and the processing unit. The second part consists of possible attacks on high-speed communications between the WBAN system and the medical server.

The objective of this thesis is to meet some of the problems of detecting attacks in a WBAN system for remote medical monitoring. To achieve this goal, we propose an algorithm to detect the jamming attacks targeting the wireless communications medium between the sensors and the processing unit. In addition we propose a method of measuring divergence to detect the flooding attacks targeting the high-speed communications between the WBAN system and the medical server.

Keywords: wireless medical sensor networks, WBAN systems, attack detection, jamming, flooding, divergence measure, detection rate, false detection rate.

Remerciements

Cette thèse s'est déroulée, au sein du Laboratoire d'Informatique de l'université PAris DEscartes (LIPADE), sous la direction de Monsieur Ahmed Mehaoua, professeur à l'université Paris Descartes et directeur de l'équipe réseaux multimédia et sécurité. Je tiens à lui exprimer ma profonde reconnaissance pour m'avoir fait confiance en acceptant de diriger cette thèse ainsi que pour ses conseils qui m'ont permis de mener à bien ce travail.

Ma gratitude va également vers Monsieur Osman Salem qui a encadré la moitié de mes travaux de thèse.

Je remercie vivement Monsieur Ahmed Karmouch, professeur à l'Université d'Ottawa, et Monsieur Yacine Ghamri-Doudane, professeur à l'Université de la Rochelle, d'avoir accepté la lourde tâche d'être rapporteurs de cette thèse.

Je remercie également Monsieur Farid Naït-Abdesselam, professeur à l'Université Paris Descartes, et Monsieur Yacine Hadjadj-Aoul, maître de conférences à l'Université de Rennes 1, de m'avoir fait l'honneur de bien vouloir participer au jury de cette thèse.

Merci à l'école doctorale EDITE de Paris qui m'a attribué une bourse doctorale. J'aimerai noter spécialement Monsieur Christian Queinnec l'ancien directeur de l'EDITE, que je le remercie pour sa compréhension et ses qualités humaines.

Mes collègues du bureau ainsi que les membres de l'administration sont priés de trouver ici l'expression de ma sincère gratitude.

Je remercie tous les membres de ma grande famille ainsi que tous mes amis qui m'ont encouragé et m'ont accordé leur confiance.

Je garde une place toute particulière à ma famille : mon père Fawzi, ma mère Jamileh, ma sœur Rana et sa famille et mon frère Rani et sa famille. Je voudrais leur exprimer toute ma profonde reconnaissance parce qu'ils m'ont constamment aidé par leurs encouragements et leur soutien moral pour achever cette thèse ainsi que pour leur soutien sans limites aux moments les plus difficiles.

Enfin un grand merci sans égal à mon chère frère Dr. Rani Makke pour son soutien à tous les niveaux et son encouragement tout au long de mes études en France.

Tables des matières

RESUME **5**

ABSTRACT **7**

REMERCIEMENTS **9**

TABLES DES MATIERES **11**

LISTE DES FIGURES **15**

LISTE DES TABLEAUX **17**

CHAPITRE I : INTRODUCTION GENERALE **19**

1. CONTEXTE ET PROBLEMATIQUE 19
2. PRINCIPALES CONTRIBUTIONS DE LA THESE 20
3. ORGANISATION DU MEMOIRE 21
4. LISTE DES PUBLICATIONS 23

CHAPITRE II : LES RESEAUX DE CAPTEURS MEDICAUX SANS FIL **25**

1. INTRODUCTION 25
2. ARCHITECTURE DES RESEAUX WBAN 27

2.1. Les réseaux WBAN 27

2.1.1. Comparaison entre les réseaux WBAN et les réseaux WSN 27
2.1.2. Les sous-systèmes d'un système WBAN de surveillance médicale 29
2.1.3. Topologies des réseaux WBAN 30

2.2. Les nœuds capteurs 33

2.2.1. Définition d'un capteur médical 33
2.2.2. Les capteurs médicaux 33
2.2.3. Architecture d'un nœud-capteur 37
2.2.4. Caractéristiques des capteurs 39
2.2.5. Systèmes d'exploitation pour les capteurs 40

2.3. Architecture de communication dans les systèmes WBAN 43

2.3.1. Communications «Intra-BAN» 44
2.3.2. Communications «Inter-BAN» 44
2.3.3. Communications « Au-delà de BAN» 45
2.3.4. Protocoles de communications sans fil 45

3. LES SYSTEMES WBAN DANS LE DOMAINE MEDICAL 49

3.1. Les avantages apportés par les systèmes WBAN dans le domaine médical 49
3.2. Les applications des WBAN dans le domaine de surveillance médicale 51

3.2.1. La surveillance des activités de la vie quotidienne 52
3.2.2. La détection de chute et du mouvement 52
3.2.3. Le suivi de prise des médicaments 52
3.2.4. La localisation des patients ou de l'équipe médicale 52
3.2.5. La surveillance de l'état de santé 53
3.2.6. La Bio-surveillance 54
3.2.7. La prédiction des maladies 54

3.3. Etat de l'art sur les projets de recherches des systèmes WBAN 54

4. LES DEFIS ET LES CONTRAINTES DES RESEAUX WBAN 56
4.1. Les défis des réseaux WBAN 56
4.1.1. Le défi d'énergie 56
4.1.2. Tolérance aux pannes 57
4.1.3. La sécurité 57
4.2. Les contraintes des réseaux WBAN 58
4.2.1. Contraintes matérielles 59
4.2.2. Contraintes réseaux 59
5. CONCLUSION 60

CHAPITRE III : LES ATTAQUES ET LES ANOMALIES DANS LES SYSTEMES WBAN 61

1. INTRODUCTION 61
2. LES ATTAQUES ET LES ANOMALIES DANS LES SYSTEMES WBAN 62
2.1. Classifications des attaquants 62
2.1.1. Selon son intention 62
2.1.2. Selon sa position par rapport au réseau 62
2.1.3. Selon sa capacité 63
2.2. Classification des attaques possibles dans un système WBAN 63
2.2.1. Les attaques qui visent les nœuds capteurs 64
2.2.2. Les attaques qui visent les communications sans fil dans les sous-systèmes « intra-BAN et inter- BAN » .65
2.2.3. Les attaques qui visent les communications dans le sous-système « au-delà de BAN » 66
2.3. Classifications des anomalies au sein des RCSF médicaux 67
2.3.1. Les anomalies du réseau 68
2.3.2. Les anomalies des nœuds 69
2.3.3. Les anomalies des données 70
2.3.4. Les techniques de détection des anomalies dans les RCSF 71
3. ETAT DE L'ART SUR LES TRAVAUX DE RECHERCHE CONCERNANT LA DETECTION DE L'ATTAQUE DE *JAMMING* 75
3.1. Avant propos 75
3.2. Méthodes proposées pour la détection de l'attaque Jamming 77
3.2.1. Xu et al. [70] 77
3.2.2. Reyes et al. [78] 78
3.2.3. Misra et al. [77] 79
3.2.4. Cakiroglu et al. [73] 80
3.2.5. Fragkiadakis et al. [82] 81
3.2.6. Hamieh et al. [80] 81
3.3. Critères de comparaison 82
3.4. Les mesures défense contre les attaques de jamming 83
3.4.1. Réglementation de la puissance transmise 84
3.4.2. Etalement de spectre par saut de fréquence (FHSS) 84
3.4.3. Etalement de spectre à séquence directe (DSSS) 84
3.4.4. FHSS/DSSS hybride 85
3.4.5. Technologie Ultra large bande 85
4. NOS CONTRIBUTIONS 85
5. CONCLUSION 86

CHAPITRE IV : DETECTION DES ATTAQUES DE *JAMMING* DANS LES RESEAUX WBAN 87

1. INTRODUCTION 87
2. LES ATTAQUES DE BROUILLAGE RADIO (*JAMMING ATTACKS*) 88
2.1. Brouilleur constant (Constant jammer) 89
2.2. Brouilleur trompeur (Deceptive jammer) 90
2.3. Brouilleur aléatoire (Random jammer) 90
2.4. Brouilleur réactif (Reactive jammer) 90
3. CRITERES DE DETECTION DES ATTAQUES *JAMMING* 90

3.1. Taux de paquets reçues ou Packet Delivery Ratio (PDR) *91*
3.1.1. L'influence des différents types des brouilleurs sur la valeur du PDR 92
3.2. Taux de paquets erronés ou Bad Packet Ratio (BPR) *92*
3.2.1. L'influence des différents types des brouilleurs sur la valeur du BPR 92
3.3. Quantité d'énergie consommée ou Energy Consumption Amount (ECA) *93*
3.3.1. L'influence des différents types des brouilleurs sur le niveau de l'ECA 93
3.4. Taux de paquets envoyés ou Packet Send Ratio (PSR) *94*
3.4.1. L'influence des différents types des brouilleurs sur la valeur du PSR 94
3.5. Indicateur de puissance du signal reçu ou Received Signal Strength Indicator (RSSI) *95*
3.5.1. L'influence des différents types de brouilleurs sur le niveau du RSSI 96
4. NOTRE PROPOSITION POUR LA DETECTION DU *JAMMING* DANS LES RESEAUX WBAN 96
4.1. Approche proposée *97*
4.2. Calcule des seuils *98*
4.2.1. Seuil pour PDR 99
4.2.2. Seuil pour BPR 99
4.2.3. Seuil pour ECA 100
4.2.4. Seuil pour RSSI 100
4.2.5. Seuil pour PSR 100
4.3. Méthode proposée pour la détection de jamming *101*
5. RESULTATS EXPERIMENTAUX 103
5.1. Environnement de simulation *104*
5.2. Application des algorithmes de détection et d'identification des attaques de jamming *108*
5.3. Evaluation des performances *109*
5.3.1. Détection à 2 paramètres 110
5.3.2. Détection à 3 paramètres 113
5.3.3. Détection à 4 paramètres 116
5.3.4. Discussion 119
5.3.5. Récapitulatif 120
6. CONCLUSION 122

CHAPITRE V : DETECTION DES ATTAQUES DE *FLOODING* DANS LES RESEAUX IP MEDICAUX 123

1. INTRODUCTION 123
2. LES ATTAQUES DOS DANS LES RESEAUX IP 124
2.1. Les attaques par surcharge *125*
2.1.1. Le SYN flood 125
2.1.2. Le PING flood 126
2.1.3. Le Smurf 126
2.2. Les attaques par failles *126*
2.2.1. Teardrop Attack 127
2.2.2. Ping of Death 127
2.3. Les attaques distribuées *127*
3. MODELES DE MESURE DE DIVERGENCE 128
3.1. Hellinger Distance (HD) *128*
3.2. Chi-square Divergence (CSD) *129*
3.3. Kullback-Leibler Divergence (KLD) *130*
3.4. Jensen-Shannon Divergence (JSD) *130*
3.5. Notre proposition Power Divergence (PD) *131*
4. L'ATTAQUE SYN *FLOODING* DANS LES RESEAUX IP 132
4.1. Détection des attaques SYN flooding dans les réseaux IP *133*
4.2. Structure de données Sketch *133*
4.3. Architecture du système de détection et son fonctionnement *135*
4.4. Calcul du seuil *136*

5. APPLICATIONS SUR DES TRACES D'UN TRAFIC INTERNET 136
5.1. Résultats expérimentaux 139
5.2. Evaluation des performances 142
5.2.1. Discussion 144
6. CONCLUSION 145

CHAPITRE VI : CONCLUSION GENERALE ET PERSPECTIVES 147

1. CONCLUSION GENERALE 147
2. PERSPECTIVES 149

LISTE DES ACRONYMES 151

BIBLIOGRAPHIE 155

Liste des figures

FIGURE 1 SYSTEME DE SURVEILLANCE MEDICALE WBAN 26
FIGURE 2 ARCHITECTURE D'UN SYSTEME DE SURVEILLANCE MEDICALE [9] 29
FIGURE 3 LES TOPOLOGIES DANS LES RESEAUX WBAN 31
FIGURE 4 EXEMPLES DE CAPTEURS MEDICAUX 34
FIGURE 5 « CONSOMMATION MOYENNE DE PUISSANCE VS DEBIT » POUR LES CAPTEURS CORPORELS 34
FIGURE 6 ARCHITECTURE D'UN NŒUD-CAPTEUR 38
FIGURE 7 ECHANTILLON DES CAPTEURS 40
FIGURE 8 ARCHITECTURE GENERALE DES COMMUNICATIONS DANS UN SYSTEME BAN [1] 44
FIGURE 9 SURVEILLANCE MEDICALE A DISTANCE DES PERSONNES AGEES 50
FIGURE 10 LES AVANTAGES APPORTES PAR LES WBAN DANS LE DOMAINE MEDICAL 51
FIGURE 11 LES ANOMALIES DANS LES RCSF 68
FIGURE 12 TECHNIQUES DE DETECTION DES ANOMALIES 72
FIGURE 13 APPROCHE BASEE SUR LA CLASSIFICATION 73
FIGURE 14 RELATION ENTRE PDR ET RSSI 78
FIGURE 15 SYSTEME WBAN DE SURVEILLANCE MEDICALE A DISTANCE 85
FIGURE 16 COMMUNICATION DES DONNEES PHYSIOLOGIQUES DANS UN SYSTEME WBAN 87
FIGURE 17 DIFFERENTS TYPES DE BROUILLEURS [34] 89
FIGURE 18 UN SYSTEME WBAN SOUS L'INFLUENCE D'UNE ATTAQUE DE *JAMMING* 97
FIGURE 19 CALCULE DES SEUILS POUR LES PARAMETRES 98
FIGURE 20 ORGANIGRAMME QUI REPRESENTE LES ETAPES POUR DETECTER LE *JAMMING* 102
FIGURE 21 RESEAU SIMULE 104
FIGURE 22 VALEUR MOYENNE DU PDR AVEC TE = 1 MIN 105
FIGURE 23 VALEUR MOYENNE DU BPR AVEC TE = 1 MIN 106
FIGURE 24 VALEUR MOYENNE DU PSR AVEC TE = 1 MIN 106
FIGURE 25 VALEUR MOYENNE DU PDR AVEC TE = 1 MIN 107
FIGURE 26 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/12 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 110
FIGURE 27 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/12 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 111
FIGURE 28 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/12 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 111
FIGURE 29 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/2 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 111
FIGURE 30 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/2 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 112
FIGURE 31 DR, FAR ET EFFICACITE DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/2 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 112
FIGURE 32 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/12 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 113
FIGURE 33 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/12 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 114
FIGURE 34 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/12 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 114

FIGURE 35 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/2 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 114
FIGURE 36 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/2 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 115
FIGURE 37 DR, FAR ET EFFICACITE DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/2 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 115
FIGURE 38 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/12 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 116
FIGURE 39 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/12 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 117
FIGURE 40 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/12 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 117
FIGURE 41 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/2 S, 2Σ (A GAUCHE), 3Σ (A DROITE)) 117
FIGURE 42 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/2 S, 4Σ (A GAUCHE), 5Σ (A DROITE)) 118
FIGURE 43 DR, FAR ET EFFICACITE DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/2 S, 6Σ (A GAUCHE), 7Σ (A DROITE)) 118
FIGURE 44 SYSTEME DE SURVEILLANCE MEDICALE A DISTANCE 123
FIGURE 45 *SYN FLOOD ATTACK* 125
FIGURE 46 *SMURF ATTACK* 126
FIGURE 47 *DDOS ATTACK* 128
FIGURE 48 ENVOIE DES DONNEES COLLECTEES PAR LES CAPTEURS A L'EQUIPE MEDICALE VIA UN RESEAU INTERNET 132
FIGURE 49 STRUCTURE DE DONNEES SKETCH 134
FIGURE 50 LES ATTAQUES INJECTEES 137
FIGURE 51 NOMBRE TOTAL DE PAQUETS AVANT L'INJECTION DES ATTAQUES (A GAUCHE) ET APRES L'INJECTION DES ATTAQUES (A DROITE) 138
FIGURE 52 NOMBRE TOTAL DE SEGMENTS TCP AVANT L'INJECTION DES ATTAQUES (A GAUCHE) ET APRES L'INJECTION DES ATTAQUES (A DROITE) 138
FIGURE 53 NOMBRE DE SYN AVANT L'INJECTION DES ATTAQUES (A GAUCHE) ET APRES L'INJECTION DES ATTAQUES (A DROITE) 139
FIGURE 54 HELLINGER DISTANCE (A GAUCHE) ET POWER DIVERGENCE POUR B=0.5 (A DROITE) 140
FIGURE 55 KULLBACK-LEIBLER DIVERGENCE (A GAUCHE) ET POWER DIVERGENCE POUR B=1 (A DROITE) 140
FIGURE 56 CHI-SQUARE DIVERGENCE (A GAUCHE) ET POWER DIVERGENCE POUR B=2 (A DROITE) 141
FIGURE 57 POWER DIVERGENCE POUR B=1.5 (A GAUCHE) ET POWER DIVERGENCE POUR B=2.5 (A DROITE) 141
FIGURE 58 JENSEN-SHANNON DIVERGENCE 142
FIGURE 59 COURBE ROC 143
FIGURE 60 TAUX DE DETECTION ET TAUX DE FAUSSE ALARME 144

Liste des tableaux

TABLEAU 1 DIFFERENCES ENTRE WBAN ET WSN 28
TABLEAU 2 LES AVANTAGES ET LES INCONVENIENTS DES TOPOLOGIES DANS LES RESEAUX WBAN 33
TABLEAU 3 CAPTEURS UTILISES DANS LES SYSTEMES WBAN ET LEUR FONCTION, TOPOLOGIE ET DEBIT 37
TABLEAU 4 CARACTERISTIQUES DES CAPTEURS LES PLUS COURANTS 40
TABLEAU 5 COMPARAISON ENTRE LES CARACTERISTIQUES DE QUELQUES SYSTEMES D'EXPLOITATION 41
TABLEAU 6 COMPARAISON ENTRE PLUSIEURS PROJETS DE RECHERCHE BAN (BODY AREA NETWORK) [1] 45
TABLEAU 7 COMPARAISON ENTRE LES DIFFERENTES TECHNOLOGIES SANS FIL 48
TABLEAU 8 LES CONTRAINTES DE SECURITE DANS UN RCSF CORPORELS 58
TABLEAU 9 CLASSIFICATIONS DES ATTAQUANTS 63
TABLEAU 10 CLASSIFICATION DES ATTAQUES POSSIBLES DANS UN SYSTEME DE SURVEILLANCE MEDICALE A DISTANCE 64
TABLEAU 11 CLASSIFICATION DES ANOMALIES DANS LES RCSF 71
TABLEAU 12 EVALUATION DES DIFFERENTES APPROCHES DE DETECTION DES ANOMALIES 75
TABLEAU 13 COMPARAISON ENTRE LES TRAVAUX DE RECHERCHE CONCERNANT LA DETECTION DU JAMMING 83
TABLEAU 14 LES STRATEGIES DES DIFFERENTS TYPES DE BROUILLEURS 89
TABLEAU 15 PDR AVEC DIFFERENTS TYPES DES BROUILLEURS 92
TABLEAU 16 BPR AVEC DIFFERENTS TYPES DES BROUILLEURS 93
TABLEAU 17 ECA AVEC DIFFERENTS TYPES DES BROUILLEURS 94
TABLEAU 18 PSR AVEC DIFFERENTS TYPES DES BROUILLEURS 95
TABLEAU 19 RELATION ENTRE PDR ET RSSI 95
TABLEAU 20 NIVEAU DU RSSI AVEC DIFFERENTS TYPES DES BROUILLEURS 96
TABLEAU 21 PARAMETRES DE SIMULATION 104
TABLEAU 22 LA VALEUR MOYENNE DU PDR, BPR, PSR ECA ET RSSI AVEC DEBIT =1 PAQUET/12 S 107
TABLEAU 23 LA VALEUR MOYENNE DU PDR, BPR, PSR ECA ET RSSI AVEC DEBIT =1 PAQUET/2 S 108
TABLEAU 24 VALEURS UTILISEES DANS LA SIMULATION 109
TABLEAU 25 RESULTATS NUMERIQUES DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/12 S) 112
TABLEAU 26 RESULTATS NUMERIQUES DANS LE CAS (2-PARAMETRES, DEBIT=1 PAQUET/2 S) 113
TABLEAU 27 RESULTATS NUMERIQUES DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/12 S) 115
TABLEAU 28 RESULTATS NUMERIQUES DANS LE CAS (3-PARAMETRES, DEBIT=1 PAQUET/2 S) 116
TABLEAU 29 RESULTATS NUMERIQUES DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/12 S) 118
TABLEAU 30 RESULTATS NUMERIQUES DANS LE CAS (4-PARAMETRES, DEBIT=1 PAQUET/2 S) 119
TABLEAU 31 COMPARAISON ENTRE NOTRE PROPOSITION ET QUELQUES TRAVAUX DE RECHERCHE 121
TABLEAU 32 CAS PARTICULIER DE POWER DIVERGENCE 132

Chapitre I : Introduction générale

1. Contexte et problématique

L'essor des nouvelles technologies ainsi que les progrès effectués dans les domaines des micro-électroniques, des télécommunications, des réseaux et du traitement de l'information ont entraîné l'apparition de nouveaux outils et objets communicants qui améliorent notre qualité de vie. Parmi ces objets communicants nous intéressons aux capteurs.

Au cours des dernières décennies et grâce à l'avancée des systèmes embarqués et des technologies sans fil, les Réseaux de Capteurs Sans Fil (RCSF), ou « *Wireless Sensor Network* (WSN) », sont de plus en plus utilisés dans de nombreux domaines. Parmi ces domaines, nous nous intéressons aux RCSF pour les applications médicales.

Imaginons un ensemble de petits appareils électroniques, autonomes, équipés de capteurs et capables de communiquer entre eux via un médium sans fil, chacun de ces petits appareils constitue un nœud capteur médical. Ces nœuds déployés sur le corps du patient ou dans son environnement forment ensemble un réseau de capteurs sans fil médicaux qui est capable de surveiller l'état de santé du patient en collectant des informations physiologiques et de communiquer ensuite ces informations à une équipe médicale à distance.

L'un des défis majeurs du monde de ces dernières décennies a été l'augmentation continue de la population des personnes âgées dans les pays développés. Durant la dernière décennie, le nombre de personnes âgées et dépendantes n'a cessé de progresser en France, les personnes de 65 ans ou plus représentent environ 17,5% de la population au 1er Janvier 2013 (contre 16,1 % il y a dix ans) [106]. D'où la nécessité de fournir des soins de qualité à une population en croissance rapide, tout en réduisant les coûts des soins de santé. Donc la mise en œuvre de systèmes permettant de réduire les frais d'hospitalisation des patients et de minimiser le temps de présence du personnel médical est un véritable challenge.

Dans ce contexte, de nombreux travaux de recherche portent sur l'utilisation des réseaux de capteurs sans fil médicaux dans les systèmes WBAN (Wireless Body Area Network), pour faciliter et améliorer la qualité du soin et de surveillance médicale à distance. Ces réseaux

sont caractérisés par la mobilité de leurs nœuds capteurs, par leur facilité de déploiement et leur auto-organisation, ce qui est un point avantageux pour la surveillance des personnes âgées, des personnes à mobilité réduite, des personnes à risques et des personnes ayant des maladies chroniques ainsi que pour la surveillance de leur environnement de vie.

Les réseaux des capteurs sans fil médicaux sont utilisés aujourd'hui dans la médecine pour surveiller certains signes vitaux comme la température, la pression artérielle ou le rythme cardiaque, etc. Donc les systèmes WBAN permettent non seulement d'améliorer la qualité de vie des patients, mais aussi le suivi des patients en temps réel et d'intervenir le plus rapidement possible dans les cas d'urgences.

Ces réseaux de capteurs médicaux sans fils soulèvent de nouveaux défis technologiques en termes de sécurité et de protection contre les anomalies et les attaques. Le mode de communication sans fil utilisé entre ces capteurs et l'unité de traitement (puits ou *sink* en anglais) accentue ces vulnérabilités.

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

En effet les vulnérabilités dans un système WBAN de surveillance médicale à distance se décomposent en deux parties principales. La première partie se compose des anomalies possibles dans les nœuds capteurs et les attaques possibles sur le réseau des capteurs médicaux et sur le médium de communications sans fils entre ces capteurs et le nœud de collecte. La deuxième partie se compose des attaques possibles sur les communications à haut débit entre le système WBAN et le serveur médical.

2. Principales contributions de la thèse

Une partie de notre travail dans cette thèse est consacré à faire un état de l'art sur les systèmes WBAN en présentant l'architecture des nœuds capteurs et leurs caractéristiques, l'architecture des systèmes WBAN et leurs caractéristiques et protocoles de communications,

les applications et les avantages des WBAN dans le domaine médical et les exigences et challenges pour les WBAN.

Dans la deuxième partie, et afin de répondre en partie aux problèmes de sécurité et de détection des attaques dans un système WBAN de surveillance médicale à distance, nous cherchons dans cette partie à présenter les différentes attaques et anomalies possibles dans ce système et à proposer et évaluer des solutions pour la détection des attaques.

Notre contribution principale comporte deux volets essentiels:

La proposition d'un algorithme pour la détection de l'attaque de brouillage radio (*Jamming attack*) et l'identification du type de brouillage radio: nous définissons un algorithme qui repose sur la comparaison entre les valeurs de cinq paramètres réseau mesurés à chaque période « Te » et un seuil relatif à chacun de ces paramètres. La validation du modèle est réalisée par simulation et l'évaluation de cet algorithme est réalisée en comparant les résultats du taux de détection et du taux de fausses alarmes avec deux autres méthodes.

La proposition d'une méthode de mesure de divergence pour détecter les attaques de type *SYN flooding* : cette méthode est basée sur une approche statistique, la validation de cette méthode est réalisée sur des traces réelles, et l'évaluation de cette méthode est réalisée en comparant les résultats du taux de détection et du taux de fausses alarmes avec quatre autres méthodes.

3. Organisation du mémoire

Cette thèse est organisée en six chapitres répartis en deux parties principales : une partie état de l'art et une partie contribution. La partie état de l'art présente les systèmes WBAN et leurs applications dans le domaine médical et les attaques et anomalies possibles dans les systèmes WBAN de surveillance médicale à distance. La partie contribution expose nos propositions pour détecter deux types d'attaques.

Le mémoire est organisé de la façon suivante :

Le Chapitre I présente le contexte général, les motivations, les problématiques et les principales contributions de ce travail.

Dans le Chapitre II, nous présentons l'architecture d'un nœud capteur, ses caractéristiques, les systèmes d'exploitation embarqués dans les capteurs et les différents types de capteurs

corporels utilisés dans la médecine. Nous décrivons les caractéristiques des réseaux WBAN : leurs spécificités par rapport aux réseaux WSN, les topologies les plus utilisées pour le déploiement des réseaux WBAN, les protocoles de communications sans fil utilisés dans les différentes parties d'un système WBAN de surveillance médicale à distance. Nous présentons aussi les applications des réseaux WBAN dans le domaine de surveillance médicale et leurs avantages apportés pour la médecine, ainsi qu'un état de l'art sur les projets de recherche utilisant les WBAN. Nous décrivons aussi les principaux challenges pour les réseaux WBAN.

Dans le Chapitre III, nous discutons les contraintes de sécurité dans les RCSF médicaux, nous classifions les attaquants selon trois critères, et nous décrivons les différents types d'attaques possibles dans un système WBAN de surveillance médicale à distance et nous les classifions selon plusieurs critères. Puis nous décrivons les anomalies possibles dans les réseaux de capteurs sans fils d'un système WBAN et nous parlons brièvement des techniques de détection des anomalies dans les réseaux de capteurs sans fil. Ensuite, nous présentons un état de l'art sur les travaux de recherche concernant la détection de l'attaque *jamming* dans les réseaux sans fils et nous faisons une comparaison entre ces méthodes selon plusieurs critères. Enfin, nous présentons quelques solutions proposées pour défendre contre ce type d'attaque dans les réseaux sans fil.

Dans le Chapitre IV, nous définissons quatre types de l'attaque *jamming*. Nous présentons les paramètres réseau que nous allons utiliser comme critères pour la détection du *jamming* et l'identification du type de *jamming*. Nous expliquons l'influence de chaque type de *jamming* sur la valeur de chacun de ces paramètres réseau. Puis nous présentons notre proposition pour la détection du *jamming* en détaillant les étapes de l'algorithme. Ensuite, nous décrivons l'environnement de simulation, et nous présentons les résultats obtenus. Pour évaluer notre proposition, nous faisons une comparaison de performances avec deux autres propositions en termes de taux de détection et de taux de fausses alarmes. Enfin, nous discutons les résultats obtenus.

Dans le Chapitre V, nous présentons quelques types de l'attaque déni de service. Puis nous exposons notre approche proposée, où nous définissons la structure des données « *Sketch* ». Nous donnons les définitions des mesures de divergences existantes et la définition de la mesure de divergence proposée « *Power Divergence* » que nous allons utiliser dans la détection de l'attaque *SYN flooding*. Nous présentons l'architecture du système et le seuil utilisé pour la détection de l'attaque *SYN flooding*. Pour appliquer notre méthode, nous utilisons des traces réelles collectées d'un trafic internet où nous présentons les courbes de

variations du nombre de paquets et du nombre de SYN avant et après l'injection d'un certain nombre d'attaques ayant des intensités différentes. Puis nous présentons les résultats obtenus, et nous évaluons les performances des différentes mesures de divergence en termes de taux de détection et de taux de fausses alarmes. Cette étape d'évaluation permet de montrer l'intérêt de la solution proposée. Enfin, nous discutons la valeur optimale d'une variable critique β dans l'équation du *Power Divergence* qui donne le meilleur taux de détection avec le taux de fausses alarmes le plus réduit.

Dans le Chapitre VI, nous concluons cette thèse et nous présentons quelques perspectives de travail pour le futur.

4. Liste des publications

-Ali Makke, Ahmed Mehaoua, Rani Makke and Abderrahim Benslimane, "Jamming Attack Detection and Jammer Type Identification in Wireless Body Area Networks", submitted to the Journal of Wireless Communications and Mobile Computing, April 2014.

-Ali Makke and Ahmed Mehaoua, "Jamming Attack Detection in Wireless Body Area Networks", accepted in the 2nd IEEE International Conferences on Biomedical and Health Informatics (BHI'2014), Valencia, Spain, June 2014.

-Ali Makke, Osman Salem, Mohamad Assaad, Hassine Moungla and Ahmed Mehaoua, "Flooding Attacks Detection in Backbone Traffic Using Power Divergence", in the 7th ACM International Workshop on Performance Monitoring, Measurement and Evaluation of Heterogeneous Wireless and Wired Networks (PM2HW2N 12), Paphos, Cyprus, pages: 15-20, October 2012.

-Jean Tajer, Ali Makke, Osman Salem and Ahmed Mehaoua, "A Comparison Between divergence measures for Network Anomaly Detection", in the 7th IEEE International Conference on Network and Service Management (CNSM 11), Paris, France, pages: 1-5, October 2011.

-Osman Salem, Ali Makke, Jean Tajer and Ahmed Mehaoua, "Flooding Attacks Detection in Traffic of Backbone Networks", in the 36th IEEE Local Computer Networks (LCN 11), Bonn, Germany, pages: 441-449, October 2011.

Chapitre II : Les réseaux de capteurs médicaux sans fil

1. Introduction

Les Réseaux de Capteurs Sans Fil (RCSF) ou Wireless Sensors Networks (WSN) en anglais sont une véritable révolution en matière de réseaux informatiques sans fil et de systèmes micro électromécanique MEMS (Micro Electro Mechanical Systems).

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique et des technologies de communication sans fil ont permis de produire avec un coût raisonnable des micro capteurs, qui sont de véritables systèmes embarqués. Ces capteurs ont trois fonctions : capter les valeurs de grandeurs physiques, traiter des informations à l'aide de ces valeurs collectées et les communiquer à travers un réseau de capteurs.

Le déploiement de plusieurs capteurs sur le corps humain, en vue de collecter des données physiologiques (température, pression artérielle, rythme cardiaque, etc.) et les transmettre d'une manière autonome vers un ou plusieurs points de collecte, forme ce qu'on appelle un réseau corporel de capteurs sans fil - Wireless Body Area Network (WBAN).

Un réseau de capteurs sans fil médical est un ensemble de nœuds (chaque nœud représentant un capteur) qui sont déposés sur des objets ou des individus mouvants. Chaque nœud peut communiquer avec les autres nœuds qui sont situés dans sa zone de couverture. Les données collectées par ces nœuds sont communiquées directement ou via les autres nœuds de proche en proche à un point de collecte appelé "station de base" ou "puits". Cette station de base a une capacité de stockage et une puissance de traitement plus importantes que les capteurs. Elle peut aussi avoir un rôle de contrôleur du réseau et elle fait parfois le lien entre l'utilisateur et le réseau.

L'utilisation de ces capteurs dans le domaine médical offre énormément d'avantages et apporte des nouveaux conforts aux patients tels que la mobilité du patient, la surveillance à distance des personnes âgées et à mobilité réduite, ainsi que les soins à long terme.

Les réseaux des capteurs sans fil sont utilisés aujourd'hui dans la médecine pour surveiller certains signes vitaux. L'utilisation des réseaux sans fil pourra améliorer la qualité des soins : l'absence d'installations électriques contraignantes, la réduction de l'encombrement des fils reliant les capteurs à l'unité de traitement, la facilité de mise en place ainsi que la liberté de mouvement pour le patient.

Ils permettent non seulement d'améliorer la qualité de vie des malades, qui peuvent rester chez eux, mais aussi le suivi des patients en temps réel ainsi que l'intervention le plus rapidement possible en cas d'urgence (par exemple si les mesures remontées par les capteurs sont anormales). La Figure 1 représente un système de surveillance médicale à distance qui utilise les réseaux WBAN, où plusieurs capteurs médicaux sont déployés sur le corps du patient afin de mesurer plusieurs paramètres physiologiques. Les données mesurées seront ensuite envoyées à l'équipe médicale via un réseau haut débit afin qu'elle puisse surveiller l'état de santé du patient et faire l'action nécessaire dans les cas d'urgence.

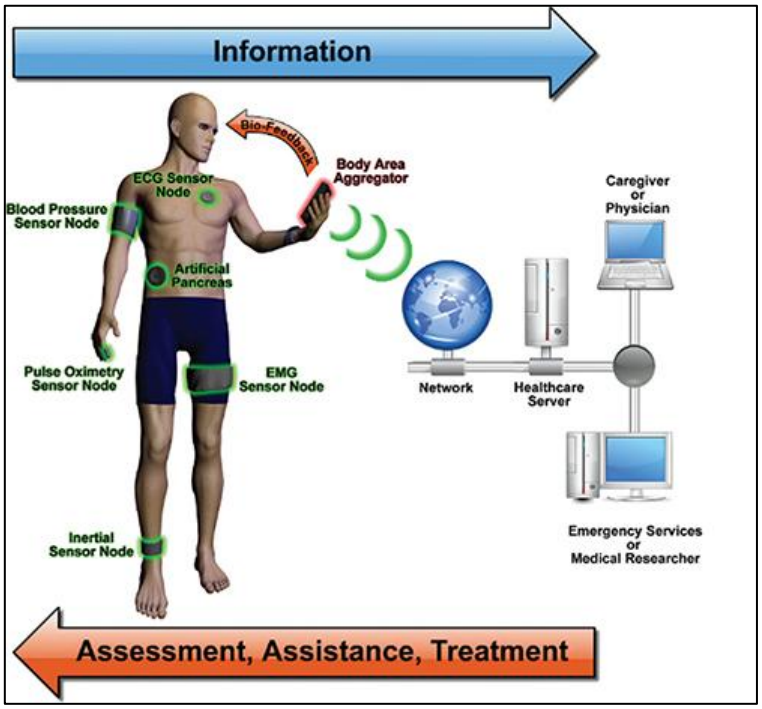


Figure 1 Système de surveillance médicale WBAN

Dans ce chapitre, nous faisons un état de l'art sur les réseaux WBAN : l'architecture des systèmes WBAN, leurs caractéristiques et leurs protocoles de communications, l'architecture des nœuds capteurs et leurs caractéristiques et les différents types de capteurs corporels, les

applications et les avantages des WBAN dans le domaine médical et les défis et contraintes pour les réseaux WBAN.

2. Architecture des réseaux WBAN

2.1. Les réseaux WBAN

2.1.1. Comparaison entre les réseaux WBAN et les réseaux WSN

2.1.1.1. Définition

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

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

2.1.1.2. Différence entre WBAN et WSN

Nous présentons ici les différences entre WBAN et WSN qui sont classifiées selon plusieurs facteurs. Le Tableau 1 résume ces différences.

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

Tableau 1 Différences entre WBAN et WSN

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

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

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

Latence: Dans le cas des réseaux WBAN, le remplacement des batteries pour les capteurs est beaucoup plus facile par rapport au cas dans les réseaux WSN dont les nœuds peuvent être physiquement inaccessibles après le déploiement. Par conséquence, il peut être nécessaire de maximiser la durée de vie des batteries dans un réseau WSN. Le temps de latence dans les

WBAN est plus petit par rapport au temps de latence dans les WSN à cause de nombre des sauts réduits.

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

2.1.2. Les sous-systèmes d'un système WBAN de surveillance médicale

Un système WBAN de surveillance médicale complet se divise en cinq sous-systèmes [9]:

-Le sous-système BAN (Body Area Network).

-Le sous-système PAN (Personal Area Network).

-La passerelle vers les réseaux étendus (WAN: Wide Area Network).

-Les réseaux étendus.

-L'utilisateur final de l'application de surveillance médicale.

La Figure 2 représente les différents sous-systèmes constituant un système de surveillance médicale.

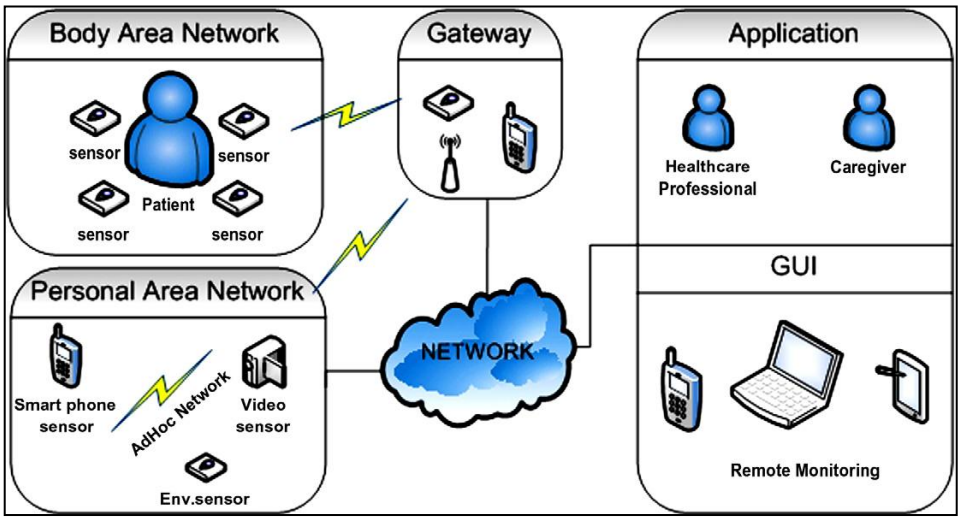


Figure 2 Architecture d'un système de surveillance médicale [9]

2.1.2.1. Le sous-système BAN

Il se compose d'un réseau de capteurs et des étiquettes RFID (Radio Frequency IDentification) qui sont déployés sur le corps du patient. Il y a plusieurs types de ces

capteurs. Par exemple les capteurs qui mesurent l'ECG, l'EEG, la température, la tension artérielle du patient, etc.

2.1.2.2. Le sous-système PAN

Ce sous-système est composé de capteurs environnementaux et des appareils déployés autour du patient. Les capteurs environnementaux, comme les capteurs qui mesurent la pression atmosphérique, la température, la luminosité et l'humidité, peuvent aider à fournir des informations riches sur l'environnement où se trouve le patient. Les appareils comme les caméras vidéo servent encore à surveiller et à localiser le patient en temps réel.

2.1.2.3. Le sous-système de passerelle

Il est responsable d'établir la connexion entre les sous-systèmes BAN et PAN d'une part et les réseaux étendus d'autre part. La passerelle peut être un dispositif portable porté par l'utilisateur comme un PDA (*Personal Digital Assistant*), un téléphone intelligent, un nœud capteur déployé dans l'environnement ainsi qu'un ordinateur portable.

2.1.2.4. Les réseaux étendus

Pour un scénario de surveillance et de suivi à distance, une infrastructure de réseau est inévitable. La passerelle peut transmettre de l'information à un ou plusieurs systèmes réseaux en fonction de l'application. Les systèmes réseaux utilisés peuvent être des réseaux cellulaires, des réseaux téléphoniques ordinaires, des réseaux satellites ou bien le réseau Internet.

2.1.2.5. L'utilisateur final

Le dernier sous-système est composé de l'utilisateur final du système de surveillance médicale qui est représenté par l'équipe médicale (médecins, infirmiers). Dans ce sous-système, les données médicales collectées sont interprétées et les actions nécessaires sont déclenchées.

2.1.3. Topologies des réseaux WBAN

Dans cette section, nous décrivons les topologies les plus utilisées pour le déploiement des réseaux WBAN. Nous distinguons les topologies suivantes : point-à-point, étoile, maille et arbre. La Figure 3 représente ces quatre topologies.

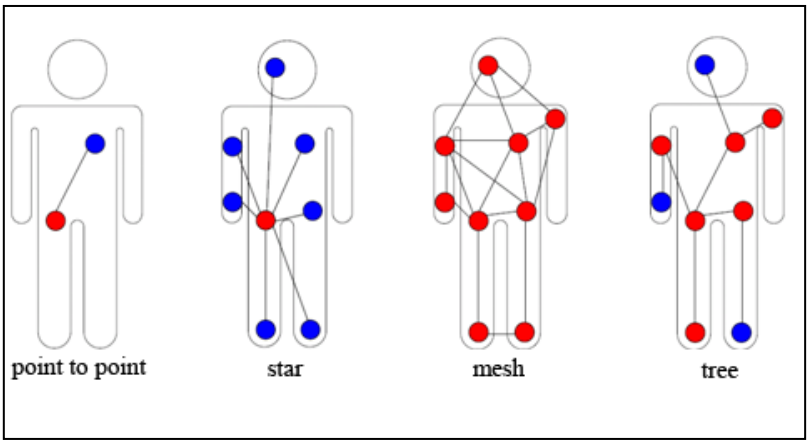


Figure 3 Les topologies dans les réseaux WBAN

2.1.3.1. Topologie Point-à-point

C'est la topologie la plus simple dans les réseaux. Cette topologie est destinée à une seule liaison, par exemple entre un collecteur de données et un nœud capteur.

Le principal avantage de cette topologie est la simplicité qui permet souvent l'utilisation d'un protocole simple, la faible latence et le débit élevé. Les inconvénients comprennent ses fonctionnalités limitées ainsi que sa faible couverture.

2.1.3.2. Topologie en Etoile

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

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

2.1.3.3. Topologie en Maille

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

transmettre un message à un autre nœud hors de sa portée de transmission, peut utiliser un nœud intermédiaire pour envoyer son message au nœud destinataire.

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

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

2.1.3.4. Topologie en Arbre

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

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

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

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

Tableau 2 Les avantages et les inconvénients des topologies dans les réseaux WBAN

2.2. Les nœuds capteurs

2.2.1. Définition d'un capteur médical

Un capteur est un dispositif ayant pour tâche de transformer une mesure physique observée en une mesure généralement électrique qui sera à son tour traduite en une donnée binaire exploitable et compréhensible pour un système d'information.

Un capteur médical se constitue d'un capteur équipé d'un circuit électronique spécifique capable de mesurer un ou plusieurs paramètres physiologiques.

Donc : capteur + circuit électronique spécifique = capteur médical.

2.2.2. Les capteurs médicaux

Dans cette section, nous décrivons plusieurs types de capteurs médicaux utilisés dans la médecine et qui sont disponibles dans le commerce [1], [21], [28]. Des exemples de ces capteurs médicaux avec leurs exigences en termes de débit (montrant l'impact sur leur consommation d'énergie) sont présentés dans la Figure 4 et la Figure 5.

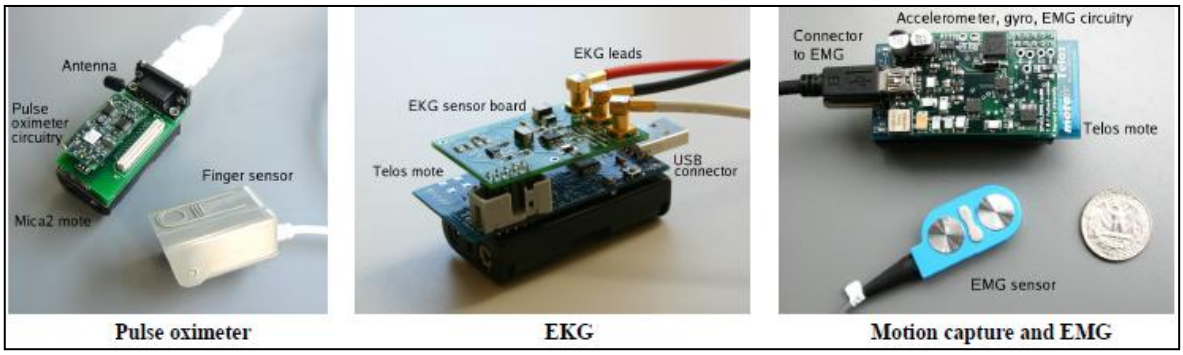


Figure 4 Exemples de capteurs médicaux

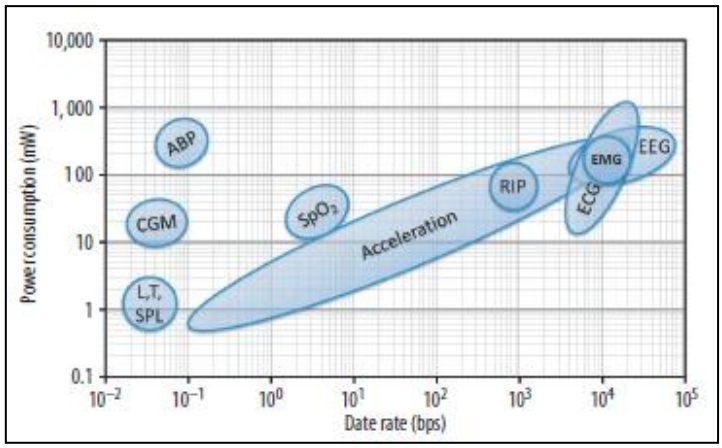


Figure 5 « Consommation moyenne de puissance vs Débit » pour les capteurs corporels [1]

2.2.2.1. Accéléromètre et Gyroscope

L'accéléromètre est utilisé pour reconnaître et surveiller la posture du corps (assis, debout, marcher et courir). Cette surveillance est essentielle pour de nombreuses applications, y compris les soins de la santé. Le système de surveillance de posture est basé sur 3 accéléromètres triaxiaux qui sont placés sur des endroits stratégiques du corps humain.

Le Gyroscope est utilisé pour la mesure ou le maintien de l'orientation et peut être utilisé conjointement avec des accéléromètres pour la surveillance des mouvements physiques.

[1] ABP: Ambulatory Blood Pressure; CGM: Continuous Glucose Monitoring; L, T, SPL: Light, Temperature, Sound Pressure Level; SpO2: Pulse oximetry; RIP: Respiratory Inductive Plethysmography; ECG: electrocardiography; EMG: electromyography; EEG: electroencephalography

2.2.2.2. Capteur de Glycémie

Il est utilisé pour mesurer la concentration de glucose dans le sang. Traditionnellement, les mesures de glucose sont effectuées en piquant un doigt et l'extraction d'une goutte de sang. Un glucomètre est utilisé pour analyser l'échantillon de sang et donner un affichage numérique du taux de glucose.

2.2.2.3. Capteur de tension artérielle

Le capteur de tension artérielle est un capteur conçu pour mesurer les pressions systolique et diastolique du sang humain, en utilisant la technique oscillométrique.

2.2.2.4. Détecteur de gaz CO2

Il mesure le niveau de dioxyde de carbone gazeux pour surveiller les changements dans le niveau du CO2, ainsi que pour surveiller la concentration d'oxygène lors de la respiration humaine.

2.2.2.5. Capteur ECG

L'Electrocardiographie est une méthode qui mesure les signaux électriques produits par le cœur. Il permet d'évaluer l'activité cardiaque (rythme cardiaque, intervalle entre deux battements) en interceptant l'activité électrique qui provient du muscle cardiaque.

L'électrocardiographie (ECG) est une représentation graphique du potentiel électrique qui commande l'activité musculaire du cœur. Ce potentiel est recueilli par des électrodes à la surface de la peau. Il permet de mettre en évidence diverses anomalies cardiaques et a une place importante dans les examens diagnostiques en cardiologie.

2.2.2.6. Capteur EEG

L'électro-encéphalographie (EEG) est une méthode d'exploration cérébrale qui mesure l'activité électrique du cerveau par des électrodes placées sur le cuir chevelu. Elle est souvent représentée sous la forme d'un tracé appelé électro-encéphalogramme. L'EEG est un examen qui renseigne sur l'activité neurophysiologique du cerveau au cours du temps et en particulier du cortex cérébral, soit dans un but diagnostique en neurologie, soit dans la recherche en neurosciences cognitives.

2.2.2.7. Capteur EMG

L'électromyogramme est un examen qui permet d'enregistrer l'activité électrique d'un muscle ou d'un nerf. Le capteur EMG mesure les signaux électriques produits par les muscles

pendant la contraction ou pendant le repos. Il permet de détecter les atteintes nerveuses périphériques et les atteintes des muscles.

2.2.2.8. Capteur Oxymétrie de pouls (SpO2)

L'oxymétrie de pouls ou saturation en oxygène est une méthode de mesure de la saturation en oxygène de l'hémoglobine au niveau des capillaires sanguins. On parle de saturation pulsée en oxygène : SpO2. Un petit clip avec un capteur est fixé au doigt de la personne. Le capteur émet un signal lumineux qui passe à travers la peau. Selon l'absorption de la lumière par l'hémoglobine oxygénée et l'hémoglobine totale dans le sang artériel, la mesure est exprimée en tant que rapport de l'hémoglobine oxygénée à la quantité totale d'hémoglobine.

2.2.2.9. Capteurs de température et d'humidité

Le capteur de température est utilisé pour mesurer la température du corps humain et/ou de l'environnement entourant le patient. Le capteur d'humidité est utilisé pour mesurer l'humidité de l'environnement entourant le patient. Un signal d'alarme peut être émis si un certain nombre de modifications sont mesurées.

2.2.2.10. Récapitulatif

Le Tableau 3 résume les capteurs mentionnés dans les paragraphes précédents ainsi que leurs fonctions et débit de données.

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

Tableau 3 Capteurs utilisés dans les systèmes WBAN et leur fonction, topologie et débit

2.2.3. Architecture d'un nœud-capteur

La Figure 6 représente un nœud-capteur qui est composé de plusieurs éléments ou modules. Chaque module correspond à une tâche particulière de captage et d'acquisition, de traitement ou de transmission de données. Il comprend également une source d'énergie.

Chaque capteur est composé de quatre unités : l'unité d'acquisition des données, l'unité de traitement, l'unité de communication et l'unité de contrôle d'énergie.

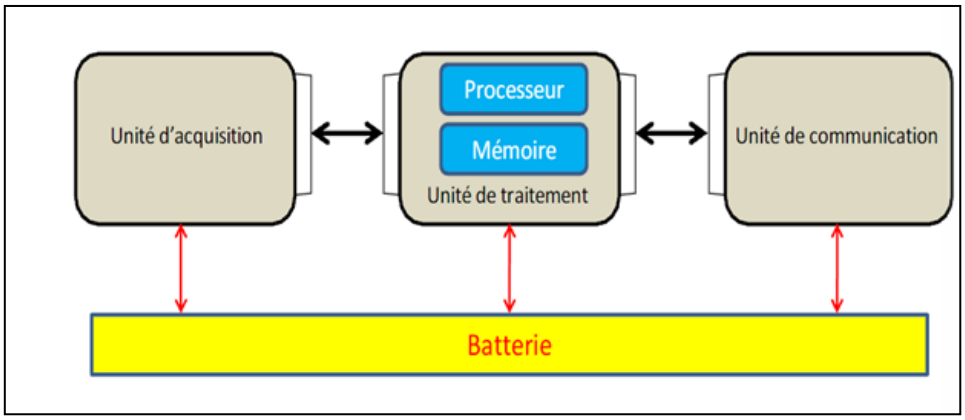


Figure 6 Architecture d'un nœud-capteur

2.2.3.1. L'unité de captage et d'acquisition des données

Elle peut contenir un ou plusieurs modules de détection. Cette unité joue le rôle d'échantillonnage et de conversion des signaux physiques en signaux électriques (conversion analogique-numérique). Les données collectées par cette unité seront ensuite traitées par l'unité de traitement.

2.2.3.2. L'unité de traitement

Elle comprend un processeur généralement associé à une petite unité de stockage. Elle fonctionne à l'aide d'un système d'exploitation spécialement conçu pour les micro-capteurs. Cette unité possède deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de communication. Elle acquiert les informations en provenance de l'unité d'acquisition et les envoie à l'unité de communication. Cette unité est chargée aussi de l'exécution des protocoles de communications qui permettent de faire collaborer le nœud avec les autres nœuds du réseau. Elle peut aussi analyser les données captées.

2.2.3.3. L'unité de communication

Unité responsable de toutes les émissions et réceptions de données via un support de communication radio qui permet la communication entre les différents nœuds du réseau. Elle peut être de type optique ou de type radiofréquence.

-Les communications de type optique sont robustes vis-à-vis des interférences électriques. Néanmoins, ne pouvant pas établir de liaisons à travers des obstacles, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes.

-Les unités de transmission de type radiofréquence comprennent des circuits de modulation, démodulation, filtrage et multiplexage ; ceci implique une augmentation de la

complexité et du coût de production du micro-capteur. Elles sont exposées aux interférences électromagnétiques, mais ont l'avantage de ne pas exiger une ligne de vue permanente entre les entités communicantes.

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

2.2.3.4. L'unité de contrôle d'énergie

Un capteur est muni d'une ressource énergétique (généralement une batterie). Étant donné sa petite taille, cette ressource énergétique est limitée. Donc l'énergie est la ressource la plus précieuse d'un réseau de capteurs car elle a une influence directe sur la durée de vie des capteurs et donc du réseau entier.

L'unité de contrôle d'énergie constitue donc une partie essentielle du système. Elle doit répartir l'énergie disponible aux autres modules de manière optimale (par exemple en réduisant les dépenses inutiles et en mettant en veille les composants inactifs).

Un nœud capteur peut se trouver dans l'un des quatre états suivants: actif en mode d'écoute, actif en mode de traitement des données, actif en mode de transmission ou non actif en mode veille. Un capteur est en veille lorsque sa radio est éteinte ; Dans ce cas, sa consommation d'énergie est presque nulle. En effet, la principale source de consommation d'énergie d'un capteur est l'utilisation du réseau sans fil via son module de radiocommunications. Cette consommation d'énergie peut être réduite par la diminution de la transmission des données.

2.2.4. Caractéristiques des capteurs

Chaque modèle de capteur a des caractéristiques spécifiques en termes de capacité de mémoire, capacité de stockage, du modèle du microcontrôleur et du débit des données. La Figure 7 représente des échantillons de capteurs et le Tableau 4 présente les principales caractéristiques des capteurs les plus connus et les plus utilisés dans le domaine de la recherche.

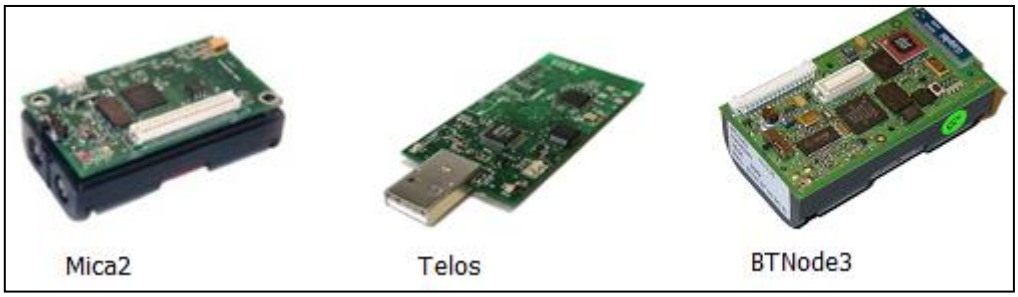


Figure 7 Echantillon des capteurs

Nom du capteur	RAM	Mémoire	Stockage	Débit	Type de Microcontrôleur
Mica	4 KB	128 KB	512 KB	40 kbps	ATMega128
Mica2				38.4 kbps	
Mica2Dot					
MicaZ				250 kbps	
Rene2	1 KB	16 KB	32 KB	10 kbps	ATMega163
TelosA	2 KB	60 KB	512 KB	250 kbps	TI MSP430
TelosB	10 KB	48 KB	1 MB		TI MSP430
Tmote Sky	10 KB	48 KB	1 MB	250 kbps	TI MSP430
BTnode3	4 KB	128 KB	180 KB	721 kbps	ATMega128
Iris	8 KB	128 KB	512 KB	250 kbps	ATmega1281
Imote	64KB	512KB	---	720 kbps	ARM7
Imote2	256KB	32KB	32 MB	500 kbps	Intel PXA271 Xscale

Tableau 4 Caractéristiques des capteurs les plus courants

2.2.5. Systèmes d'exploitation pour les capteurs

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

sont des interfaces informatiques spécifiques destinées au fonctionnement des capteurs dans les réseaux.

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

Il existe plusieurs systèmes d'exploitation pour les réseaux de capteurs sans fils comme : TinyOS, Contiki, MANTIS OS, LiteOS, RETOS, Nano-RK [24], [25], [26], [27]. Il y a certaines caractéristiques qui font la différence entre ces systèmes d'exploitation [24], par exemple : l'architecture, le modèle de programmation, la gestion de la mémoire, le langage de programmation. Le Tableau 5 fait une comparaison entre les caractéristiques de quelques systèmes d'exploitation.

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

Tableau 5 Comparaison entre les caractéristiques de quelques systèmes d'exploitation

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

2.2.5.1. TinyOS

TinyOS est un système d'exploitation open source pour les réseaux de capteurs sans fil qui trouve sa genèse au sein du laboratoire d'informatique de l'université de Berkeley et qui a été l'un des premiers systèmes d'exploitation conçus pour les réseaux de capteurs miniatures. En effet, TinyOS est le plus répandu des OS pour les réseaux de capteurs sans-fil. Il est capable d'intégrer très rapidement les innovations en relation avec l'avancement des applications et des réseaux eux-mêmes tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs.

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

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

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

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

2.2.5.2. Contiki

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

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

Le noyau Contiki reste, nativement, un système d'exploitation basé sur les événements. Pour obtenir le mode multitâche, une bibliothèque doit être installée. Les fonctions associées à cette bibliothèque n'accèdent pas directement à l'ensemble des ressources du capteur sans fil. Elles doivent, dans certains cas, faire appel à la partie du noyau dédié à la gestion des événements. Cette structure à deux niveaux a pour conséquence une dégradation des performances du système quand le mode multitâche est activé.

2.2.5.3. MANTIS OS

MANTIS (MultimodAl NeTworks of In-situ micro Sensor) OS apparu en 2005, a été conçu par l'université du Colorado [28]. C'est un système d'exploitation léger et multitâche pour les capteurs adapté aux applications où plusieurs traitements, chacun associé à un ou plusieurs processus, sont en concurrence pour accéder aux ressources du capteur sans fil.

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

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

2.3. Architecture de communication dans les systèmes WBAN

La Figure 8 illustre une architecture générale d'un système WBAN (Wireless Body Area Network) de surveillance médical, où plusieurs types de capteurs corporels envoient leurs données mesurées à un serveur par le biais d'une connexion sans fil. Ensuite, ces données sont transmises (via internet par exemple) à l'équipe médicale pour obtenir un diagnostic en temps

réel ou à une base de données médicale pour les enregistrer, ou bien à un équipement correspondant qui émet une alerte d'urgence.

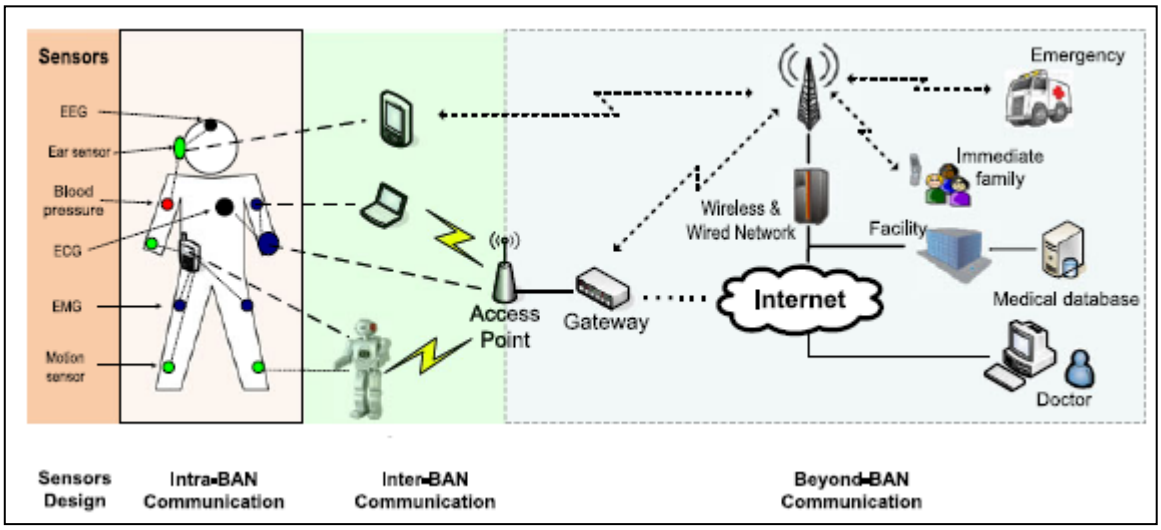


Figure 8 Architecture générale des communications dans un système BAN [1]

Nous décomposons les communications dans un système BAN en trois composantes [1]: Communications «Intra-BAN», Communications «Inter-BAN» et Communications « Au-delà de BAN».

2.3.1. Communications «Intra-BAN»

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

2.3.2. Communications «Inter-BAN»

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

2.3.3. Communications « Au-delà de BAN»

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

Le Tableau 6 présente une comparaison, en termes de type des capteurs utilisés et des protocoles de communications utilisées dans chacune des trois composantes citées ci-dessus, entre plusieurs projets de recherche BAN dans le domaine médical.

Projects	Sensors	Intra-BSN communication	Inter-BSN communication	Beyond-BSN communication	Targeted Application
CodeBlue	Pulse oximeter EKG, motion	Wired	Mesh & Zigbee	N/A	Medical care
AID-N	Pulse, Blood, Temperature,ECG	Wired	Mesh & Zigbee	Internet/WiFi/ Cellular Networks	Mass casualty incident
SMART	ECG, SpO2 sensor	Wired	802.11b	N/A	Health monitoring In waiting room
CareNet	Tri-axial accelerometer/ gyroscope	N/A	Zigbee	Multi-hop 802.11/ Internet	Remote healthcare
ASNET	Blood pressure, temperature	Star topology	GPRS/GSM	N/A	Remote health monitoring
MITHril	ECG, EKG	Wired	WiFi	N/A	Healthcare
WHMS	ECG, EMG, EEG, SpO2 & motion sensor	Star topology	WLAN/Bluetooth/ GPRS	Internet	Telemedicine

Tableau 6 Comparaison entre plusieurs projets de recherche BAN (Body Area Network) [1]

2.3.4. Protocoles de communications sans fil

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

2.3.4.1. La norme IEEE 802.15.1 / Bluetooth

Initialement, la norme Bluetooth a été proposée pour transmettre la voix et les données [2]. Elle avait pour objectif préalable de permettre des communications sur de courtes distances avec un débit de communication limitée. Ses caractéristiques ont ainsi retenu l'attention des développeurs de capteurs. Par exemple les capteurs BtNode sont conçus pour une

communication de type Bluetooth. Pour autant, le protocole Bluetooth n'est pas le protocole le plus utilisé dans les réseaux de capteurs, bien qu'il puisse répondre en partie aux problèmes de préservation de l'énergie, car il est gravement handicapé par la taille limitée du réseau qu'il peut former (8 nœuds, 1 maître et 7 esclaves).

2.3.4.2. La norme Wibree (Ultra Low Power Bluetooth)

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

2.3.4.3. La norme IEEE 802.15.3 / UWB (Ultra Wide Band)

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

2.3.4.4. La norme IEEE 802.15.4 / Zigbee

Elle est conçue pour être utilisée dans les communications à très faible puissance et sur des distances réduites. Cette technologie est utilisée dans les réseaux de capteurs sans fil [6]. Par rapport à Bluetooth, cette technologie fournit une faible latence; une couche physique « DSSS : Direct Sequence Spread Spectrum » permet aux nœuds de basculer en mode sommeil sans perdre la synchronisation. Le protocole Zigbee est basé sur le standard IEEE 802.15.4 qui définit sa couche PHY et MAC et qui permet de prolonger théoriquement la durée de vie d'un nœud sur plusieurs années. L'autre point fort de ce protocole est qu'il propose le

déploiement de réseau dense à plus de 65000 nœuds avec une portée de l'ordre de 100 mètres pour un débit de 250 Kbits/s. Ces caractéristiques en font aujourd'hui le principal protocole utilisé dans les réseaux de capteurs.

2.3.4.5. La norme IEEE 802.15.6

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

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

2.3.4.6. La norme IEEE 802.11x/WiFi

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

2.3.4.7. Choix de la norme

Le choix d'une technologie de communication sans fil dépend des services proposés, ainsi que des besoins du concepteur du réseau. Certains paramètres comme la consommation

d'énergie, le débit, la durée de vie de la pile, la portée et le nombre de nœuds supportés doivent être pris en compte. Dans le Tableau 7, nous faisons une comparaison entre les protocoles de communications cités ci-dessus [21], [23], [31], [32].

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

Tableau 7 Comparaison entre les différentes technologies sans fil

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

En tenant compte de ces contraintes, la technologie ZigBee peut être envisagée pour la transmission de données médicales collectées par les capteurs déployés sur le corps humain vers le nœud de collecte c.à.d. dans les communications intra-BAN et inter-BAN. En effet,

cette technologie présente une faible consommation d'énergie et une longue portée mais son inconvénient est le faible débit des données.

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

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

3. Les systèmes WBAN dans le domaine médical

3.1. Les avantages apportés par les systèmes WBAN dans le domaine médical

L'un des défis majeurs du monde de ces dernières décennies est l'augmentation continue de la population des personnes âgées dans les pays développés. Les études de population prévoient que dans les 20 prochaines années, les personnes ayant plus de 65 ans représenteront 20% de la population totale [9]. D'où la nécessité de fournir des soins de qualité à une population en croissance rapide, tout en réduisant les coûts des soins de santé.

Les applications médicales des réseaux de capteurs sans fil améliorent la qualité des soins et la surveillance médicale surtout pour les personnes âgées et les patients ayant des maladies chroniques. Ceci en offrant plusieurs avantages dans le domaine médical.

La Figure 9 représente un système de surveillance médicale à distance pour les personnes âgées.

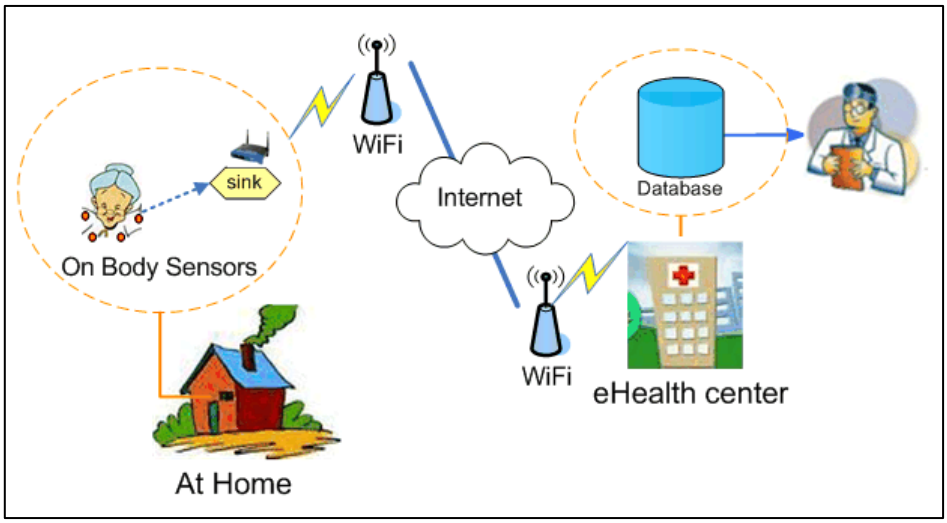


Figure 9 Surveillance médicale à distance des personnes âgées

L'avantage principal d'un tel système est la capacité de surveillance à distance. Avec une surveillance à distance, l'identification des situations d'urgence pour les patients à risque deviendra plus facile et les personnes ayant de déficience cognitive et physique peuvent avoir une vie plus indépendante et plus facile.

L'identification rapide des situations d'urgence comme les crises cardiaques ou les chutes brusques suffisent pour sauver la vie d'un patient. Sans ces systèmes de surveillance médicale en temps réel, ces situations ne seront pas identifiées, d'où un important avantage apporté par les systèmes WBAN qui est la surveillance en temps réel.

Une grande partie de la médecine moderne ne serait pas possible, ni rentable sans les capteurs corporelles tels que les thermomètres, les tensiomètres, les glucomètres, l'électrocardiographie (ECG), l'électroencéphalographie (EEG) et diverses formes de capteurs d'imageries. La capacité de surveiller en permanence l'état physiologique du patient est également essentielle pour les dispositifs interventionnels tels que les stimulateurs cardiaques et les pompes à insuline.

Les réseaux de capteurs peuvent aussi être utilisés pour assurer une surveillance permanente des organes vitaux de l'être humain grâce à des micro-capteurs qui pourront être avalés ou implantés sous la peau (surveillance de la glycémie, détection de cancers, etc.). Ils peuvent aussi faciliter le diagnostic de quelques maladies en effectuant des mesures physiologiques telles que la tension artérielle, les battements du cœur, etc. D'autre part, ces

réseaux peuvent détecter des comportements anormaux (chute d'un lit, choc, cri, etc.) chez les personnes dépendantes (handicapées ou âgées).

Nous citons encore parmi les avantages des systèmes WBAN: la liberté de mouvement pour le patient et les soins à long terme pour les patients ayant des maladies chroniques. La Figure 10 résume les avantages des réseaux WBAN dans le domaine médical.

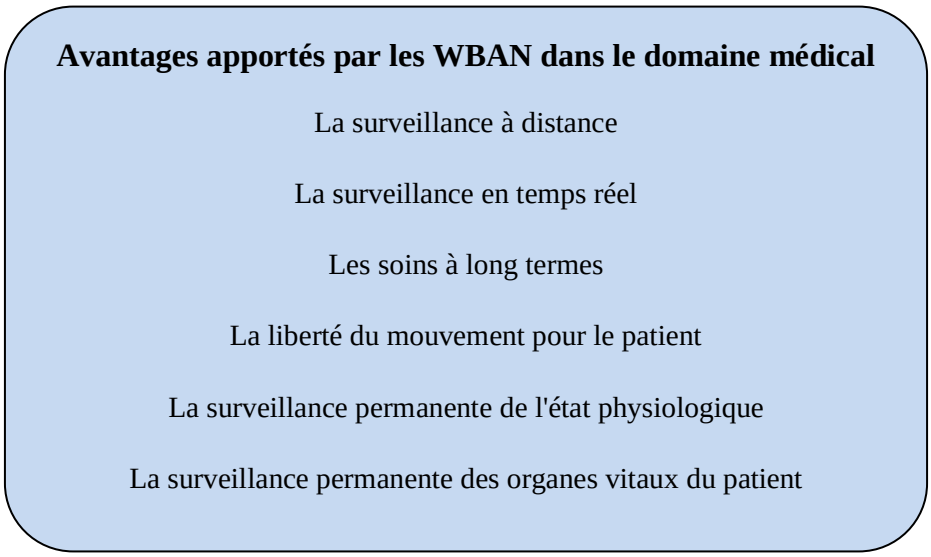


Figure 10 Les avantages apportés par les WBAN dans le domaine médical

3.2. Les applications des WBAN dans le domaine de surveillance médicale

Il existe plusieurs applications médicales pour la surveillance de la santé des patients en général et des personnes âgées en particulier. Lorsque ces applications sont explorées, nous observons que les catégories principales cibles sont [9]:

-La surveillance des activités de la vie quotidienne

-La détection de chute et du mouvement

-La localisation

-Le suivi de prise des médicaments

-La surveillance de l'état de santé

-La bio-surveillance

-La prédiction des maladies

3.2.1. La surveillance des activités de la vie quotidienne

Dans cette catégorie, les applications tentent d'aider les personnes âgées à leur domicile pour améliorer leur qualité de vie. Les capteurs observent les activités quotidiennes de ces personnes et partagent les données observés avec les équipes médicales, où les données seront traitées et analysées [10]. Ces données peuvent donner des indices sur l'état de santé de la personne, et permettrait l'intervention de l'équipe médicale dans les cas nécessaires.

3.2.2. La détection de chute et du mouvement

Les applications de détection de chute et du mouvement sont axées sur les conditions physiologiques telles que la posture et la détection de chute pour les personnes qui ont besoin de soin particulier. Par exemple, les personnes âgées qui sont sensibles à la chute soudaine qui peut entraîner leur mort ou bien les patients en convalescence après une opération [9].

3.2.3. Le suivi de prise des médicaments

La non prise des médicaments est fréquente chez les personnes âgées et les malades ayant des maladies chroniques [9], en particulier lorsque des déficiences cognitives sont présentés. Par conséquence, la surveillance et le rappel de prise des médicaments pour ce genre de malades est très important car il peut les aider à survivre d'une manière indépendante.

3.2.4. La localisation des patients ou de l'équipe médicale

Dans les systèmes de surveillance médicale, l'application de localisation peut être utilisée pour aider les personnes ayant une déficience cognitive. Ils peuvent aussi être utilises pour l'identification des emplacements des patients quand une situation d'alarme est survenue comme une crise d'épilepsie.

En plus, dans un hôpital, on peut utiliser les systèmes de localisation pour surveiller les endroits visités par les patients afin d'identifier les infections nosocomiales ou pour localiser les médecins et les personnels paramédicaux dans les cas d'urgence.

Un autre scénario médical est le cas d'urgence ou de catastrophe. Les gens sont équipés de petits badges sans fil, ce qui pourrait guider les équipes de secours et les médecins à gérer d'une façon plus efficace un nombre plus élevé de victimes [10]. Par exemple, le premier

sauveteur qui arrive dans une zone sinistrée ou dans une zone où il y a un accident avec un grand nombre de victimes, placerait un capteur sans fil sur chaque patient. Ce capteur peut envoyer les signes vitaux et l'emplacement de chaque patient à l'équipe médicale qui est à proximité.

3.2.5. La surveillance de l'état de santé

La surveillance de l'état de santé des patients est le type d'application le plus étudié des systèmes de santé omniprésents. Les signes vitaux couramment utilisés afin d'obtenir des informations complètes sur l'état de santé des patients sont : ECG, EEG, le taux de respiration, l'oxymétrie de pouls, la température corporelle, le rythme cardiaque, la pression artérielle, etc. [9], [10], [11], [13].

Dans un scénario de soins à l'hôpital ou à domicile, les patients sont équipés de minuscules capteurs portables sans fil qui mesurent les signes vitaux. Ceci permettrait aux médecins et aux infirmières de surveiller en permanence l'état de santé de leurs patients et de réagir à des changements tels que l'insuffisance respiratoire, l'arrêt cardiaque, etc.

La surveillance du niveau de glucose à l'aide d'un capteur sans fil implanté sous la peau du patient peut aider l'équipe médicale à contrôler le niveau de glucose chez les patients diabétiques et à anticiper leurs besoins en insuline. Par ailleurs, l'insuline peut être injectée automatiquement lorsqu'un certain seuil du niveau de glucose est atteint [11].

Pour des millions de patients souffrant d'asthme dans le monde [11], une crise allergique soudaine peut causer une grave menace à leur vie. Un système de réseau de capteurs sans fil peut les aider en leur présentant des nœuds de capteurs capables de détecter les allergènes dans l'air et rendre compte de l'état aux médecins et / ou aux patients d'une façon permanente.

Les maladies cardiovasculaires provoquent un grand nombre de décès dans les pays développés. La plupart de ces décès pourraient être évités si les médecins avaient été au courant sur l'état de santé actuel du patient. Des nœuds de capteurs installés sur le corps du patient d'une manière discrète pourront envoyer les informations vitales concernant les irrégularités du rythme cardiaque aux personnels médicales, ce qui leurs permet la préparation préalable du traitement nécessaire, tout en surveillant l'état de santé du patient.

Pour les patients ayant subis à l'hôpital des opérations ou des traitements qui demandent une longue période de rétablissement à domicile, un système de capteurs portables permet de

surveiller ces patients et de fournir des évaluations précises pour guider le processus de réadaptation.

3.2.6. La Bio-surveillance

Une autre application médicale pour les systèmes de capteurs sans fil est la bio-surveillance, où une série de capteurs peuvent recueillir et examiner des échantillons de l'air, du sol ou de l'eau pour prédire la diffusion épidémiologique d'une maladie. Ce qui permet aux fonctionnaires d'état et aux établissements de santé de réagir rapidement en prenant une série d'actions d'urgence [10].

3.2.7. La prédiction des maladies

Des études ont montré que les cellules cancéreuses dégagent de l'oxyde nitrique, ce qui affecte le sang dans la zone entourant une tumeur. Des capteurs avec la possibilité de détecter ces changements dans le sang ont la capacité d'identifier les cellules cancéreuses, ce qui permet aux médecins de diagnostiquer les tumeurs [11].

3.3. Etat de l'art sur les projets de recherches des systèmes WBAN

Le milieu médical trouve un grand intérêt dans l'utilisation des réseaux de capteurs sans fil. En effet, plusieurs projets et travaux de recherches ont été réalisés pour développer des systèmes utilisant les réseaux de capteurs sans fil. Ils sont principalement utilisés pour surveiller l'état de santé des patients au sein de l'hôpital. Toutes ces applications ont pour but de créer une surveillance active et permanente de la santé des patients. Nous citons parmi ces projets :

-Le projet STAR (Système Télé-Assistant Réparti) [14], consistait à concevoir une plateforme dédiée à la surveillance de personnes souffrant de troubles du rythme cardiaque. En effet, les arythmies cardiaques sont des phénomènes difficiles à diagnostiquer de part leur nature intermittente et très aléatoire.

Dans le cadre du projet STAR, le patient est équipé d'un capteur sans fil intelligent capable d'acquérir et d'analyser ses signaux ECG en temps réel. En effet, le capteur utilise un module de transmission sans fil « Bluetooth » qui lui permet de communiquer avec une passerelle présente au domicile du patient et connectée à Internet. Ensuite les données collectées par le

capteur sont envoyés via Internet vers un centre de traitement et d'intervention situé au sein d'un hôpital.

-Le projet CodeBlue a été un des premiers projets développés par l'université de Harvard utilisant les réseaux de capteurs sans fil. Il consiste à équiper des patients de capteurs relevant les informations physiologiques tel que les pulsations cardiaques, le niveau d'oxygénation, etc. [15], [30]. En cas de relevé anormal sur le patient, les capteurs transmettent l'information à un dispositif de type PDA (Personal Digital Assistant) porté par un membre du personnel soignant pour l'avertir afin qu'il intervienne sur le patient au plus vite. Ce projet a débouché sur un autre projet de l'université de Harvard, le projet Mercury [16] qui vise à surveiller les patients atteints de la maladie de Parkinson ou souffrant de crises d'épilepsie.

-Le projet MobiHealth est l'un des premiers projets européens sur le développement d'un réseau de capteurs sans fil pour la santé, basé sur les technologies de téléphonie mobile GPRS et UMTS [17]. Le réseau WBAN est constitué de capteurs et actionneurs et d'une unité de base mobile MBU « Mobile Base Unit » jouant le rôle d'un hub (topologie en étoile). La communication GPRS est utilisée pour la communication entre le WBAN et le téléphone/PDA. Ensuite, les données collectées par ce dernier sont transmises via UMTS vers le centre de surveillance [31].

-Le projet RESIDE-HIS est un projet français d'habitat intelligent pour la santé. C'est le travail d'une collaboration entre les laboratoires TIMC et CLIPS à Grenoble (par les deux équipes AFIRM et GEOD [18]). Un gilet de télé-assistance nomade appelé « VTAMN» est développé. Il embarque différents types de capteurs avec différents types de données recueillies : le poids, le taux d'oxygène dans le sang, la fréquence cardiaque et respiratoire et la glycémie. Les données sont envoyées vers un centre de surveillance à distance.

-Le projet BANET a l'objectif de fournir des modèles et des technologies pour concevoir un système de communication sans fils optimisé pour un large champ d'applications (dans le domaine de l'électronique, du médical et du sport), utilisant un réseau BAN [12]. Le but à long terme pour BANET est la réduction maximale de la consommation d'énergie du réseau BAN.

-Le projet SMART a été développé pour surveiller les signaux physiologiques des patients dans les salles d'attente des services d'urgence [1]. Il y a eu des cas dans lesquels l'équipe médicale a constaté que la santé du patient se détériore rapidement en attendant dans une salle d'urgence. Comme le temps est d'une grande importance dans ce genre de situation,

la vie des patients ne peut pas être risquée en raison du manque d'attention accordée dans les salles d'urgence. Pour aider à résoudre ce problème, le système SMART peut être utilisé pour collecter des données à partir des différents patients en attente dans une salle d'urgence, et d'envoyer ces données à un ordinateur central qui collecte et analyse les données pour émettre un signal d'alerte si l'état de santé d'un patient particulier se détériore. De cette façon, les patients peuvent recevoir un traitement avant que leur état de santé s'aggrave.

-Le projet CareNet développe un système sans fil de surveillance médicale à distance qui permet à l'équipe soignante d'accéder efficacement aux données du réseau de capteurs grâce à un système de dossier médical unifié [1], [19].

-Le projet ALARM-NET offre un système de soin médical par la surveillance continue du patient en utilisant des capteurs corporels [1]. ALARM-NET met en œuvre un réseau de capteurs sans fil qui permet aux personnels médicaux de surveiller en permanence l'état de santé des patients.

4. Les défis et les contraintes des réseaux WBAN

4.1. Les défis des réseaux WBAN

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

4.1.1. Le défi d'énergie

Le principal facteur limitant la durée de vie d'un réseau de capteurs est l'énergie. Donc l'optimisation de l'énergie est un défi qui est rencontré dans presque tous les domaines d'application des réseaux de capteurs sans fil, parmi lesquelles les applications médicales. Les capteurs actuels ont des périodes de veille durant leur inactivité pour préserver leur batterie. Les sources de consommation d'énergie dans un nœud capteur proviennent principalement de l'unité de captage, de l'unité de traitement des données et de l'unité de communications (transmission et réception sans fils) [12].

Les communications sont les actions qui coûtent le plus cher en termes d'énergie et les calculs le sont mais avec une moindre importance. Il est donc fortement nécessaire de limiter le nombre de communications entre capteurs et si possible la quantité de calculs [29].

4.1.2. Tolérance aux pannes

Dans les réseaux de capteurs sans fil, un ou plusieurs capteurs peuvent ne pas fonctionner correctement, car les capteurs sont des entités sensibles aux altérations d'états comme des phénomènes climatiques (humidité, chaleur, etc.) ou du fait d'une batterie faible. Dans ces cas, le réseau doit être capable de détecter ce type d'erreur et d'y remédier, afin de transmettre l'information et permettre au réseau d'être toujours opérationnel [29].

4.1.3. La sécurité

Les applications médicales imposent des exigences strictes en termes de fiabilité du système de bout en bout et de livraison des données [13]. La communication des données médicales entre les capteurs d'un système WBAN est soumise à des exigences de sécurité telles que la disponibilité du réseau, la confidentialité, l'authenticité, l'intégrité et la fraîcheur des données.

4.1.3.1. La disponibilité du réseau

Le réseau doit pouvoir être disponible à tout instant, c.à.d. que l'envoi d'information ne doit pas être interrompu, de même que la circulation de l'information ne doit pas être stoppée. Dans le cas d'un réseau de capteurs réactif, il faut qu'un capteur, qui détecte un événement, puisse transmettre à tout instant cette information vers la base du réseau de capteurs pour l'en informer [30].

4.1.3.2. La confidentialité des données

Le réseau doit s'assurer que les données transmises soient confidentielles et ne puissent être lues par des dispositifs ou personnes autres que l'équipe médicale (médecins, infirmiers, etc.). Une personne extérieure au réseau ne doit pas être capable de lire les informations échangées. Les données doivent être cachées ou cryptées de telle manière que personne ne puissent y accéder.

4.1.3.3. L'authentification

L'authentification des capteurs est nécessaire pour s'assurer que l'identité déclarée par un capteur est bien celle du capteur déclarant. En l'absence d'un mécanisme permettant

d'authentifier clairement un nœud du réseau, de nombreuses attaques peuvent se mettre en place.

4.1.3.4. L'intégrité des données

Les données circulant sur le réseau WBAN ne doivent pas pouvoir être altérées au cours de la communication. Il faut donc s'assurer que personne ne puisse capturer et modifier les données du réseau. Aussi, il faut vérifier que les données n'ont pas subi d'altérations dues à un disfonctionnement du matériel, qui est un risque important sur des capteurs sensibles aux altérations d'états.

4.1.3.5. La fraîcheur des données

Par fraîcheur des données, nous entendons savoir si les données sont récentes ou non. Cela signifie qu'il faut s'assurer que la donnée transmise corresponde à un état présent. La fraîcheur des données garantit ainsi que ces données ne reflètent pas un état passé [30].

4.2. Les contraintes des réseaux WBAN

Un réseau de capteurs sans fil médicaux est un réseau spécial qui a un certain nombre de contraintes par rapport à un réseau informatique classique. Ces contraintes sont le résultat des limitations concernant la mémoire du capteur, sa réserve énergétique, sa capacité de traitement ainsi que l'utilisation d'une communication sans fil. Les contraintes dans un réseau de capteurs sans fil médicaux sont classées en deux catégories : contraintes matérielles et contraintes réseau [46], [60]. Le Tableau 8 résume ces contraintes.

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

Tableau 8 Les contraintes de sécurité dans un RCSF corporels

4.2.1. Contraintes matérielles

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

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

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

Capacité de calcul limitée : Malgré les progrès dans la fabrication de capteurs de plus en plus puissants, les capteurs actuels possèdent une capacité de calcul très réduite. Cette faible capacité de calcul ne permet pas d'utiliser des algorithmes complexes, et particulièrement des algorithmes cryptographiques gourmands en ressources CPU [11], [29].

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

4.2.2. Contraintes réseaux

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

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

5. Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur les réseaux de capteurs sans fils médicaux. Après une introduction générale sur les réseaux de capteurs sans fil médicaux, nous avons parlé des systèmes WBAN où nous avons fait une comparaison entre les réseaux WBAN et WSN. Puis nous avons décrit les sous-systèmes constituant un système WBAN de surveillance médical à distance ainsi que les topologies les plus utilisées pour le déploiement des réseaux WBAN.

Ensuite nous avons donné une définition technique du capteur médical et nous avons présenté plusieurs types de capteurs médicaux avec leurs fonctions. Puis nous avons présenté l'architecture d'un nœud capteur, ses caractéristiques et les systèmes d'exploitation dans les capteurs. Après nous avons présenté l'architecture des communications dans les systèmes WBAN, et les protocoles de communications sans fil qui peuvent être utilisés.

Dans la deuxième partie du chapitre, nous avons parlé des avantages apportés par les systèmes WBAN dans le domaine médical et nous avons décrit les différentes applications dans le domaine de la surveillance médicale. Puis nous avons fait un état de l'art sur les projets de recherche sur les systèmes WBAN dans le domaine médical.

Finalement, nous avons parlé des contraintes et des principaux défis pour les systèmes WBAN dans les applications de surveillance médicale.

Dans le chapitre suivant, nous allons faire un état de l'art sur les attaques et les anomalies potentielles dans les systèmes WBAN en les classifiant selon la partie du système WBAN qu'elles visent. Puis nous concentrerons sur un type d'attaque qui est le brouillage radio (*Jamming attack*) en présentant quelques travaux de recherches qui traitent la détection de ce type d'attaque.

Chapitre III : Les attaques et les anomalies dans les systèmes WBAN

1. Introduction

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

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

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

Dans ce chapitre, nous faisons un état de l'art sur les attaques et les anomalies possibles dans les systèmes WBAN ainsi que sur les travaux de recherche concernant la détection de l'attaque de brouillage radio (*jamming*).

2. Les attaques et les anomalies dans les systèmes WBAN

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

2.1. Classifications des attaquants

Différents types de modèles d'attaquants avec différentes motivations peuvent mener une même attaque, ce qui rend la modélisation d'un attaquant essentielle dans l'étude de la sécurité des réseaux de capteurs. La modélisation d'un attaquant dépend du type de l'attaque à exécuter, de sa position par rapport au réseau et du nombre d'adversaires utilisés. Dans un réseau de capteurs, un attaquant peut être classifié selon plusieurs critères (Tableau 9).

2.1.1. Selon son intention

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

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

2.1.2. Selon sa position par rapport au réseau

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

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

2.1.3. Selon sa capacité

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

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

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

Tableau 9 Classifications des attaquants

2.2. Classification des attaques possibles dans un système WBAN

Les réseaux de capteurs sans fils médicaux sont vulnérables à un nombre considérable d'attaques. Ces attaques sont menées de manières différentes et peuvent être classées selon leur but en trois catégories principales [61] : les attaques qui visent la vie privée et l'authentification, les attaques qui visent l'intégrité de service et les attaques qui visent la disponibilité du réseau.

Dans cette section, nous décrivons une liste représentative des attaques les plus possibles qu'on peut trouver dans les systèmes WBAN [46], [47], [48], [49], [50], [51], [62], [63], [64], [67], [68]. Ces attaques seront classifiées selon la cible qu'ils visent dans le système WBAN. Le Tableau 10 représente une classification des attaques possibles dans un système WBAN de surveillance médicale à distance.

Cible attaquée	Nom de l'Attaque	But/résultat de l'attaque	Active/passive	Couche	Menace	Attaquant
Les nœuds capteurs	Privation de mise en veille	Epuiser la batterie du nœud / nœud hors service	Active	Liaison	Intégrité, disponibilité	Externe
	Flooding	Saturer le réseau et épuiser la mémoire et l'énergie des nœuds	Active	Transport	Intégrité, disponibilité	Externe
	Insertion de boucles infinies	Saturer le réseau et épuiser l'énergie des nœuds	Active	Réseau et routage	Intégrité, disponibilité	Interne
Communications sans fil intra et inter-BAN	Jamming	Empêcher, intercepter ou bloquer la communication dans le réseau / messages endommagés ou perdus	Active	Physique, liaison	Intégrité, disponibilité	Externe
	Ecoute passive	Intercepter les informations /confidentialité cassée	Passive	Application	Confidentialité	Externe
Communications par Internet (Au delà de BAN)	Sniffing	Lire l'information / confidentialité cassée	Passive	---	Confidentialité	Externe
	Man in the middle	Contrôler la conversation / écouter, modifier ou supprimer des données	Active	Multi	Intégrité, confidentialité	Externe
	Réplication des données	Enregistrer et envoyer des paquets à une date ultérieure / tromper le réseau	Active	Réseau	Intégrité	Interne
	Attaque par déni de service	Saturer un serveur ou bloquer le trafic / service non disponible	Active	Multi	Intégrité, disponibilité et confidentialité	Externe, Interne

Tableau 10 Classification des attaques possibles dans un système de surveillance médicale à distance

2.2.1. Les attaques qui visent les nœuds capteurs

2.2.1.1. Privation de mise en veille

Dans ce type d'attaque, un attaquant envoie un grand nombre de messages à un capteur du réseau pour l'obliger a rester en mode de réception ou bien en lui demandant beaucoup de calcul [62]. L'objectif de l'attaquant est d'empêcher par différente manière le capteur de se mettre en veille afin d'épuiser son énergie jusqu'à ce qu'il devienne hors service. Dans un système WBAN de surveillance médicale à distance, si un capteur devient hors service, il ne peut plus mesurer les données physiologiques ni les transférer sur le réseau et donc l'équipe

médicale ne peut plus recevoir des informations vitales sur l'état de santé du patient ce qui est dangereux pour la santé du patient.

2.2.1.2. Flooding (Inondation)

Le *Flooding* consiste à utiliser un ou plusieurs nœuds capteurs malicieux ou un dispositif particulier avec une puissance d'émission forte, pour envoyer régulièrement des messages sur le réseau afin de le saturer. Le *Flooding* est une attaque active qui est de même type que les attaques de déni de service dans les réseaux classiques. Dans cette attaque, le but de l'adversaire est d'épuiser la mémoire et l'énergie d'un nœud capteur légitime, où il envoi successivement des demandes de connexions avec ce nœud, ce qui engendrera à terme sa mise hors service [42], [44].

2.2.1.3. Insertion de boucles infinies

Un attaquant peut utiliser deux ou plusieurs nœuds malveillants pour envoyer une infinité de messages sur le réseau. Comme ces messages seront envoyés sans cesse par le réseau comme un jeu de ping-pong, les capteurs vont consommer leur énergie et le réseau va être saturé [44], [62].

2.2.2. Les attaques qui visent les communications sans fil dans les sous-systèmes « intra-BAN et inter- BAN »

2.2.2.1. Ecoute passive

Cette attaque consiste à écouter le réseau et à intercepter les informations circulant sur le médium [44], [62]. Elle est facilement réalisable si les messages circulant sur le réseau ne sont pas cryptés.

Par ailleurs, l'écoute passive est difficile à détecter, car de par sa nature passive, elle ne modifie pas l'activité du réseau mais elle attaque directement la confidentialité des données envoyées dans le réseau, donc un attaquant de ce type pourrait lire les données médicales des patients.

2.2.2.2. Jamming (Brouillage radio)

Le *jamming* est une attaque très connue qui s'en prend à la communication sans fil. Lors d'une attaque de *jamming*, un attaquant envoie des signaux sur la même fréquence utilise par le réseau de capteurs sans fil pour brouiller les ondes radio [33], [34], [35], [44], [62]. Les nœuds du réseau n'ont alors plus accès au médium et ne peuvent plus communiquer du fait de

ce brouillage radio. Or, un réseau sans accès au médium est un réseau hors service donc le *jamming* est une attaque de type déni de service.

Cette attaque est en général exécutée à l'aide d'un dispositif plus performant que de simples nœuds à cause des exigences énergétiques nécessaires et pour arriver à perturber le réseau de façon continue.

2.2.3. Les attaques qui visent les communications dans le sous-système « au-delà de BAN »

2.2.3.1. Sniffing attack

Si les données ne sont pas cryptées, les paquets envoyés sur le réseau Internet peuvent être espionnées. Ensuite, un attaquant peut reconstruire l'intégralité des données et lire les informations.
Bien que cette attaque est une attaque passive, mais la confidentialité des données médicales envoyées à l'équipe médicale sera violée, et l'attaquant peut avoir accès a des informations privées des patients.

Donc l'utilisation d'une attaque de *sniffing* permet à l'attaquant de lire les communications sur le réseau et d'analyser le réseau afin de récupérer des informations précieuses sur ses vulnérabilités pour les utiliser ultérieurement pour planter ou endommager le réseau.

2.2.3.2. Man in the middle attack

L'attaque « *Man in the middle* » est une écoute active, dans laquelle l'attaquant fait des connexions indépendantes avec les victimes. Ces dernières croient qu'elles parlent directement entre elles via une connexion privée, alors qu'en fait toute la conversation est contrôlée par l'attaquant. Avec cette attaque, un attaquant peut écouter, modifier ou supprimer des données.

Par exemple, dans un système de surveillance médicale à distance, l'attaquant peut contrôler les communications entre le serveur personnel (domicile du patient) et le serveur médical (Hôpital) et donc il peut écouter, modifier ou supprimer ces données médicales ce qui est très dangereux pour l'état de santé du patient.

2.2.3.3. Réplication des données

Si les paquets envoyés sur le réseau peuvent être lus et enregistrés par un attaquant, il peut encore renvoyer ces mêmes paquets à une date ultérieure pour tromper le réseau.

Pour illustrer cette attaque, on peut prendre pour exemple un réseau de capteurs qui a pour objectif de collecter des informations physiologiques du patient et de les envoyer via internet à une équipe médicale à distance. Si une alarme est détectée sur l'état de santé du patient et envoyée à l'équipe médicale, l'attaquant pourra enregistrer ce paquet, même s'il est chiffré et qu'il ne peut pas le déchiffrer, puis l'émettre à une autre date comme étant une deuxième alarme.

Cette attaque est réalisable si le paquet ne contient pas d'information concernant la date de l'envoi ou si cette date est accessible et facilement modifiable par l'attaquant.

2.2.3.4. Attaque par déni de service

C'est l'une des attaques actives les plus connues ayant pour but de rendre indisponible un service et d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Elle peut saturer par différents moyens un ordinateur ou un serveur jusqu'à ce qu'un arrêt survienne à cause de la surcharge, ou de bloquer le trafic ce qui entraîne une perte d'accès aux ressources réseau par les utilisateurs autorisés.

Dans la télémédecine, ce genre d'attaque met en danger la disponibilité du réseau. Par exemple, si un médecin utilise la télémédecine pour opérer un patient avec un serveur en temps réel, le serveur envoie et reçoit des informations vidéo. Si un attaquant attaque le serveur par une attaque de type déni de service, le médecin ne pourrait plus terminer l'opération. Donc ce type d'attaque peut dégrader la qualité de soin ou de surveillance médicale à distance.

2.3. Classifications des anomalies au sein des RCSF médicaux

Les anomalies dans les RCSF peuvent aller de défauts, telles que les pannes matérielles complètes, aux performances inattendues du système, telle que la dégradation progressive. Notons que certaines valeurs aberrantes (outliers) parmi les données mesurées par les capteurs peuvent signifier des événements dans la zone surveillée, et ne doivent pas être déclarées comme des anomalies du réseau.

Nous pouvons classifier les anomalies dans les réseaux de capteurs sans fil en trois classes [65], [66] qui sont présentés dans la Figure 11:

- Les anomalies du réseau.

- Les anomalies des nœuds.

- Les anomalies des données.

Dans la suite, nous détaillons les classes d'anomalies et nous décrivons les types d'anomalies possibles dans chacune d'elles.

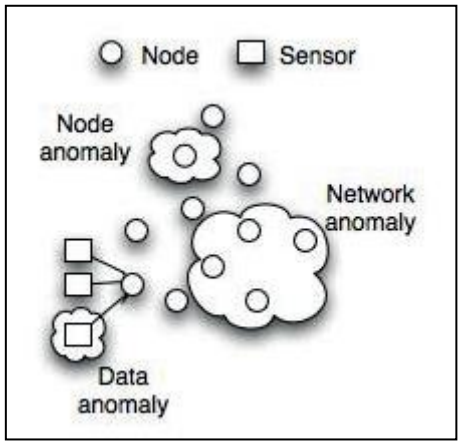


Figure 11 Les anomalies dans les RCSF

2.3.1. Les anomalies du réseau

2.3.1.1. Perte de la connectivité

Le type d'anomalie du réseau le plus simple à détecter est la perte de connectivité. L'interruption du flux de paquets provenant d'un ou de plusieurs nœuds indique une perte de connectivité avec ce ou ces nœuds. La perte de connectivité peut se produire à un groupe de nœuds, voire à tous les nœuds du réseau.

La détection des pertes de connectivité suit un processus simple: toute entité du réseau peut garder une trace des paquets provenant d'autres nœuds. L'absence de réception de paquets à partir d'un nœud ou de groupe de nœuds pour une certaine durée prédéfinie par l'opérateur signale la perte partielle ou complète de la connectivité avec ce ou ces nœuds.

Alternativement, les opérateurs peuvent fixer un seuil pour le nombre de paquets manqués avant de signaler une perte de connectivité.

Le processus de localisation de cette anomalie repose tout simplement sur l'extraction des identifiants du nœud ayant des paquets manquants. L'identification de ce nœud peut être réalisée soit par une base de données centrale ou bien localement par un nœud capteur, selon l'architecture de détection.

Les causes possibles derrière la perte de connectivité sont variables. Par exemple, si nous avons une perte de connectivité avec un groupe de nœuds ayant un nœud parent commun, donc la cause probable du problème est une défaillance matérielle ou logicielle au niveau du nœud parent. Par ailleurs, si nous avons perdu la connectivité avec plusieurs nœuds qui sont reparties sur l'ensemble du réseau, la cause probable dans ce cas est moins évidente, et pourrait être liée à la dégradation de l'état de ces nœuds.

2.3.1.2. Connectivité intermittente

La connectivité intermittente se produit lorsque la fréquence de réception des données à partir de certains nœuds est très variable par rapport à un seuil de stabilité de liaison réglé par l'opérateur. La détection de cette anomalie consiste à fixer un certain seuil sur le taux de paquets délivrés ou sur la variabilité de qualité de liaison.

La plupart des protocoles de collecte dans les RCSF incluent un numéro de séquence unique pour chaque paquet, de sorte qu'une simple vérification des écarts de numéro de séquence peut identifier le nombre de paquets manquants de chaque nœud du réseau.

La cause principale de la connectivité intermittente dans la plupart des cas est la grande variabilité de la qualité de liaison et de l'intensité du signal reçu. La connectivité intermittente dans un groupe de nœuds géographiquement concentrés dans une région du réseau indique qu'il existe des bruits élevés, des multi-trajets, ou des interférences affectant cette région.

2.3.2. Les anomalies des nœuds

2.3.2.1. Problèmes de batterie

Il y a deux possibilités lorsque la batterie ne fournit pas assez de puissance, soit un niveau de charge insuffisante de la batterie, soit une défaillance matérielle de la batterie. Donc il faut recharger la batterie dans le premier cas et la remplacer par une nouvelle batterie dans le second cas.

2.3.2.2. Défaillance d'un nœud

La mémoire, le CPU ou la radio d'un nœud, pourraient entrer dans un état d'échec durant le déploiement. Cette situation peut se produire à cause d'un composant matériel défectueux, ou par l'intégration d'un logiciel de mauvaise qualité. La détection de ce genre d'anomalie est difficile, car le problème dans un composant spécifique peut ne présenter aucun symptôme détectable par les nœuds voisins ou au niveau du nœud de collecte.

Par contre, si un ou plusieurs nœuds arrêtent leurs activités, ce genre d'anomalie est plus facilement détectable. Donc si un nœud cesse d'interagir avec n'importe quel autre nœud pour une période prédéterminée, le nœud est alors déclaré comme défaillant.

2.3.3. Les anomalies des données

Il existe trois types d'anomalies pour les données:

-« *l'anomalie temporelle* » sur un nœud due à la variation des valeurs des données mesurées par ce nœud en fonction du temps.

-« *l'anomalie spatiale* » sur un nœud unique due à la différence entre la valeur mesurée par ce nœud et les valeurs mesurées par les nœuds voisins.

-« *l'anomalie spatio-temporelle* » détectée par un certain nombre d'emplacements de nœuds en raison du changement des valeurs des données mesurées au fil du temps et de l'espace.

2.3.3.1. Les anomalies temporelles

Les anomalies temporelles des données sur un nœud présentent des symptômes tel qu'une grande variabilité dans les valeurs mesurées par un même capteur, l'absence de changement dans les valeurs mesurées par un même capteur (le capteur donne la même valeur tous le temps) ou bien la mesure des valeurs extrêmes par le capteur.

La grande variabilité dans les valeurs mesurées par un même capteur signifie la production d'un événement dans l'environnement surveillé par ce capteur, ou bien à cause des fluctuations de la tension du capteur.

Dans certains cas, les valeurs mesurées par un capteur peuvent rester les mêmes pendant une longue durée de temps, ce qui peut indiquer un état de verrouillage du capteur ou que le capteur n'a pas réussi à obtenir des nouvelles mesures.

Parfois, un capteur peut donner des mesures avec des valeurs extrêmes qui ne sont pas logiques, cela dû à un dysfonctionnement de la sonde du capteur.

2.3.3.2. Les anomalies spatiales

Les anomalies spatiales des données sur un nœud peuvent être détectées en comparant la valeur mesurée par ce nœud avec celles mesurées par les capteurs voisins. Par exemple, si la valeur de la température mesurée par un nœud est différente de celles mesurées par tous les nœuds voisins, alors il est très probable que les données sont spatialement anormales, et cela

dû à une erreur de mesure par ce nœud. Ceci s'applique à certains types de données qui ont généralement une faible variation spatiale.

2.3.3.3. Les anomalies spatio-temporelles

Les anomalies spatio-temporelles des données combinent les deux variations spatiales et temporelles. Le diagnostique de cette anomalie doit tenir compte des données de l'ensemble du réseau (c.à.d. de tous les nœuds du réseau) pendant une certaine période de temps. L'anomalie temporelle peut être détectée localement sur chaque nœud, alors que les anomalies spatiales et spatio-temporelles nécessitent une interaction entre-nœuds plus compliquée pour établir l'existence de l'anomalie.

Le Tableau 11 résume les anomalies citées ci-dessus en les classifiant selon leur classe, leur type et le diagnostic de chacune d'elles.

Classification des anomalies	Type d'anomalie	Diagnostique
Les anomalies du réseau	Perte de la connectivité	Taux de livraison de paquets = 0
	Connectivité intermittente	Grande variabilité dans le taux de livraison des paquets
Les anomalies des nœuds	Problème de batterie	Diminution du voltage de la batterie
	Défaillance d'un nœud	Manque d'interaction avec les nœuds voisins
Les anomalies des données	Anomalies temporelles	Surveillance des valeurs mesurées par un même nœud capteur en fonction du temps*
	Anomalies spatiales	Comparer la valeur mesurée par le nœud avec celles mesurées par ses voisins**
	Anomalies spatio-temporelles	* et **

Tableau 11 Classification des anomalies dans les RCSF

2.3.4. Les techniques de détection des anomalies dans les RCSF

Les algorithmes de détection des anomalies dans les réseaux de capteurs peuvent être généralement classés en quatre approches qui sont présentées dans la Figure 12. Ces approches sont les approches basées sur les statistiques, les approches basées sur la

classification, les approches basées sur le plus proche voisin et les approches basées sur le *clustering* [52], [53], [54], [55], [56], [57], [58], [59], [66].

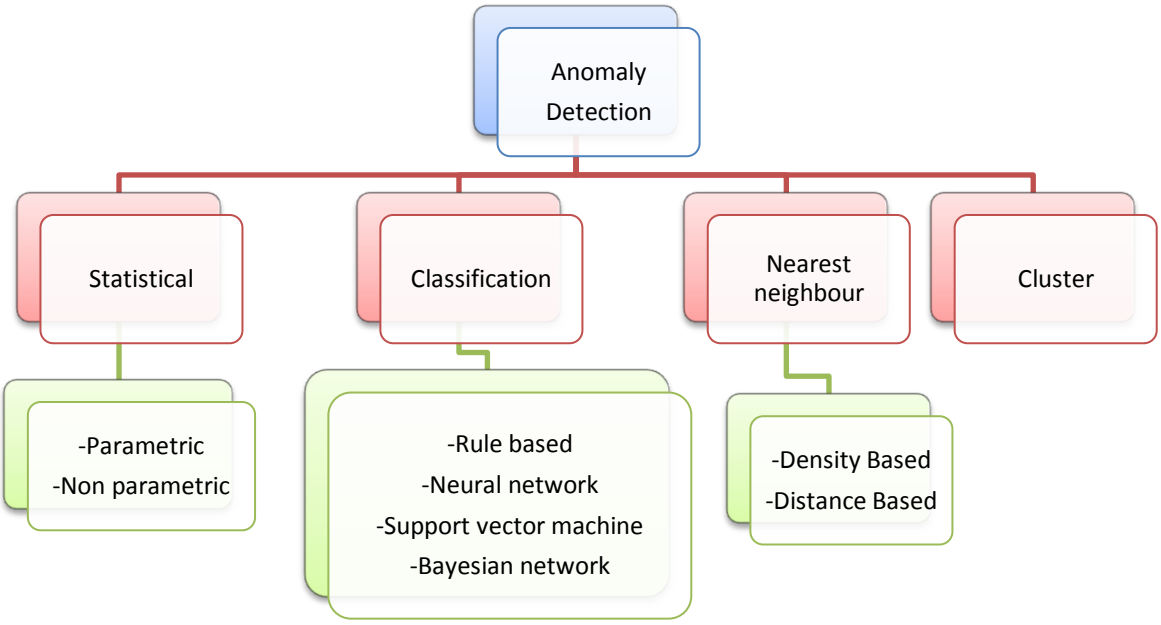


Figure 12 Techniques de détection des anomalies

2.3.4.1. Approches statistiques

Les approches fondées sur les statistiques ont été largement utilisées pour détecter les anomalies dans divers domaines tels que la détection d'intrusion dans les réseaux, la détection des défauts et la détection des fraudes.

Les techniques statistiques ajustent un modèle statistique (généralement un comportement normal) pour les données fournies. Ensuite, elles appliquent un test d'inférence statistique pour déterminer si une instance appartient à ce modèle ou non. Les instances qui ont une faible probabilité d'être générées à partir du modèle appris, sont déclarées comme des anomalies.

Les approches statistiques utilisent l'apprentissage paramétrique et non-paramétrique selon la façon dans laquelle le modèle de distribution de probabilité a été construit.

2.3.4.2. Techniques d'apprentissage paramétriques

Les techniques d'apprentissage paramétriques supposent que toutes les distributions des données utilisées pour le modèle sont connues et proviennent d'une distribution statistique telle que la distribution gaussienne ou la distribution normale. Certaines caractéristiques de

cette distribution peuvent être calculées en utilisant la moyenne et la covariance des données d'origine. Les points de données qui s'écartent significativement de la distribution des données connue peuvent être déclarés comme des anomalies.

2.3.4.3. Techniques d'apprentissage non paramétriques

Les techniques d'apprentissage non paramétriques tirent la forme générale de la fonction de distribution statistique à partir des données et des paramètres du modèle. Elles ne font aucune hypothèse sur les propriétés statistiques des données.

Ces techniques utilisent des seuils définis par l'utilisateur afin d'identifier les points des données anormales. Les techniques d'apprentissage non-paramétriques offrent une plus grande flexibilité par rapport aux techniques d'apprentissage paramétriques car elles ne nécessitent aucune connaissance préalable de la distribution des données.

2.3.4.4. Approches basées sur la classification

Les approches basées sur la classification sont des approches utilisées dans l'exploration des données et l'apprentissage automatique. Cette approche construit les classes en utilisant un ensemble de données d'apprentissage puis elle classifie les nouvelles données dans l'une des classes (normale ou anormale) comme présenté dans la Figure 13. Il s'agit d'une technique qui ne nécessite aucune connaissance des données d'apprentissage et suppose que le classificateur peut apprendre dans un espace caractéristique donné et de faire la différence entre les classes normales et anormales.

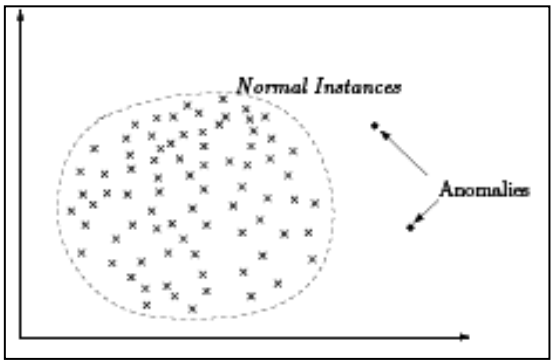


Figure 13 Approche basée sur la classification

2.3.4.5. Approche du plus proche voisin

La détection d'anomalies en utilisant la technique du plus proche voisin utilise la mesure de similarité entre les points de données pour détecter les anomalies. Cette technique est basée

sur l'hypothèse que les données normales ont généralement des proches voisins tandis que les données anormales sont généralement loin des autres points. Deux méthodes sont utilisées pour mesurer la similarité entre les points de données [54].

La première méthode utilisée est basée sur la distance, par exemple la distance euclidienne, alors les points de données qui sont loin par rapport aux autres points sont des valeurs anormales.

La seconde méthode utilise le calcul de la densité relative des voisins de chaque point de données pour déterminer les anomalies, donc les points de données qui appartiennent à une région de faible densité peuvent être déclarés comme anormaux.

2.3.4.6. Approche basée sur le *clustering*

Dans les approches à base de cluster, les points de données similaires obtenues à partir des données d'apprentissage sont regroupés en cluster. Les points de données peuvent être déclarés comme des anomalies s'ils n'appartiennent pas au cluster ou s'ils tombent dans un petit cluster. La plupart des systèmes de détection d'anomalies basés sur les clusters utilisent la distance euclidienne pour déterminer la taille du cluster.

Nous faisons une brève évaluation en termes de points forts et points faibles des différentes approches de détection des anomalies dans le Tableau 12.

Approches	Statistique	Classification	Plus proche voisins	Clustering
Points forts	-Les techniques d'apprentissage paramétriques peuvent effectivement identifier les valeurs aberrantes si un modèle de distribution de probabilité est acquis. -Les techniques d'apprentissage non paramétriques sont attractives en raison du fait qu'elles ne font aucune hypothèse sur les caractéristiques de la distribution.	-Fournissent un ensemble précis des valeurs aberrantes par la construction d'un modèle de classification.	-Ne font aucune hypothèse sur la distribution des données.	-Ne nécessitent pas une connaissance préalable de la distribution des données pour détecter les anomalies.
Points faibles	-Les techniques d'apprentissage paramétriques peuvent être inutiles si les données des capteurs ne suivent pas la répartition prédéfinie.	-Complexité de calcul.	-Défi du choix des paramètres d'entrée appropriés.	-Le choix d'une largeur appropriée pour le cluster.

Tableau 12 Evaluation des différentes approches de détection des anomalies

3. Etat de l'art sur les travaux de recherche concernant la détection de l'attaque de *jamming*

3.1. Avant propos

Comme indiqué dans les chapitres précédents, nous nous intéressons dans cette thèse aux attaques de *jamming* dans les réseaux de capteurs médicaux sans fils. Dans la suite de ce chapitre, nous allons dresser un état de l'art sur les travaux de recherche et les méthodes utilisées pour détecter l'attaque de *jamming* dans les réseaux de capteurs sans fil ainsi de faire une comparaison entre ces méthodes selon plusieurs critères.

Comme nous avons déjà défini l'attaque de *jamming* dans la section 2.2.2, le brouilleur (*jammer*) essaye d'envoyer des signaux radio sur la même fréquence utilisée par le réseau de capteurs afin d'interférer les communications sans fil entre les nœuds émetteurs et les nœuds récepteurs. Ceci peut être réalisé par le brouilleur en attaquant soit la couche physique, soit la couche de liaison et peut se faire par plusieurs méthodes parmi lesquelles nous citons : le

jamming réactive, le *jamming* aléatoire, le *jamming* trompeur et le *jamming* constant (nous définissons ces types de *jamming* dans le Chapitre IV).

Ce brouillage radio va avoir une influence directe sur les valeurs de plusieurs paramètres du réseau, donc l'augmentation ou la diminution des valeurs de ces paramètres sera un indice d'existence d'une attaque de *jamming*. Donc, ces paramètres peuvent être utilisés dans la détection du *jamming*. Parmi ces paramètres nous citons : PDR, PSR, BPR, BER, ECA, CST, RSSI et SNR. Dans la suite, nous donnons la définition de chacun des ces paramètres.

-Packet Delivery Ratio (PDR) : Le PDR est le rapport entre le nombre de paquets délivrés avec succès à un nœud destinataire et le nombre de paquets envoyés par le nœud émetteur.

-Packet Send Ratio (PSR) : Le PSR est le rapport entre le nombre de paquets envoyés avec succès par un nœud et le nombre de paquets qu'il a l'intention d'envoyer.

-Bad Packet Ratio (BPR) : Le BPR est le rapport entre le nombre de paquets erronés reçus par un nœud et le nombre total de paquets reçus par ce nœud sur une période donnée.

-Bit Error Rate (BER) : La BER est calculé comme le rapport entre le nombre de bits corrompus et le nombre total de bits reçus par un nœud lors d'une session de transmission.

-Energy Consumption Amount (ECA) : Le paramètre ECA est défini comme étant la quantité d'énergie approximativement consommée par un nœud pendant une période déterminée.

-Carrier Sensing Time (CST) : Dans les protocoles de la couche MAC (*Medium Access Control*), comme le protocole *Carrier Sense Multiple Access* (CSMA), chaque nœud essaye de détecter le moment où le support est libre pour qu'il puisse ensuite envoyer ses propres paquets. La période pendant laquelle le nœud doit attendre pour que le support (canal) devienne libre est appelé *Carrier Sensing Time* (CST). Cette période est calculée comme étant la durée moyenne du temps écoulé entre l'instant où un nœud est prêt à envoyer son paquet et l'instant où le support se libère pour que le nœud puisse émettre son paquet.

-Received Signal Strength Indicator (RSSI) : Le RSSI est l'indicateur d'intensité de la puissance contenue dans un signal radio reçu au niveau du nœud récepteur.

-Signal-to-Noise Ratio (SNR) : C'est le rapport entre la puissance du signal reçu et la puissance du bruit reçu (puissance de brouillage dans le cas du *jamming*) au niveau d'un nœud.

Dans le Chapitre IV, nous décrivons plus en détail les paramètres que nous allons utiliser dans notre algorithme de détection du *jamming*, ainsi que l'influence de chaque type de *jamming* sur la valeur de chacun de ces paramètres.

3.2. Méthodes proposées pour la détection de l'attaque *Jamming*

Dans cette section, nous allons présenter une sélection des travaux proposés pour la détection du *jamming* et qui sont basés sur les paramètres cités ci-dessus.

3.2.1. Xu et al. [70]

Les auteurs ont effectué une étude intensive sur la détection de l'attaque *jamming* en utilisant trois capteurs : un émetteur, un récepteur et un brouilleur (*jammer*) avec une plate-forme MICA2. Ils ont utilisé un algorithme pour détecter l'existence d'un brouilleur en utilisant les deux paramètres suivants: *Packet Delivery Ratio (PDR)* et *Received Signal Strength Indication (RSSI)* et cela pour distinguer entre les cas normaux et les cas où il y a une attaque *jamming*. Plusieurs scénarios ont été appliqués pour mesurer les valeurs de *PDR* et *RSSI*. Le principe de l'algorithme utilisé fait la distinction entre deux régions, l'une est la région sous *jamming* et l'autre est la région normale.

A chaque mesure de ces deux paramètres au niveau d'un nœud, si la valeur du *PDR* mesurée par ce nœud est inférieure à la valeur d'un seuil *PDRth* et en même temps la valeur du RSSI mesurée est supérieure à la valeur d'un seuil *RSSIth*, donc on constate qu'on est dans la région de *jamming* et alors le nœud est supposé sous attaque de *jamming*. La Figure 14 présente la région sous *jamming* (région hachée) où les valeurs mesurées de *PDR* sont inférieures à un seuil *PDRth* et les valeurs de *RSSI* sont supérieures à un seuil *RSSIth*. Par contre, les points en dehors de cette région sont dans la région normale.

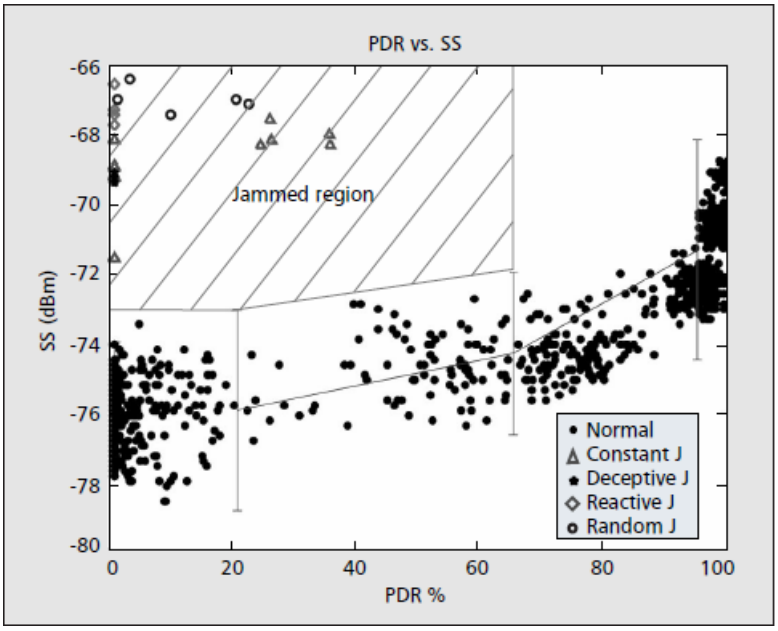


Figure 14 Relation entre PDR et RSSI

Le premier inconvénient de cette méthode est que le système est testé par seulement trois nœuds : un émetteur, un récepteur, et un brouilleur.

Un autre inconvénient est que dans un tel cas, la valeur du *PDR* mesurée au niveau d'un nœud émetteur 'A', peut être faible à cause d'un problème au niveau du nœud récepteur 'B' qui ne répond pas par un paquet d'acquittement ACK vers A, et en même temps le niveau du *RSSI* au niveau de A est élevé. Dans ce cas, cette méthode va considérer que le nœud A est sous une attaque *jamming*, ce qui n'est pas le cas. Donc l'utilisation de ces deux paramètres seuls n'est pas suffisante et alors cette méthode va augmenter le nombre de fausse alarme. Dans le Chapitre IV, nous prouvons cet inconvénient.

3.2.2. Reyes et al. [78]

Les auteurs ont présenté une technique pour détecter la perte de liaison dans les réseaux sans fils. Les auteurs utilisent les quatre paramètres suivants : PDR, BPR et RSSI décrits ci-dessus ainsi qu'un autre paramètre qu'ils appellent CCA (*Clear Channel Assessment*). Le CCA est une variable qui compte le nombre de fois où l'émetteur trouve le canal occupé en essayant d'envoyer un paquet. Ces quatre paramètres sont utilisés pour évaluer l'état de la liaison, et en cas de perte, pour déterminer la cause probable de la perte de la liaison.

Leur méthode consiste à utiliser un système appelé « *Fuzzy Inference System* » qui a comme entrée les valeurs des quatre paramètres mentionnés ci-dessus, et qui seront utilisées

pour calculer la valeur de l'indice de brouillage « *Jamming Index* (JI) ». L'indice de brouillage (JI) est une valeur comprise entre 0% (qui signifie l'absence de *jamming*) et 100% (qui signifie l'existence d'un *jamming* absolu). Ce calcul sera fait par chacun des nœuds du réseau. Donc chaque nœud sera capable de détecter s'il a perdu la liaison et de savoir si cette perte résulte d'une attaque de *jamming* ou non.

Les auteurs présentent une gamme de valeurs pour chacun des quatre paramètres utilisés par le programme afin que ce dernier puisse décider en fonction de ces valeurs de l'état de la liaison et de la cause possible dans le cas où la liaison est considérée perdue. Enfin, ils présentent leurs résultats qui montrent que le système présente une bonne efficacité.

L'inconvénient de cette méthode est qu'elle nécessite un calcul compliqué au niveau des nœuds, ce qui est coûtant en terme d'énergie. En plus, cette méthode nécessite une capacité de calcul élevée, ce qui n'est pas le cas dans les nœuds capteurs qui présentent des contraintes à ce niveau.

En outre, cette méthode nécessite une configuration préalable de certain nombre de variables relatives à chacun des paramètres utilisés. Pour fixer les valeurs de ces variables, il faut d'abord utiliser des valeurs qui semblent logiques puis les corriger en comparant les résultats obtenus de l'indice de brouillage avec les résultats attendus et cela en faisant plusieurs tests jusqu'à trouver les valeurs optimales de ces variables.

3.2.3. Misra et al. [77]

Les auteurs ont défini plusieurs types de *jamming* et plusieurs paramètres réseau. Puis, ils ont choisi quatre types de *jamming* qui sont : *constant, reactive, deceptive et random jamming* avec deux intensités de puissance différentes.

Ensuite, ils ont présenté leur méthode qui est la même méthode utilisée par Reyes et al. (*Fuzzy Inference System)* mais en utilisant des paramètres différents. Ils ont choisi d'utiliser le SNR qui est le rapport signal/bruit et le BPR où ils ont appelé *Packets Dropped per Terminal (PDPT*) qui est la valeur moyenne du nombre des paquets rejetés par un nœud durant un cycle de simulation.

Les nœuds du réseau mesurent le niveau du RSSI reçu ainsi que le nombre total de paquets reçus et le nombre de paquets reçus avec succès. Les nœuds envoient ces valeurs à la station de base qui effectue le calcul du rapport SNR et du PDPT et ensuite les utilise pour calculer

l'indice de *jamming* (JI) pour chaque nœud. Donc la station de base sera capable de savoir quel nœud parmi les nœuds du réseau est sous l'influence d'une attaque de *jamming*.

Plusieurs simulations sont réalisées en utilisant tous les types de *jamming* cités ci-dessus. Les auteurs ont utilisés plusieurs nœuds et un *jammer* et ils ont calculés l'indice JI pour chacun des nœuds du réseau. Si la valeur de JI est élevée donc le nœud correspondant est considéré sous attaque *jamming*. Par contre, si la valeur de JI est faible, le nœud correspondant est considéré qu'il n'est pas sous l'influence de *jamming*.

Enfin, les auteurs ont évalué leur méthode en termes de taux de détection et de taux de fausses détections. Leur méthode a prouvé qu'elle peut avoir un taux de détection élevé et un taux de fausses détections faible.

Par rapport à la méthode de Reyes et al., cette méthode a pu résoudre le problème de calcul compliqué au niveau des nœuds car tout le calcul est fait au niveau de la station de base.

3.2.4. Cakiroglu et al. [73]

Les auteurs ont proposé un algorithme pour la détection du *jamming* qui est basé sur les valeurs des seuils pour trois paramètres qui sont : *PDR, BPR et ECA.*

Au début, les auteurs ont défini plusieurs types de l'attaque *jamming*. Ensuite, ils ont réalisé plusieurs tests de simulation sur le réseau en mesurant, à chaque période de 60 secondes, les valeurs de PDR, BPR, et ECA au niveau d'un nœud de ce réseau. Ces mesures ont été effectuées dans les conditions normales (sans *jamming)* et sous les différents types de *jamming* qu'ils ont déjà définis. Ensuite, ils ont présenté les valeurs maximale, minimale et moyenne de chacun de ces paramètres.

D'après les résultats obtenus, ils ont calculés les seuils pour chacun des trois paramètres, et ils ont présenté les conditions où on peut considérer que le nœud est sous l'influence d'une attaque de *jamming*. En effet, si la valeur du *PDR* est plus grande que la valeur de son seuil ou si les valeurs des trois paramètres *(PDR, BPR et ECA)* sont plus petites que les valeurs de leurs seuils, alors il n'y a pas de *jamming* ; Dans le cas contraire, le nœud sera considéré sous l'influence d'un type de *jamming.*

Enfin, les auteurs ont appliqué leur méthode et ont évalué les performances de leur algorithme en termes de taux de détection et de taux de fausses alarmes. Les résultats prouvent que la méthode est efficace car elle a présenté un taux de détection élevé et un taux faible de fausses détections.

Par contre, cette méthode présente un inconvénient. En effet, dans un scénario où le niveau du *PDR* est inférieur à son seuil, le niveau de *BPR* est supérieur à son seuil et la valeur de l'*ECA* est inférieure à son seuil, cette méthode considère que la cause de ces valeurs est toujours due à une attaque de *jamming*. Mais en réalité, ces valeurs peuvent être le résultat d'un niveau faible de la puissance reçue au niveau de ce nœud. Dans le Chapitre IV, nous allons prouver que l'utilisation d'un paramètre supplémentaire (qui est le RSSI dans notre proposition) en plus des trois paramètres utilisés dans cette méthode va diminuer le taux de fausses détections et va donner une efficacité plus élevée dans la détection de l'attaque *jamming*.

3.2.5. Fragkiadakis et al. [82]

Les auteurs ont proposé une méthode pour la détection des attaques sur la couche physique et parmi ces attaques le *jamming*. La méthode est basée sur la détection des changements survenus sur le niveau du rapport signal sur bruit (SNR). Ils ont proposé deux algorithmes de détection, le premier est un algorithme avec un simple seuil et le deuxième s'appelle *Cumulative Sum (Cusum) algorithm*. Ils ont réalisé plusieurs expérimentations en utilisant deux types de *jamming*, l'un avec une intensité élevée et l'autre avec une intensité faible. Puis ils ont évalué les résultats de détection des deux algorithmes en termes de taux de détection et de taux de fausses alarmes. Ils ont trouvé qu'avec les deux types de *jamming* (intensité élevée et intensité faible), l'algorithme *Cusum* présente des performances plus élevées que l'algorithme avec un simple seuil et cela par un taux de détection plus élevé et un taux faible de fausses alarmes.

L'algorithme *Cusum* est très performant, mais le point faible de cette méthode est qu'elle est basée seulement sur un paramètre qui le niveau du SNR, ce qui n'est pas suffisant car on peut avoir des cas où le niveau SNR est faible mais pas à cause d'une attaque de *jamming*. En plus, cette méthode n'est pas capable d'identifier le type de *jammer* dans le cas où elle détecte une attaque de *jamming*.

3.2.6. Hamieh et al. [80]

Les auteurs ont proposé une méthode pour détecter le *jamming* dans les réseaux Ad-Hoc sans fil. Dans ce travail, les auteurs supposent que le brouilleur (*jammer*) transmet ses signaux quand il détecte une activité sur le réseau, ce qui est le cas d'une attaque *jamming* réactive. Pour distinguer ente les cas normaux et les cas de *jamming*, ils ont proposé de mesurer la

dépendance entre les périodes d'erreur (*periods of error*) et les temps de réceptions correctes (*correct reception times*) car l'accès au canal par le brouilleur est dépendant de l'accès au canal des nœuds actifs.

Afin de mesurer cette dépendance, les auteurs ont utilisé le coefficient de corrélation qui est une mesure statistique de la relation entre deux variables aléatoires.

Ils ont présenté les résultats de simulation obtenus de la valeur moyenne du Coefficient de Corrélation (CC) pour tous les nœuds constituant le réseau. Les résultats montrent que la valeur du CC calculé entre *« correct reception times»* et *« periods of error »* en cas de *jamming* est plus grande que celle dans le cas normal.

L'idée de cette méthode est bonne, mais les auteurs ne précisent pas comment on peut détecter le *jamming* c.à.d. quelle est la valeur seuil du CC qui nous permet de distinguer entre le cas d'une attaque *jamming* et le cas normal.

En plus, cette méthode ne prend en compte qu'un seul type de *jamming* qui est le *jamming* réactif. Donc elle n'est pas capable à détecter les autres types de *jamming.*

3.3. Critères de comparaison

Dans ce paragraphe, nous faisons une comparaison entre les méthodes présentées ci-dessus en prenant en compte les critères suivants :

-Les paramètres mesurés et utilisés par chaque méthode.

-Si la détection de *jamming* se fait par chacun des nœuds constituant le réseau ou bien par la station de base.

-La nécessité d'utiliser des seuils par l'algorithme de détection.

-La complexité de calcul dans l'algorithme.

-L'obligation des nœuds à communiquer avec la station de base pour signaler la détection d'une attaque de *jamming*.

-L'efficacité de détection pour chacune des méthodes.

-La capacité des méthodes à identifier le type de *jamming*.

Le Tableau 13 résume cette comparaison.

Critères de comparaison	Xu et al.	Reyes et al.	Misra et al.	Fragkiadakis et al.	Cakiroglu et al.
Paramètres mesurés	PDR et RSSI	PDR, BPR, RSSI et CCA	SNR et PDPT	SNR	PDR, BPR et ECA
Détection de l'attaque effectuée par :	Nœud individuel	Nœud individuel	Station de base	Nœud individuel	Nœud individuel
Utilisation des seuils	Oui	Non	Non	Oui	Oui
Complexité de calcul (1:plus simple, 4: plus complexe)	1	4	3	3	2
Efficacité de détection (++: plus efficace, +: moins efficace)	+	++	++	+	++
Obligation de communiquer avec la station de base	Oui	Oui	Non	Oui	Oui
Capabilité à identifier le type de jamming	Non	Non	Oui	Non	Non

Tableau 13 Comparaison entre les travaux de recherche concernant la détection du jamming

Tous ces travaux de recherche étaient faits dans le cadre de détection de l'attaque de *jamming* dans les réseaux sans fil ou les réseaux de capteurs sans fil (WSN). Dans le Chapitre IV, nous allons présenter notre méthode de détection de *jamming* dans le contexte d'un réseau de capteurs médicaux sans fil (WBAN).

3.4. Les mesures défense contre les attaques de *jamming*

Il existe plusieurs techniques de défense contre le *jamming*. Dans cette section, nous présentons quelques solutions parmi les solutions proposées pour minimiser le *jamming* dans les réseaux sans fil [69].

3.4.1. Réglementation de la puissance transmise

L'utilisation de faible puissance d'émission par un nœud diminue la probabilité de découverte par un attaquant (un attaquant doit d'abord localiser la cible avant de transmettre le signal de brouillage).

En même temps, l'augmentation de la puissance transmise implique une plus grande résistance contre le brouillage, car dans ce cas, un signal de brouillage fort est nécessaire pour surmonter le signal utile.

Pour cela, un pourcentage considérable de nœuds de capteurs actuellement utilisés dans les réseaux de capteurs possède la capacité de changer la puissance transmise de leur émetteur.

3.4.2. Etalement de spectre par saut de fréquence (FHSS)

L'étalement de spectre par saut de fréquence ou « *Frequency Hopping Spread Spectrum* (FHSS) » en anglais est une méthode de transmission des signaux par ondes radio qui utilise plusieurs canaux (sous-porteuses) répartis dans une bande de fréquence selon une séquence pseudo-aléatoire connue de l'émetteur et du récepteur. La méthode FHSS offre plusieurs avantages :

-Elle minimise l'interception non autorisée et le brouillage contre les transmissions radio entre les nœuds.

-Elle traite efficacement l'effet des chemins multiples (*multi-path*).

-Plusieurs réseaux de capteurs peuvent coexister dans le même espace sans causer des problèmes d'interférence.

Mais l'un des principaux inconvénients de saut de fréquence est celui de la bande passante totale nécessaire qui est beaucoup plus large que celle requise pour transmettre les mêmes données à l'aide d'une seule fréquence porteuse. En effet, la transmission sur chaque fréquence dure une période très limitée, de sorte que la fréquence n'est pas occupée pour des longues durées d'où une faible utilisation de chaque porteuse.

3.4.3. Etalement de spectre à séquence directe (DSSS)

L'étalement de spectre à séquence directe ou « *Direct Sequence Spread Spectrum (DSSS)* » est une technique d'étalement de spectre utilisée dans les réseaux sans fil. Cette technologie consiste à transmettre pour chaque bit de donnée une séquence appelée bruit pseudo-aléatoire. Ainsi chaque bit valant '1' est remplacé par une séquence de bits et chaque

bit valant 0 par son complément. Grâce à cette technique, de l'information redondante est transmise ce qui permet d'effectuer des contrôles d'erreurs voire de la correction d'erreurs.

3.4.4. FHSS/DSSS hybride

L'utilisation hybride entre FHSS et DSSS augmente la résistance au brouillage et interférence et minimise l'interception non autorisée.

3.4.5. Technologie Ultra large bande

Ultra large bande (UWB) est une technique de modulation radio basée sur la transmission simultanée d'impulsions de très courtes durées sur un large spectre d'une bande de fréquence. L'utilisation de cette technologie dans les réseaux de capteurs rend le signal transmis par les nœuds très difficile à intercepter ou à brouiller et également résistant aux effets de trajets multiples.

4. Nos contributions

Dans les deux chapitres suivants, nous allons focaliser nos contributions sur la détection de deux types d'attaques dans un système WBAN de surveillance médicale à distance représenté dans la Figure 15. La première attaque concerne le brouillage radio *(jamming)* qui vise les communications sans fil inter-BAN et intra-BAN du système WBAN. La deuxième attaque concerne le *flooding* qui vise les communications au-delà du BAN (Internet dans notre cas).

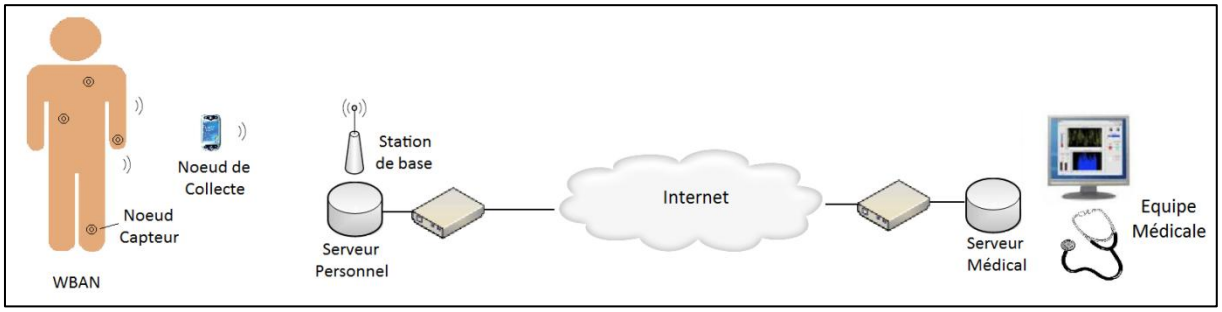


Figure 15 Système WBAN de surveillance médicale à distance

5. Conclusion

Dans ce chapitre, nous avons établi un état de l'art sur les attaques et les anomalies possibles dans les systèmes WBAN ainsi que sur les travaux de recherche concernant la détection de l'attaque de brouillage radio (*jamming*).

Nous avons commencé ce chapitre par une introduction sur les vulnérabilités dans les réseaux WBAN. Nous avons alors parlé de la nécessité des systèmes de sécurité et de détection des attaques dans ces réseaux en citant les différentes contraintes de sécurité dans les réseaux de capteurs sans fil.

Puis nous avons classifié les types des attaquants selon trois critères. Nous avons aussi décrit les différents types d'attaques possibles dans un système WBAN de surveillance médicale à distance et nous les avons classifiées selon plusieurs critères.

Après, nous avons décrit les anomalies possibles dans les réseaux de capteurs sans fils d'un système WBAN, en les classifiant en trois classes : anomalies de réseaux, anomalies des nœuds et anomalies des données. Puis nous avons parlé brièvement des techniques de détection des anomalies dans les RCSF.

Ensuite, nous avons fait un état de l'art sur les travaux de recherche concernant la détection de l'attaque *jamming* dans les réseaux sans fils. Nous avons fait une comparaison entre ces méthodes selon plusieurs critères. Enfin, nous avons présenté quelques solutions proposées pour défendre contre ce type d'attaque dans les réseaux sans fil.

Dans le chapitre suivant, nous présentons notre méthode de détection de *jamming* dans les réseaux de capteurs sans fil d'un système WBAN.

Chapitre IV : Détection des attaques de *jamming* dans les réseaux WBAN

1. Introduction

Dans un système WBAN de surveillance médicale à distance, un réseau de capteurs corporels sans fil est déployé sur le corps du patient afin de mesurer des informations physiologiques et les envoyer à un nœud de collecte via un médium de transmission de données sans fil. Ce nœud de collecte à son tour envoie ces informations à une station de base comme le montre la Figure 16. Ces données envoyées sont vulnérables à plusieurs genres d'attaques et/ou d'anomalies.

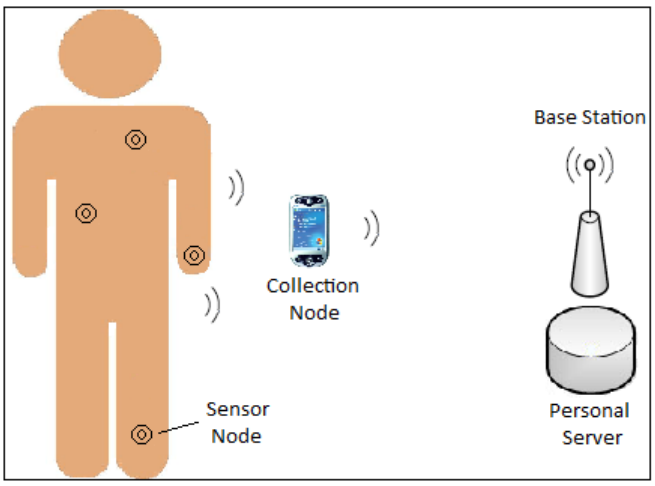


Figure 16 Communication des données physiologiques dans un système WBAN

Ces attaques et anomalies peuvent intercepter, modifier ou brouiller les données physiologiques envoyées par les capteurs vers le nœud de collecte, ce qui peut empêcher l'équipe médicale de recevoir les données physiologiques qui décrivent l'état réel du patient. Par conséquence, ces attaques et anomalies sont très dangereuses pour la santé des patients parce qu'elles peuvent agir d'une façon négative sur la qualité des soins.

Donc la détection de ces attaques et anomalies constitue un grand défi. Cette détection est indispensable pour sécuriser les communications entre les capteurs et le nœud de collecte et pour assurer la fiabilité des données médicales communiquées par les capteurs.

Ce chapitre traite l'attaque par brouillage radio (*Jamming*) dans les réseaux sans fils et présente les différents types de brouilleurs ainsi qu'il décrit les critères utilisés pour la détection de ce type d'attaque. A la fin de ce chapitre, nous présentons notre contribution sur la détection des différents types de *jamming* dans un réseau de capteurs médicaux sans fil.

2. Les attaques de brouillage radio (*Jamming attacks*)

Le *Jamming* ou brouillage radio est une sorte d'attaque de déni de service dans les communications sans fil, qui perturbe le fonctionnement des couches physique ou des couches de liaison dans les nœuds légitimes en envoyant des signaux illégitimes.

Le brouillage radio est une technique de transmission d'un signal radio visant à interrompre, souvent volontairement, des communications en diminuant le rapport signal sur bruit. Des brouillages non-intentionnels peuvent survenir lorsqu'un opérateur transmet des ondes sur une fréquence occupée, sans avoir vérifié préalablement l'utilisation de la fréquence, ou en n'ayant pas réussi à entendre de station sur cette fréquence. Ce concept peut être utilisé dans les réseaux sans fil pour empêcher l'information de passer.

Il existe plusieurs modèles de l'attaque *jamming* que nous avons étudiés. Les auteurs dans [34], [70], [71], [72], [73], [74] ont défini plusieurs modèles de l'attaquant brouilleur tel que le brouilleur constant, le brouilleur trompeur, le brouilleur aléatoire et le brouilleur réactif. La Figure 17 et le Tableau 14 présentent ces différents types de brouilleurs. Dans la suite nous définissons ces brouilleurs et leurs effets sur la communication entre les nœuds du réseau de capteurs sans fil.

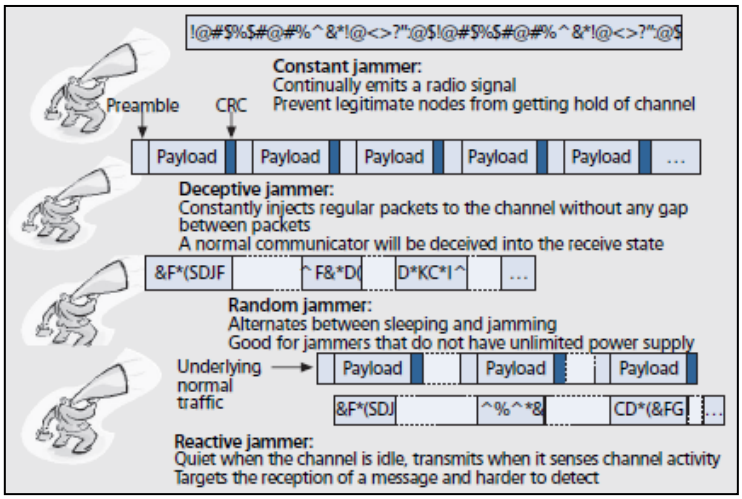


Figure 17 Différents types de brouilleurs [34]

Type de brouilleur	Stratégie
Brouilleur constant	émet en permanence un signal radio sur le canal.
Brouilleur trompeur	injecte en permanence des paquets sur le canal.
Brouilleur aléatoire	attaque le réseau à des intervalles de temps aléatoires, et dort dans le reste du temps.
Brouilleur réactif	écoute le réseau, et déclenche l'attaque lorsqu'une communication est initiée dans le réseau.

Tableau 14 Les stratégies des différents types de brouilleurs

2.1. Brouilleur constant (*Constant jammer*)

Dans le cas d'un brouilleur constant, le brouilleur émet en permanence un signal radio sur le canal de communication sans attendre que le canal se libère. Le signal émis peut être constitué d'une séquence aléatoire de bits [34], [73], [74].

Le but de ce type de brouilleur est de créer des interférences sur les nœuds émetteurs afin de corrompre leurs paquets au niveau du récepteur, ainsi que d'occuper le canal, ce qui empêche les nœuds émetteurs d'avoir accès au canal. Donc la communication entre les nœuds du réseau sera suspendue. Cependant, ce type d'attaquants n'est pas éco-énergétique, donc il n'est pas le bon choix pour les applications à puissance limitée.

2.2. Brouilleur trompeur (*Deceptive jammer*)

Dans le cas d'un brouilleur trompeur, le brouilleur injecte en permanence des paquets légitimes sur le canal avec des taux élevés et sans espaces entre les transmissions [34], [70], [73], [74]. De cette manière, les nœuds restent en mode de réception en permanence même s'ils ont des données à transmettre. Donc, le moyen de communication reste indisponible tout le temps.

L'inconvénient pour ce type de brouilleur est son efficacité énergétique car l'émission des signaux en permanence sur le support sans fil limite leur capacité d'être autonome et ne pas dépendre d'une source d'alimentation externe.

2.3. Brouilleur aléatoire (*Random jammer*)

Le brouilleur aléatoire attaque le réseau à des intervalles de temps aléatoires (ce qu'on appelle période d'attaque), et dort dans le reste du temps (période de *sleep*) [34], [70], [73], [74]. Le brouilleur aléatoire imite le brouilleur constant ou trompeur, mais il est plus économe en énergie par rapport à eux.

2.4. Brouilleur réactif (*Reactive jammer*)

Le brouilleur réactif écoute toujours le réseau, et déclenche l'attaque lorsqu'une communication est initiée dans le réseau. Lorsqu'il détecte une transmission de paquets, il transmet immédiatement un signal radio afin de provoquer une collision au niveau du récepteur. Par conséquence, les paquets légitimes envoyés par les nœuds de capteurs sont endommagés. Ce type d'attaque est aussi appelé *jamming* intélligent [34], [70], [73], [74]. Les brouilleurs réactifs écoutent le réseau d'une façon permanente, donc ils ne sont pas économes en termes d'énergie.

3. Critères de détection des attaques *jamming*

Les attaques de brouillage (*jamming attacks*) peuvent entraîner des conditions anormales, en empêchant, interceptant ou bloquant la communication dans le réseau de capteurs médicaux.

Un nombre de paramètres réseau suggère qu'il pourrait y avoir une attaque *jamming* contre le réseau menée par un brouilleur. Des valeurs anormales de ces paramètres peuvent être considérées comme une alerte d'attaque *jamming*, comme par exemple l'augmentation du taux de collision, l'augmentation du taux de paquets erronés (BPR : Bad Packet Ratio) ou bien la diminution du taux des paquets reçues (PDR : Packet Delivery Ratio).

Mais ces valeurs anormales peuvent aussi être la conséquence des conditions naturelles du réseau. Par exemple, les défauts matériels ou logiciels dans les nœuds de capteurs ou les changements dans l'environnement peuvent également déclencher des conditions similaires aux scénarios causés par les brouilleurs [73].

Dans cette section, nous décrivons les paramètres réseau que nous allons utiliser ultérieurement dans notre algorithme afin de détecter les attaques de brouillage radio et identifier le type de brouilleur.

3.1. Taux de paquets reçues ou *Packet Delivery Ratio* (PDR)

Le PDR est le rapport entre le nombre des paquets qui sont délivrés avec succès à une destination sur le nombre de paquets qui ont été envoyés par l'expéditeur [34], [70], [73], [77], [78], [81].

$$PDR = \frac{Nombre\ de\ paquets\ délivrés}{Nombre\ de\ paquets\ envoyés}$$

Un nœud émetteur confirme la délivrance d'un paquet uniquement lorsqu'elle reçoit un paquet d'acquittement ACK de la part du nœud récepteur. Si le mécanisme (RTS / CTS / DATA / ACK) est utilisé, le PDR peut être calculé en comparant le nombre des paquets envoyés (RTS et DATA) au nombre des paquets reçus (CTS et ACK). Cette méthode peut être appliquée à l'émetteur.

Une autre mesure consiste à calculer le rapport entre le nombre de trames reçues correctement par le récepteur sur le nombre de trames qui ont été envoyées dans le canal. Cette méthode peut être appliquée au niveau du récepteur.

La valeur du paramètre PDR ne diminue pas seulement à cause d'un brouillage, mais également à cause des connexions imparfaites, des défauts dans les nœuds voisins et des collisions. Par conséquence, le PDR ne peut pas être utilisé seul pour identifier si le réseau est sous une attaque de *jamming* ou pas.

3.1.1. L'influence des différents types des brouilleurs sur la valeur du PDR

Les brouilleurs réactif et constant altèrent la plupart des paquets de control ou de données dans le réseau. Donc la valeur du PDR est trop faible lors d'une attaque de type *jamming* réactif ou constant. D'autre part, le brouilleur trompeur occupe le canal de communication tout le temps, ce qui empêche les nœuds capteurs d'envoyer leurs paquets. Par conséquence, la valeur du PDR ne peut pas être supérieure à zéro. Par contre, le brouilleur aléatoire attaque le réseau à des intervalles de temps aléatoires et peut endommager une partie des paquets de données ou de contrôle, ce qui mène à une valeur faible du PDR qui dépend des durées d'attaque du brouilleur [70], [73]. Le Tableau 15 résume le niveau du PDR en fonction des différents types des brouilleurs :

Brouilleur	Constant	Réactif	Aléatoire	Trompeur
PDR	Trop faible	Trop faible	Faible	0%

Tableau 15 PDR avec différents types des brouilleurs

3.2. Taux de paquets erronés ou *Bad Packet Ratio* (BPR)

Le BPR est le rapport entre le nombre de paquets erronés reçus par un nœud et le nombre total des paquets reçus par ce nœud sur une période donnée.

$$BPR = \frac{Nombre\ de\ paquets\ erronés\ reçus}{Nombre\ total\ de\ paquets\ reçus}$$

Les nœuds déterminent la qualité des paquets en utilisant le test CRC (*Cyclic Redundancy Check*) et les rejettent si le résultat du test est négatif. La mesure du BPR se fait au niveau du nœud récepteur [73], [77].

Les paramètres PDR et BPR démontrent la qualité de la communication pour l'émetteur et le récepteur respectivement. Ces deux paramètres sont inversement proportionnels dans la plupart des cas mais peuvent avoir en même temps des valeurs faibles dans des cas particuliers.

3.2.1. L'influence des différents types des brouilleurs sur la valeur du BPR

La valeur du BPR est très élevée dans les cas d'un *jamming* constant ou réactif. Or dans le cas d'un *jamming* trompeur, les nœuds ne peuvent ni envoyer ni recevoir des paquets car le canal de communication est occupé en permanence par le brouilleur, ce qui mène à une valeur

nulle du BPR. Dans le cas d'un *jamming* aléatoire, la valeur du BPR dépend des durées d'attaque du brouilleur [73]. Le Tableau 16 résume le niveau du BPR en fonction des différents types des brouilleurs.

Brouilleur	Constant	Réactif	Aléatoire	Trompeur
BPR	Très élevé	Très élevé	Elevé	0%

Tableau 16 BPR avec différents types des brouilleurs

3.3. Quantité d'énergie consommée ou *Energy Consumption Amount* (ECA)

Le paramètre ECA est défini comme étant la quantité d'énergie approximativement consommée par un nœud pendant une période déterminée. Ce paramètre peut être l'un des paramètres utilisés pour détecter une attaque *jamming* [73], [77].

Chaque nœud capteur consomme un courant de 'I' mA. La valeur de 'I' dépend de l'état du nœud, c.à.d. s'il est en mode de transmission, réception ou en mode de veille. Cela signifie qu'avec une batterie de 'U' volt, le module radio du nœud dissipe une puissance : P = (I x U) mW.

La valeur de la quantité d'énergie consommée par un nœud pendant une période « Te » est calculée selon l'équation suivante :

$$ECA = Tt \times Pt + Tr \times Pr + Ts \times Ps$$

Où Tt est le temps durant lequel le nœud de collecte est en mode de transmission, Tr est le temps durant lequel le nœud de collecte est en mode de réception et Ts est le temps durant lequel le nœud de collecte est en mode de veille.

Pt est la puissance dissipée par le nœud pendant la période de transmission, Pr est la puissance dissipée par le nœud pendant la période de réception et Ps est la puissance dissipée par le nœud pendant le mode de veille.

3.3.1. L'influence des différents types des brouilleurs sur le niveau de l'ECA

Dans le cas d'un *jamming* aléatoire, trompeur ou constant, le brouilleur oblige les nœuds capteurs à consommer plus d'énergie. En fait, pendant la période de *jamming*, le brouilleur trompeur oblige les nœuds à rester en mode de réception, tandis que le brouilleur constant les

oblige à rester en mode d'écoute, ce qui obligent les nœuds capteurs à consommer plus d'énergie que dans le cas normal (où ils peuvent passer en mode de veille tant qu'ils ne sont pas ni en mode de transmission ni en mode de réception).

Donc les nœuds capteurs consomment plus d'énergie si le réseau est sous une attaque de *jamming* (constant, trompeur ou aléatoire) et par conséquence, le niveau de l'ECA sera trop élevé [73]. Dans le cas d'un *jamming* réactif, la consommation d'énergie par le nœud reste normale. Le Tableau 17 résume le niveau du BPR avec différents types des brouilleurs.

Brouilleur	Constant	Réactif	Aléatoire	Trompeur
ECA	Très élevé	Normal	élevé	Très élevé

Tableau 17 ECA avec différents types des brouilleurs

3.4. Taux de paquets envoyés ou *Packet Send Ratio* (PSR)

Le PSR est le rapport entre le nombre de paquets qui sont envoyés avec succès par un nœud et le nombre de paquets qu'il a l'intention d'envoyer [34], [70], [73], [77], [78], [80] [81]. Par exemple, si un nœud veut envoyer « n » paquets, mais seulement « m » paquets d'entre eux ont été envoyé (avec m < n), alors :

$$PSR = \frac{m}{n} = \frac{Nombre\ de\ paquets\ envoyés\ avec\ succès}{Nombre\ de\ paquets\ destinés\ à\ être\ envoyés}$$

Le nombre de paquets censés être transmis par un nœud au cours d'une période de temps donnée est le résultat de multiplication de la durée de disponibilité du canal vers ce nœud pendant la période donnée par la vitesse de transmission des paquets.

Le PSR peut être mesuré par un dispositif sans fil en traçant le nombre de paquets qu'un nœud a l'intention d'envoyer et le nombre de paquets qui sont envoyés avec succès.

Les signaux de brouillage peuvent rendre le support de communication occupé et les files d'attente du nœud émetteur vont se remplir rapidement. Donc les paquets arrivant à une file d'attente pleine seront abandonnés.

3.4.1. L'influence des différents types des brouilleurs sur la valeur du PSR

Dans le cas d'un brouilleur trompeur, le PSR est égal à zéro parce que les nœuds sont toujours en mode de réception et ils n'envoient aucun paquet. Par contre, dans le cas d'un brouilleur réactif, la valeur de PSR est très élevée car le brouilleur attend les nœuds pour

qu'ils envoient leurs paquets puis il attaque le réseau. Dans le cas d'un brouilleur constant, le niveau du PSR est trop faible. Finalement, dans le cas d'un brouilleur aléatoire, le taux du PSR dépend des durées d'attaque du brouilleur [70], [73]. Le Tableau 18 résume le niveau du PSR selon les différents types de brouilleurs.

Brouilleur	Constant	Réactif	Aléatoire	Trompeur
PSR	Trop faible	Très élevé	Faible	0%

Tableau 18 PSR avec différents types des brouilleurs

3.5. Indicateur de puissance du signal reçu ou *Received Signal Strength Indicator* (RSSI)

Le RSSI est l'indicateur d'intensité de la puissance d'un signal radio reçu au niveau du nœud récepteur. Le RSSI n'est pas en soi une métrique logique pour indiquer qu'il y a de brouillage, mais lorsqu'il est utilisé en combinaison avec d'autres indicateurs tels que le PDR, ils forment une combinaison efficace pour détecter le brouillage [34], [70], [77].

Dans un scénario normal, où il n'y a pas d'interférence, une intensité de signal élevée correspond à un niveau élevé du PDR, et une intensité de signal faible correspond à un niveau faible du PDR. Par contre, un faible niveau du PDR n'implique pas nécessairement que l'intensité du signal est faible. Donc c'est la relation entre les deux paramètres qui va permettre de faire la différence entre le cas d'une attaque de *jamming* et le cas des autres scénarios. Le Tableau 19 résume la relation entre le PDR et le RSSI.

PDR	RSSI	Scénario
PDR=0	intensité du signal faible	échec du nœud voisin
PDR=0	intensité du signal élevée	nœud sous attaque *jamming*
Niveau PDR faible	intensité du signal faible	nœud voisin lointain
Niveau PDR faible	intensité du signal élevée	nœud sous attaque *jamming*

Tableau 19 Relation entre PDR et RSSI

3.5.1. L'influence des différents types de brouilleurs sur le niveau du RSSI

Le niveau du RSSI subit une augmentation durant l'attaque de *jamming* et cela quel que soit le type du brouilleur. Le Tableau 20 résume le niveau du PSR selon les différents types de brouilleurs.

Brouilleur	Constant	Réactif	Aléatoire	Trompeur
RSSI	Très élevé	Très élevé	Très élevé	Très élevé

Tableau 20 Niveau du RSSI avec différents types des brouilleurs

4. Notre proposition pour la détection du *jamming* dans les réseaux WBAN

Pour se défendre contre les attaques de brouillage dans un réseau de capteurs médicaux sans fils, la première étape consiste à détecter l'existence du brouillage radio. Ensuite, il faut différencier entre le *jamming* et les autres facteurs qui peuvent également entraîner l'apparition des symptômes semblables au *jamming*, comme par exemple les défauts matériels ou logiciels dans les nœuds de capteurs ou la faible énergie de la batterie.

Dans cette section, nous présentons notre proposition pour la détection du *jamming* dans un réseau de capteurs médicaux sans fils.

La Figure 18 représente le système étudié. Nous avons un certain nombre de nœuds de capteurs médicaux déployés sur le corps d'un patient. Le rôle de ces capteurs est de mesurer les valeurs d'un certain nombre de paramètres physiologiques, et d'envoyer les données à un nœud de collecte via un médium de transmission de données sans fil. Ce nœud de collecte qui présente des capacités de calcul et d'énergie plus importantes par rapport aux autres nœuds capteurs envoie à son tour ces informations à une station de base.

Nous appliquons les quatre types de l'attaque *jamming* cités ci-dessus sur ce réseau de capteurs sans fils. Nous utilisons alors notre algorithme basé sur les valeurs des paramètres réseau afin de détecter l'attaque de *jamming* et d'identifier le type de brouilleur.

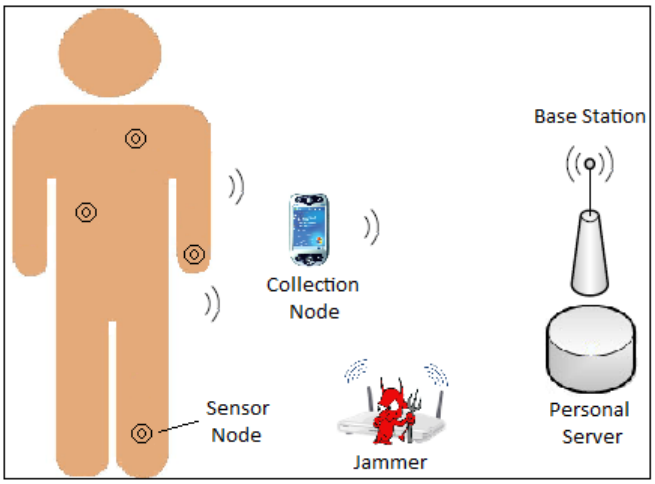


Figure 18 Un système WBAN sous l'influence d'une attaque de *jamming*

4.1. Approche proposée

Pendant chaque période de temps prédéfinie « Tc », les capteurs médicaux mesurent les valeurs d'un certain nombre de paramètres physiologiques. Ils communiquent par la suite ces valeurs à un nœud de collecte via un médium de communication sans fils. Ce nœud de collecte par son tour envoie les données collectées à une station de base reliée à un serveur personnel. Cela veut dire qu'à chaque « Tc », chacun des capteurs médicaux envoie un paquet, contenant la valeur du paramètre physiologique qu'il a mesuré, au nœud de collecte qui par son tour envoie un paquet contenant ces informations à une station de base qui enregistre les données dans un serveur personnel. Ces données seront ensuite transférées à l'équipe médicale via le réseau internet.

A chaque intervalle de temps « Te », le nœud de collecte effectue une mesure des valeurs des paramètres réseau (PDR, BPR, ECA, RSSI et PSR). Donc à chaque « Te », nous avons une valeur pour chacun de ces paramètres réseau. Nous avons choisi le nœud de collecte pour faire ces mesures parce qu'il présente des capacités de calcul et d'énergie plus importantes par rapport aux autres nœuds capteurs.

Notre algorithme consiste à comparer à chaque intervalle de temps « Te », la valeur de chacun des paramètres : PDR, BPR, ECA et RSSI, avec un seuil relatif à chacun d'eux. La comparaison entre la valeur de chaque paramètre et son seuil à chaque intervalle « Te » va identifier s'il existe une attaque de brouillage ou pas.

Dans le cas de la présence d'une attaque de brouillage, la comparaison de la valeur du PSR avec des seuils prédéfinis va identifier le type de brouilleur.

4.2. Calcule des seuils

Nous utilisons une méthode statistique pour déterminer les conditions normales et anormales du réseau. Cette méthode comprend une approche simple dans laquelle une limite inférieure (LCL : Lower Control Limit) et une limite supérieure (UCL: Upper Control Limit) peuvent être calculées à l'aide de la valeur moyenne et de l'écart type de la distribution normale. Dans la Figure 19, μ représente la valeur moyenne et $\boldsymbol{\sigma}$ l'écart type**.** Dans la distribution normale, les données se trouvent entre LCL et UCL. Les valeurs en dehors de l'intervalle [LCL, UCL] sont désignées comme des valeurs anormales.

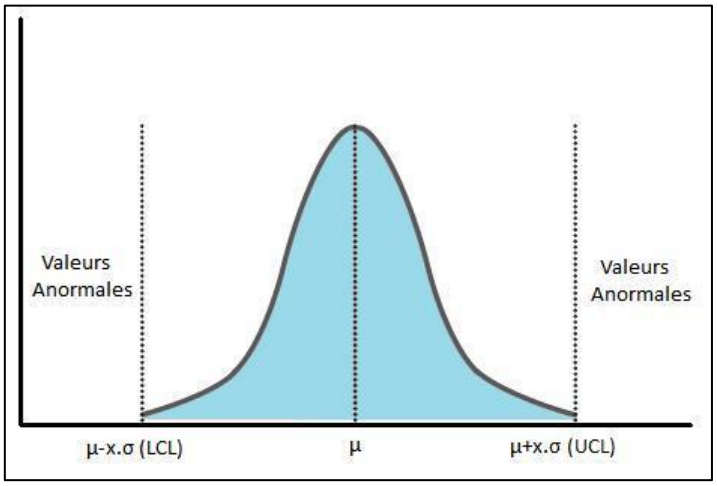


Figure 19 Calcule des seuils pour les paramètres

Après une période d'initialisation qui dure une période $Tinit$ où nous supposons durant laquelle que le réseau est dans une condition normale (pas de *jamming*), les valeurs de $\boldsymbol{\sigma}$ et de la valeur moyenne $\boldsymbol{P}\mu$ de chacun des paramètres sont calculées à partir de $\boldsymbol{n}$ valeurs mesurées.

Ensuite, les valeurs des seuils sont calculées à partir de l'équation suivante :

$$\boldsymbol{Pth} = \boldsymbol{P}\mu \pm \boldsymbol{x}.\boldsymbol{\sigma}$$

Avec :

$$\boldsymbol{P}\mu = \frac{\sum_{k=1}^{n} \boldsymbol{P_k}}{\boldsymbol{n}}$$

Où $\boldsymbol{Pth}$ est la valeur du seuil pour chaque paramètre $\boldsymbol{P}$ et $\boldsymbol{P}\mu$ est la valeur moyenne de $\boldsymbol{n}$ valeurs du paramètre $\boldsymbol{P}$ mesurées pendant la période d'initialisation. Le paramètre $\boldsymbol{\sigma}$ représente l'écart-type de $\boldsymbol{P}$ et $\boldsymbol{x}$ est une variable.

La mise à jour des seuils est faite en introduisant les nouvelles valeurs de $\boldsymbol{P}$ dans le calcul de $\boldsymbol{P}\mu$ et $\boldsymbol{\sigma}$.

Donc:

$$\boldsymbol{Pth_i} = \boldsymbol{P}\mu_{\boldsymbol{i}} \pm \boldsymbol{x}.\boldsymbol{\sigma_i}$$

Avec :

$$\boldsymbol{P}\mu_{\boldsymbol{i}} = \frac{\sum_{\boldsymbol{k=1}}^{\boldsymbol{i-1}} \boldsymbol{P_k}}{\boldsymbol{i-1}}$$

Avec $\boldsymbol{Pth_i}$ est la valeur du seuil pour chaque paramètre $\boldsymbol{P}$ à l'instant $\boldsymbol{i}$. $\boldsymbol{P}\mu_{\boldsymbol{i}}$ est la valeur moyenne de toutes les valeurs du paramètre $\boldsymbol{P}$ précédant l'instant $\boldsymbol{i}$ et $\boldsymbol{\sigma_i}$ représente l'écart-type de $\boldsymbol{P}$ à l'instant $\boldsymbol{i}$.

4.2.1. Seuil pour PDR

Nous cherchons LCL pour calculer la valeur de PDRth, donc le seuil pour le PDR est calculé selon l'équation suivante:

$$\boldsymbol{PDRth} = \boldsymbol{PDR}\mu - \boldsymbol{x}.\boldsymbol{\sigma}$$

Avec :

$$\boldsymbol{PDR}\mu = \frac{\sum_{\boldsymbol{k=1}}^{\boldsymbol{n}} \boldsymbol{PDR_k}}{\boldsymbol{n}}$$

Les valeurs de PDR qui sont inférieures à PDRth sont des valeurs qui seront considérées comme des valeurs anormales, car ces valeurs signifient que le nombre de paquets qui sont reçus avec succès est faible et par conséquence, il existe un problème sur le médium de communication.

4.2.2. Seuil pour BPR

Nous cherchons UCL pour calculer la valeur de BPRth, donc le seuil pour le BPR est calculé par l'équation suivante:

$$\boldsymbol{BPRth} = \boldsymbol{BPR}\mu + \boldsymbol{x}.\boldsymbol{\sigma}$$

Avec :

$$\boldsymbol{BPR}\mu = \frac{\sum_{\boldsymbol{k=1}}^{\boldsymbol{n}} \boldsymbol{BPR_k}}{\boldsymbol{n}}$$

Les valeurs de BPR qui sont supérieures à BPRth sont des valeurs qui seront considérées comme des valeurs anormales, car ces valeurs signifient que le nombre de paquets erronés reçus est élevée par conséquence, il existe un problème sur le médium de communication.

4.2.3. Seuil pour ECA

Nous cherchons UCL pour calculer la valeur de ECAth, donc le seuil pour l'ECA est calculé par l'équation suivante:

$$\boldsymbol{ECAth} = \boldsymbol{ECA}\mu + \boldsymbol{x}.\boldsymbol{\sigma}$$

Avec :

$$\boldsymbol{ECA}\mu = \frac{\sum_{k=1}^{n} \boldsymbol{ECA_k}}{\boldsymbol{n}}$$

Les valeurs de ECA qui sont supérieures à ECAth sont des valeurs qui seront considérées comme des valeurs anormales, car ces valeurs signifient que la quantité d'énergie consommée par le nœud est très élevée par rapport à la valeur moyenne de ECA.

4.2.4. Seuil pour RSSI

Nous cherchons LCL pour calculer la valeur de RSSIth, donc le seuil pour le RSSI est calculé par l'équation suivante :

$$\boldsymbol{RSSIth} = \boldsymbol{RSSI}\mu - \boldsymbol{x}.\boldsymbol{\sigma}$$

Avec :

$$\boldsymbol{RSSI}\mu = \frac{\sum_{k=1}^{n} \boldsymbol{RSSI_k}}{\boldsymbol{n}}$$

Les valeurs de RSSI qui sont plus petites que RSSIth sont des valeurs qui seront considérées comme des valeurs anormales, car ces valeurs signifient que le niveau de la puissance reçue au niveau du nœud est très faible.

4.2.5. Seuil pour PSR

Pour PSR, nous utilisons deux seuils pour identifier le type de *jamming*. Pour le seuil PSRth1, nous cherchons LCL en supposant que le réseau est sous des conditions normales. Pour le seuil PSRth2, nous cherchons UCL en supposant que le réseau est mis sous des attaques de *jamming* constant et trompeur. En fait, dans les cas de *jamming* constant ou *jamming* trompeur, les valeurs de PSR sont très faibles ou égales à zéro, et dans le cas de

conditions normales ou *jamming* réactif, les valeurs de PSR sont très élevées. Donc les valeurs de PSR pendant le *jamming* aléatoire sont comprises entre PSRth1 et PSRth2.

Alors les seuils pour le PSR sont calculés par les équations suivantes :

$$\boldsymbol{PSRth1} = \boldsymbol{PSR}\mu_{\boldsymbol{1}} - \boldsymbol{x}.\boldsymbol{\sigma_1}$$

$$\boldsymbol{PSRth2} = \boldsymbol{PSR}\mu_{\boldsymbol{2}} + \boldsymbol{x}.\boldsymbol{\sigma_2}$$

Avec :

$$\boldsymbol{PSR}\mu = \frac{\sum_{k=1}^{n} \boldsymbol{PSR_k}}{\boldsymbol{n}}$$

4.3. Méthode proposée pour la détection de *jamming*

L'organigramme dans la Figure 20 présente les étapes dans notre algorithme pour détecter la présence de l'attaque de brouillage et identifier le type de brouilleur.

A chaque intervalle de temps « Te », nous avons une valeur pour chacun des paramètres réseau. Après une période d'initialisation, le système calcule les seuils relatifs à chacun de ces paramètres en utilisant les équations fournies dans le paragraphe 4.2.

Après cette phase d'initialisation, chaque nouvelle valeur des paramètres PDR, BPR, ECA, RSSI et PSR sera enregistrée afin de la comparer à la valeur de son seuil PDRth, BPRth, ECAth, RSSIth et (PSRth1, PSRth2) respectivement.

Après cette comparaison, si une des trois conditions suivantes est réalisée, alors cela signifie qu'il existe une attaque de brouillage.

$$\boldsymbol{Condition\ 1}: \ PDR < PDRth \ et \ BPR < BPRth \ et \ ECA > ECAth \ et \ RSSI > RSSIth$$

$$Ou$$

$$\boldsymbol{Condition\ 2}: \ PDR < PDRth \ et \ BPR > BPRth \ et \ ECA < ECAth \ et \ RSSI > RSSIth$$

$$Ou$$

$$\boldsymbol{Condition\ 3}: \ PDR < PDRth \ et \ BPR > BPRth \ et \ ECA > ECAth \ et \ RSSI > RSSIth$$

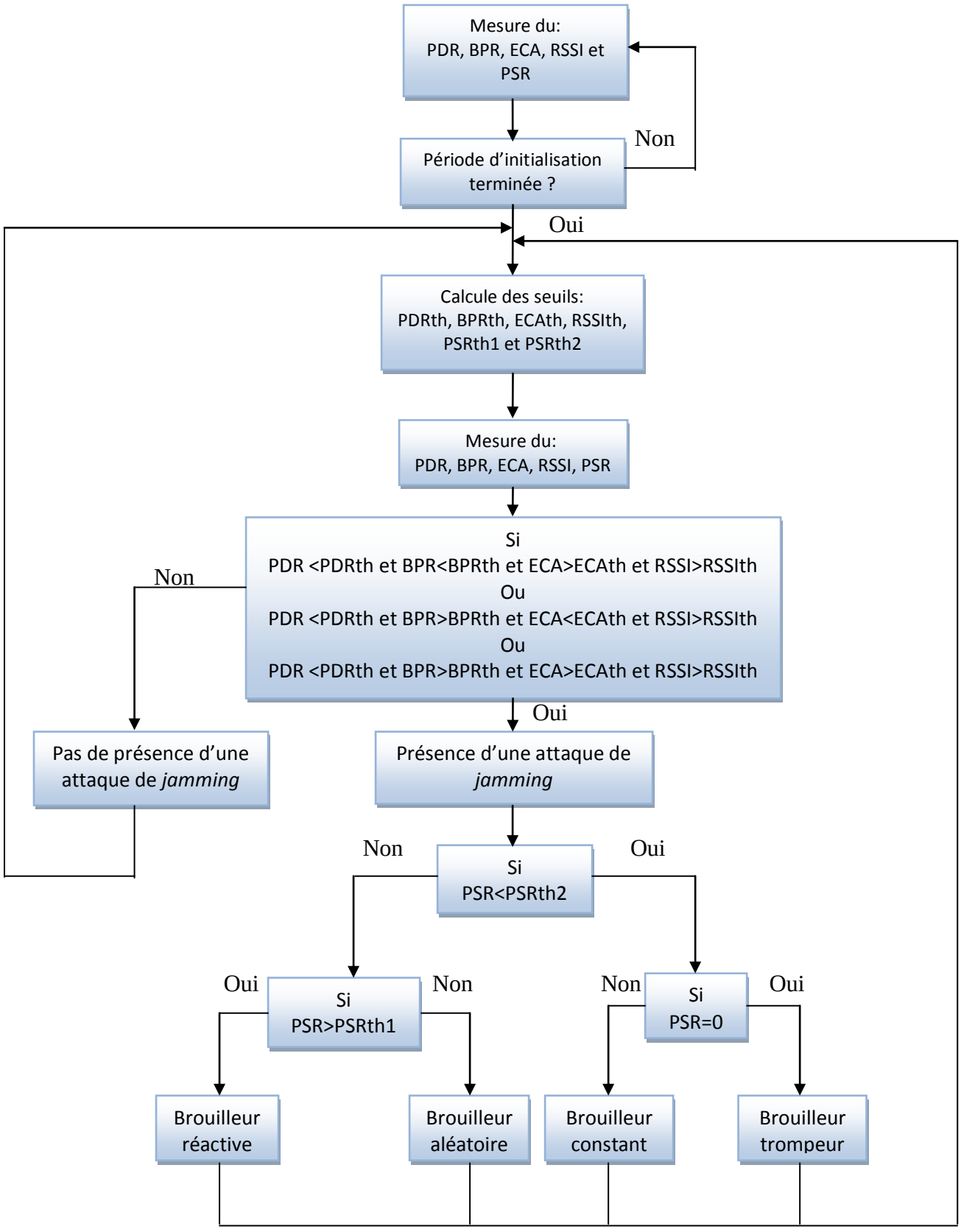


Figure 20 Organigramme qui représente les étapes pour détecter le *jamming*

Les trois conditions ci-dessus sont extraites des tableaux : Tableau 15, Tableau 16, Tableau 17, et Tableau 20. En effet, dans le cas d'un *jamming* trompeur, la condition « 1 » est réalisée, dans le cas d'un *jamming* réactif, la condition « 2 » est réalisée et dans le cas d'un *jamming* constant et/ou aléatoire, la condition « 3 » est réalisée.

Si aucune de ces conditions n'ait réalisée, cela veut dire qu'il n'y a pas une attaque de brouillage. Par contre, si au moins une de ces conditions est réalisée, alors il y a une présence d'une attaque de brouillage et dans ce cas nous utilisons la valeur du PSR pour identifier le type de brouilleur en comparant cette valeur avec un premier seuil PSRth2.

Si la valeur du PSR est inférieure à la valeur PSRth2 alors il y a deux cas de figures : si PSR est égal à zéro alors nous sommes dans le cas d'un brouilleur trompeur et si PSR a une valeur différente de zéro alors nous sommes dans le cas d'un brouilleur constant.

Par contre, si PSR est supérieure à PSRth2, nous réalisons un deuxième test en comparant la valeur du PSR avec un deuxième seuil PSRth1. Si la valeur de PSR est supérieure à la valeur de PSRth1, alors nous sommes dans le cas d'un brouilleur réactif, sinon alors nous sommes dans le cas d'un brouilleur aléatoire.

5. Résultats Expérimentaux

Dans cette partie, nous présentons nos résultats de simulation. Nous appliquons notre algorithme et nous faisons une comparaison avec d'autres propositions de détection du *jamming*.

Dans cette comparaison, nous démontrons que l'utilisation des quarte paramètres réseau PDR, BPR, ECA et RSSI est nécessaire pour augmenter le taux de détection du *jamming* et diminuer le taux de fausses détection et que l'utilisation de deux ou trois paramètres uniquement parmi ces paramètres n'est pas suffisante et peut conduire à avoir un taux plus élevé de fausses détection.

Dans ce travail, nous faisons une comparaison entre notre proposition et deux autres propositions pour détecter la présence du *jamming*. L'une des propositions existantes utilise la valeur du PDR et le niveau du RSSI uniquement, l'autre utilise la valeur du PDR, la valeur du BPR et le niveau de l'ECA. Notre proposition combine ces quatre paramètres réseau, c.à.d. PDR, BPR, ECA et RSSI.

5.1. Environnement de simulation

Pour appliquer les algorithmes de détection de brouillage, nous avons utilisé un modèle de simulation qui représente un réseau de capteurs médicaux sans fil, où nous avons quatre capteurs qui mesurent des paramètres physiologiques du patient et envoient leurs données à un nœud de collecte, puis ce nœud envoie les données à une station de base. A chaque intervalle Tc, chacun des capteurs envoie un paquet contenant la valeur mesurée au nœud de collecte. Puis le nœud de collecte envoie par son tour un paquet contenant toutes les données physiologiques à une station de base comme le montre la Figure 21.

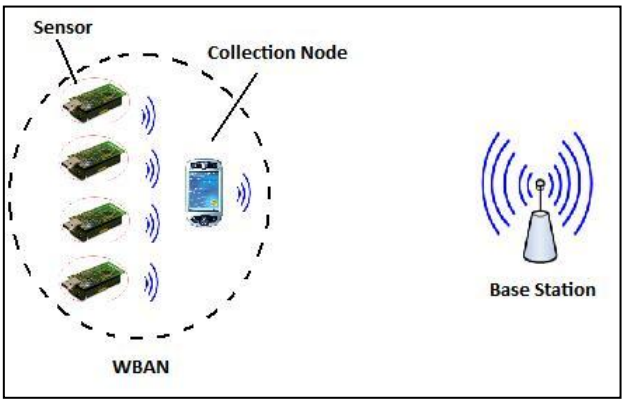


Figure 21 Réseau simulé

Nous avons utilisé le simulateur OMNet++ qui est un environnement de simulation d'évènements discrets. Il est largement utilisé dans la communauté scientifique afin de simuler les réseaux de communication. Le Tableau 21 illustre les paramètres de simulation utilisés.

Number of nodes	6
Sensor node type	MICA2
Radio unit consumption (transmit/receive/sleep)	16.5mA/ 9.6mA /3µA
MAC protocol	S-MAC
(Active/Sleep) period	(0.1s/11.9s) and (0.1s/1.9s)
Data rate	1 packet/12s and 1 packet/2s
Simulation time	720 min (43200 sec)
Sampling interval (Te)	1, 2 and 5 minutes

Tableau 21 Paramètres de simulation

A chaque intervalle Te, le nœud de collecte effectue une mesure des paramètres réseau PDR, BPR, ECA, RSSI et PSR.

Nous avons réalisé une phase d'initialisation d'une valeur $Tinit = 300$ minutes pour calculer les seuils. Durant cette phase, nous avons mis le réseau WBAN sous différentes conditions: *Normal Condition (NoC), Constant Jamming (CoJ), Reactive Jamming (ReJ), Deceptive Jamming (DeJ) et Random Jamming (RaJ).*

Ensuite, nous avons calculé la valeur moyenne de chacun des paramètres réseau en utilisant un débit de données faible (1 paquet/12 s) et un autre débit plus élevé (1 paquet/2 s), avec une mesure des paramètres réseau au niveau du nœud de collecte toutes les Te = 1, 2 et 5 minutes.

Nous allons présenter graphiquement les résultats dans le cas où le débit = 1 paquet/12 s et Te = 1 minute. La Figure 22 représente la valeur moyenne du PDR calculée au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1 minute.

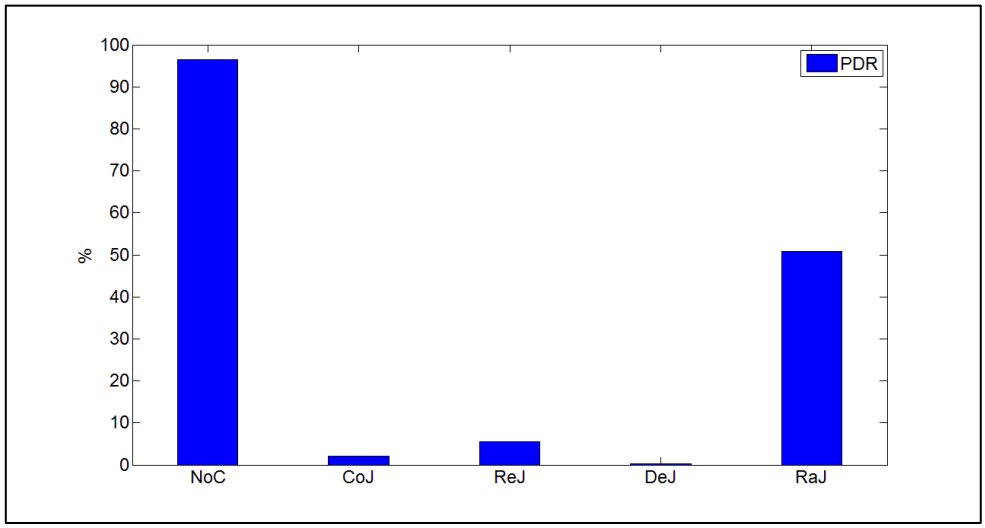


Figure 22 Valeur moyenne du PDR avec Te = 1 min

La Figure 23 représente la valeur moyenne du BPR calculée au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1 minute.

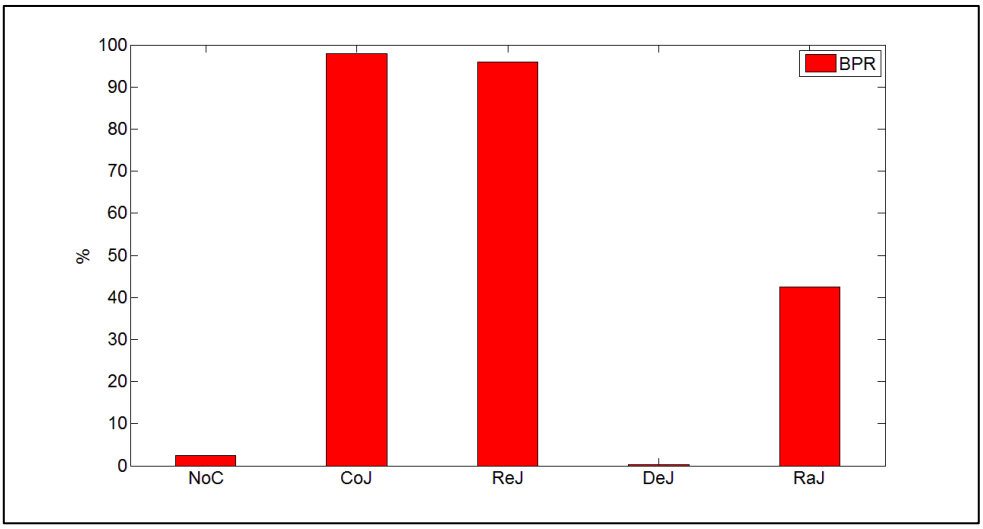


Figure 23 Valeur moyenne du BPR avec Te = 1 min

La Figure 24 représente la valeur moyenne du PSR calculée au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1 minute.

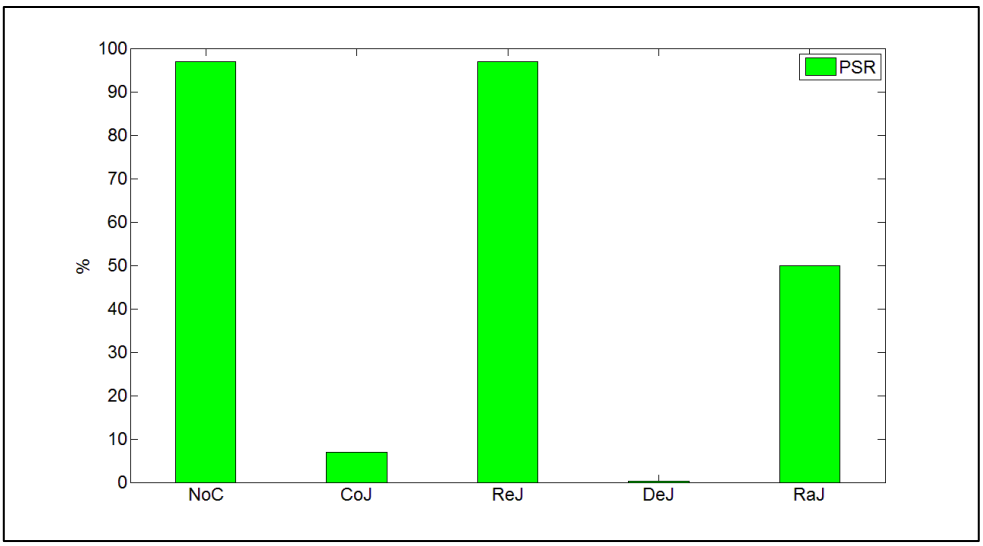


Figure 24 Valeur moyenne du PSR avec Te = 1 min

La Figure 22 représente la valeur moyenne de l'ECA calculée au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1 minute.

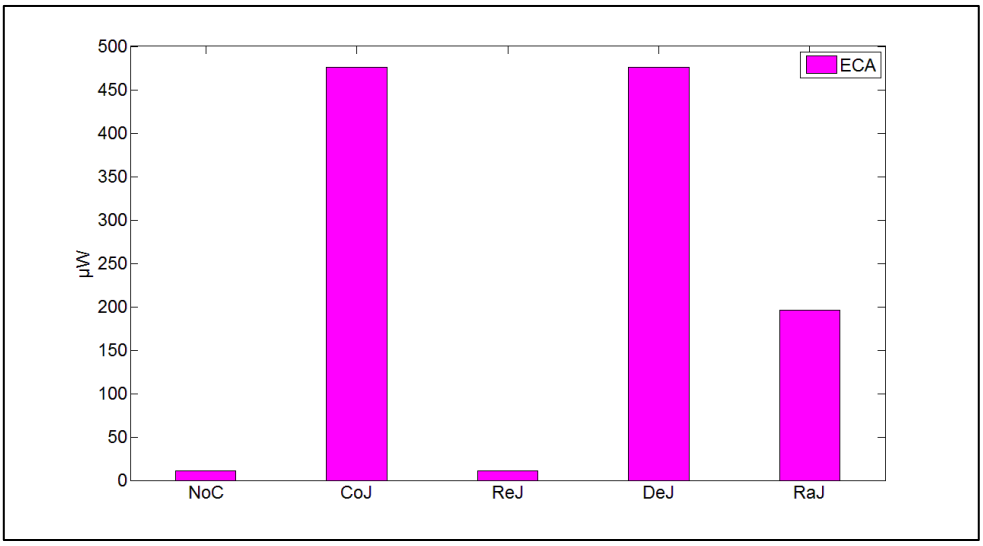


Figure 25 Valeur moyenne du PDR avec Te = 1 min

Le Tableau 22 représente les résultats des valeurs moyennes de PDR, BPR, PSR ECA et RSSI calculées au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1, 2 et 5 minutes dans le cas où le débit = 1 paquet/12 s.

Débit	Débit = 1 paquet /12 s														
Te	Te = 1 min					Te = 2 min					Te = 5 min				
Condition	NoC	CoJ	ReJ	DeJ	RaJ	NoC	CoJ	ReJ	DeJ	RaJ	NoC	CoJ	ReJ	DeJ	RaJ
PDR (%)	96.4	2	5.5	0	50.8	96.4	2	5.5	0	50.8	96.4	2	5.5	0	50.8
BPR (%)	2.5	98	96	0	42.5	2.5	98	96	0	42.5	2.5	98	96	0	42.5
PSR (%)	97	4.3	97	0	52.7	97	4.3	97	0	52.7	97	4.3	97	0	52.7
ECA (µW)	11	476	11	476	196	22	952	22	952	392	55	2380	55	2380	980
RSSI (dBm)	-32.1	-12.7	-12.7	-12.7	-12.7	-32.1	-12.7	-12.7	-12.7	-12.7	-32.1	-12.7	-12.7	-12.7	-12.7

Tableau 22 La valeur moyenne du PDR, BPR, PSR ECA et RSSI avec débit =1 paquet/12 s

Le Tableau 23 représente les résultats des valeurs moyennes de PDR, BPR, PSR ECA et RSSI calculées au niveau du nœud de collecte à partir d'une simulation du réseau de 300 minutes avec un Te = 1, 2 et 5 minutes dans le cas où le débit = 1 paquet/2 s.

Débit	Débit = 1 paquet /2 s														
Te	Te = 1 min					Te = 2 min					Te = 5 min				
Condition	NoC	CoJ	ReJ	DeJ	RaJ	NoC	CoJ	ReJ	DeJ	RaJ	NoC	CoJ	ReJ	DeJ	RaJ
PDR (%)	96	2.25	6.4	0	48.8	96	2.25	6.4	0	48.8	96	2.25	6.4	0	48.8
BPR (%)	2.6	98.5	96.2	0	42.3	2.6	98.5	96.2	0	42.3	2.6	98.5	96.2	0	42.3
PSR (%)	97.3	5.4	97	0	50.6	97.3	5.4	97	0	50.6	97.3	5.4	97	0	50.6
ECA (µW)	66	2856	66	2856	1176	132	5712	132	5712	2352	330	14280	330	14280	5880
RSSI (dBm)	-32	-12	-12	-12	-12	-32	-12	-12	-12	-12	-32	-12	-12	-12	-12

Tableau 23 La valeur moyenne du PDR, BPR, PSR ECA et RSSI avec débit =1 paquet/2 s

Ensuite nous avons réalisé deux simulations de 720 minutes (12 heures) de communication entre les capteurs du réseau, l'une en utilisant un débit de données faible (un paquet toutes les douze secondes) et l'autre en utilisant un débit plus élevé (un paquet toutes les deux secondes), avec une mesure des paramètres réseau au niveau du nœud de collecte toutes les Te = 1, 2 et 5 minutes.

Nous avons appliqué durant ces simulations six scénarios :

Dans les quatre premiers scénarios, nous avons appliqué du brouillage radio sur le réseau WBAN en utilisant respectivement les quatre types de *jamming : jamming* constant, *jamming* réactif, *jamming* aléatoire et *jamming* trompeur.

Dans le cinquième scénario, nous avons éloigné le nœud de collecte des quatre capteurs. Et dans le sixième scénario, nous avons appliqué un *jamming* aléatoire sur la station de base.

Dans la suite, nous appliquons les algorithmes sur le réseau simulé et nous présentons les résultats obtenus.

5.2. Application des algorithmes de détection et d'identification des attaques de *jamming*

Pour détecter le *jamming*, nous avons appliqué les trois algorithmes de détection du *jamming* (mentionnés au début de la section 5) sur le réseau simulé. Comme nous avons déjà mentionné, nous utilisons dans la première proposition les paramètres PDR et RSSI

uniquement. Dans la deuxième proposition, nous utilisons les paramètres PDR, BPR et ECA et dans la troisième proposition nous utilisons les paramètres PDR, BPR et ECA et RSSI.

Le PSR est utilisé dans les trois propositions pour identifier le type de *jamming*. Dans la suite, et pour des raisons de simplification, nous allons nommer la première proposition « Détection à 2 paramètres », la deuxième proposition « Détection à 3 paramètres » et la troisième proposition qui est notre proposition « Détection à 4 paramètres».

Dans la suite de cette section, nous allons présenter les résultats obtenus en appliquant les trois propositions de détection de *jamming* sur le réseau simulé et cela en utilisant deux débit de données différents. Pour chaque débit, nous allons utiliser trois valeurs différentes de « Te » comme nous avons déjà mentionné et cela dans le but de trouver la relation entre le débit des données et la valeur de « Te » qui donne les résultats les plus performants en termes de taux de détection et de taux de fausses détections. Nous utilisons aussi plusieurs valeurs pour la variable x qui entre dans le calcul des seuils. Le Tableau 24 représente les valeurs utilisées pour le débit, le « Te » et x.

Débit de données	
1 paquet/12 sec	1 paquet/2 sec
x.σ	
2σ, 3σ, 4σ, 5σ, 6σ et 7σ	2σ, 3σ, 4σ, 5σ, 6σ et 7σ
Te	
1, 2 et 5 minutes	1, 2 et 5 minutes

Tableau 24 Valeurs utilisées dans la simulation

5.3. Evaluation des performances

Pour faire une comparaison en termes de performances entre les trois propositions de détection de *jamming*, nous calculons le pourcentage de détections réussies des attaques, le pourcentage de fausses détections ainsi que l'efficacité globale de l'algorithme en termes de détection et d'identification de *jamming*.

Le taux de détection (DR : *Detection Rate*) est le rapport entre le nombre des attaques détectées et le nombre totales d'attaques existantes, DR est défini comme suit :

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

Le taux de fausses alarmes (FAR: *False Alarm Rate*) est le rapport entre le nombre de fausses détections et le nombre total de détections, FAR est défini comme suit :

$$FAR = \frac{Nombre\ de\ fausses\ détections}{Nombre\ total\ de\ détections} \times 100$$

Nous définissons l'efficacité globale de l'algorithme par :

$$Eff = \frac{N - (f + m + r)}{N} \times 100$$

Avec : N est le nombre total des échantillons testées, f est le nombre de fausses détections, m est le nombre des attaques non détectées et r est le nombre des attaques qui sont détectées mais mal identifiées.

Dans la suite de cette section, nous présentons les résultats obtenus pour chaque proposition.

5.3.1. Détection à 2 paramètres

Figure 26 à Figure 31 présentent le *DR, FAR* et *l'efficacité* pour tous les cas présentés dans le Tableau 24 et cela en utilisant la proposition « Détection à 2 paramètres ». Dans chacun de ces figures, la courbe en bleu représente le taux de détection, la courbe en rouge représente le taux de fausses alarmes et la courbe en vert représente l'efficacité. Le Tableau 25 et le Tableau 26 résument les résultats numériques obtenus.

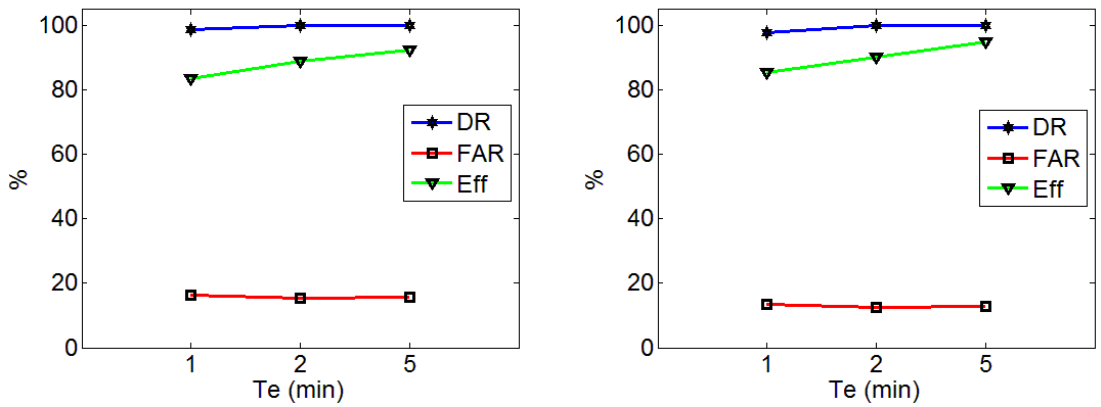


Figure 26 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/12 s, 2σ (à gauche), 3σ (à droite))

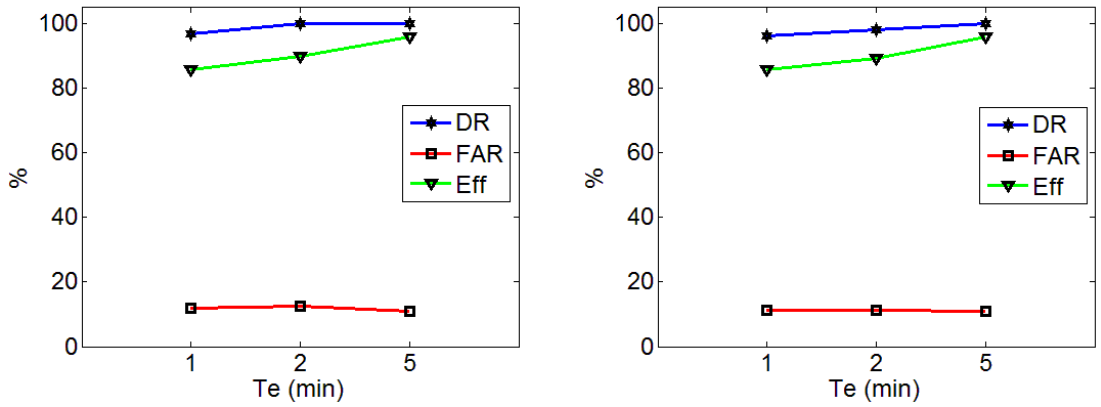


Figure 27 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/12 s, 4σ (à gauche), 5σ (à droite))

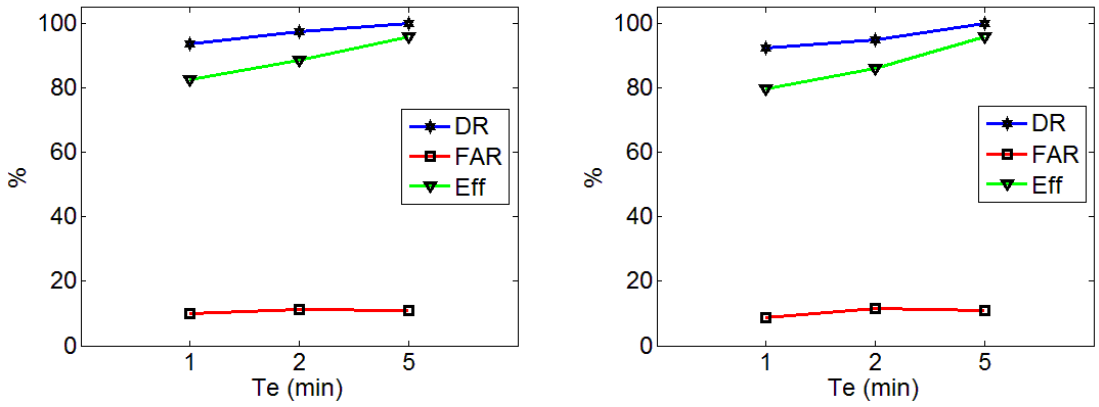


Figure 28 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/12 s, 6σ (à gauche), 7σ (à droite))

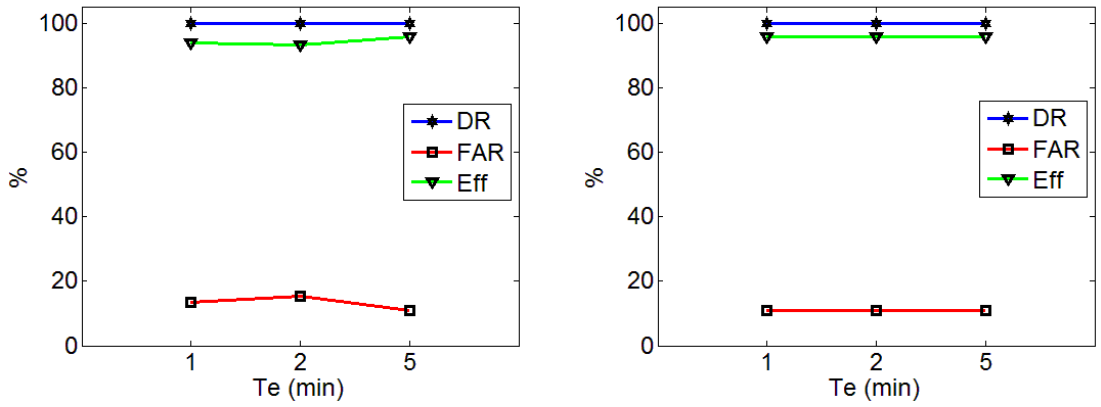


Figure 29 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/2 s, 2σ (à gauche), 3σ (à droite))

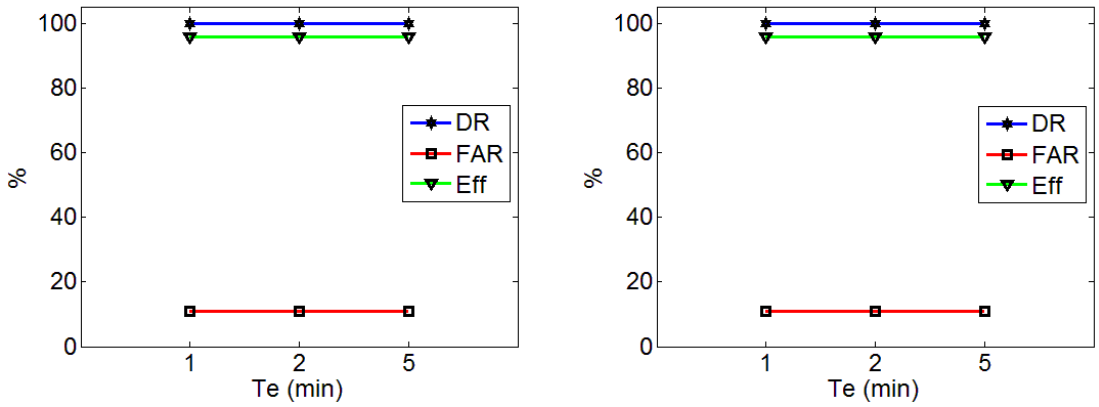


Figure 30 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/2 s, 4σ (à gauche), 5σ (à droite))

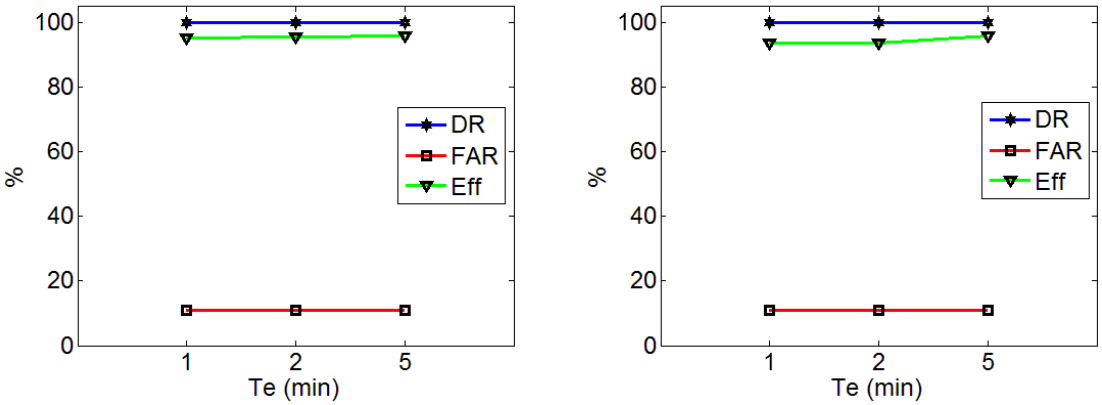


Figure 31 DR, FAR et Efficacité dans le cas (2-paramètres, Débit=1 paquet/2 s, 6σ (à gauche), 7σ (à droite))

Cas	Méthode à 2-paramètres (débit =1 paquet/12 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	98.7	16.2	83.4	97.9	13.6	85.5	97	11.7	85.8	96.2	11.2	85.6	93.7	10	82.6	92.5	8.6	79.7
Te=2 min	100	15.5	88.8	100	12.4	90.2	100	12.4	90	98.3	11.3	89.4	97.5	11.4	88.6	95	11.6	86.1
Te=5 min	100	15.7	92.3	100	12.7	95.1	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8

Tableau 25 Résultats numériques dans le cas (2-paramètres, débit=1 paquet/12 s)

Cas	Méthode à 2-paramètres (débit =1 paquet/2 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	100	13.3	94	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.2	100	11.1	93.8
Te=2 min	100	15.5	93.3	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.5	100	11.1	93.8
Te=5 min	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8

Tableau 26 Résultats numériques dans le cas (2-paramètres, débit=1 paquet/2 s)

5.3.2. Détection à 3 paramètres

Figure 37 présentent le *DR, FAR* et *l'efficacité* pour tous les cas présentés dans le Tableau 24 et cela en utilisant la proposition « détection à 3 paramètres». Dans chacun de ces figures, la courbe en bleu représente le taux de détection, la courbe en rouge représente le taux de fausses alarmes et la courbe en vert représente l'efficacité. Le Tableau 27 et le Tableau 28 résument les résultats numériques obtenus.

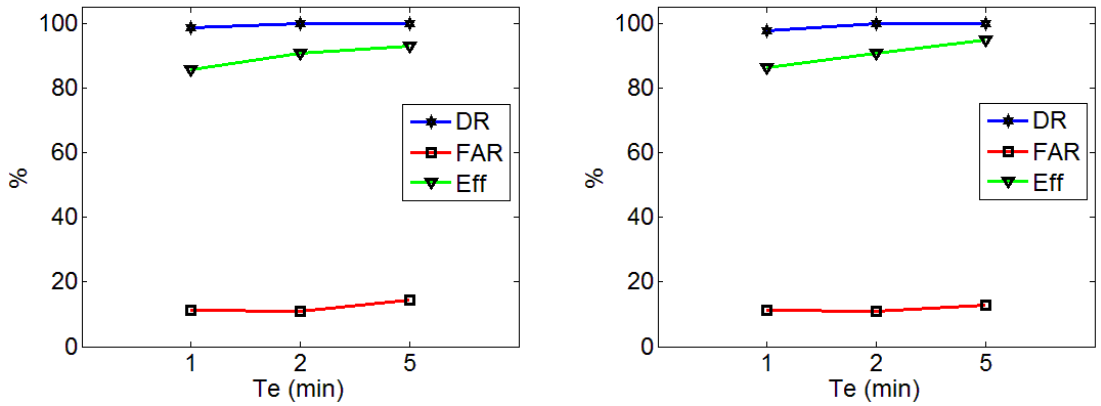


Figure 32 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/12 s, 2σ (à gauche), 3σ (à droite))

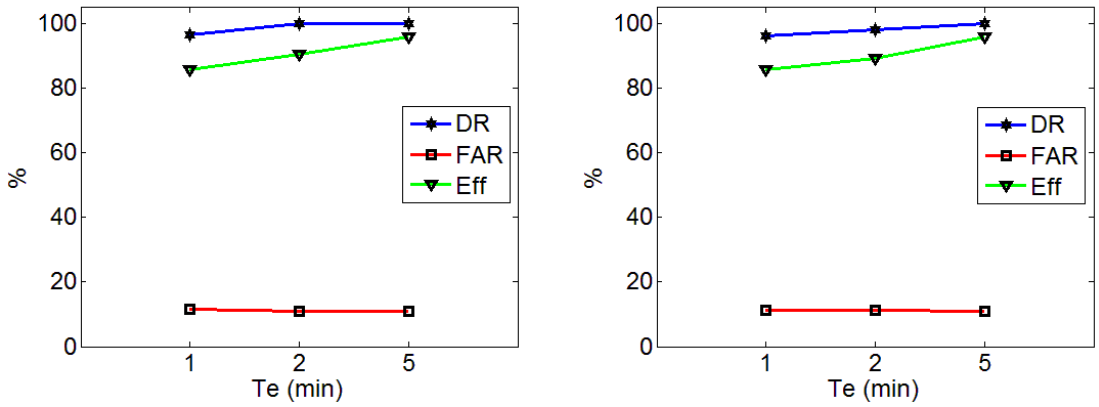


Figure 33 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/12 s, 4σ (à gauche), 5σ (à droite))

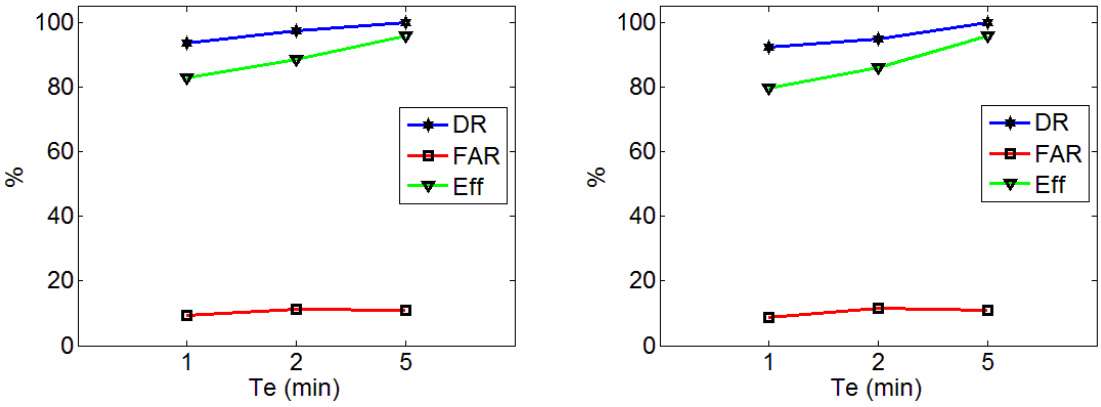


Figure 34 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/12 s, 6σ (à gauche), 7σ (à droite))

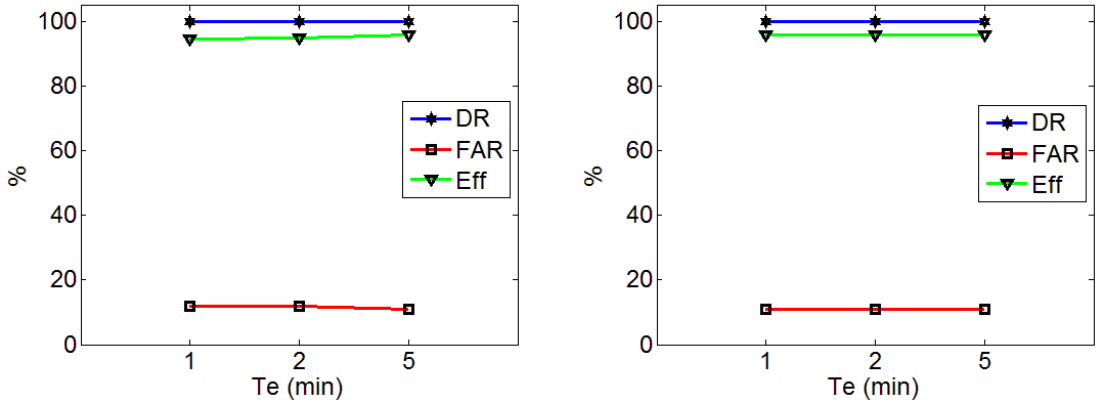


Figure 35 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/2 s, 2σ (à gauche), 3σ (à droite))

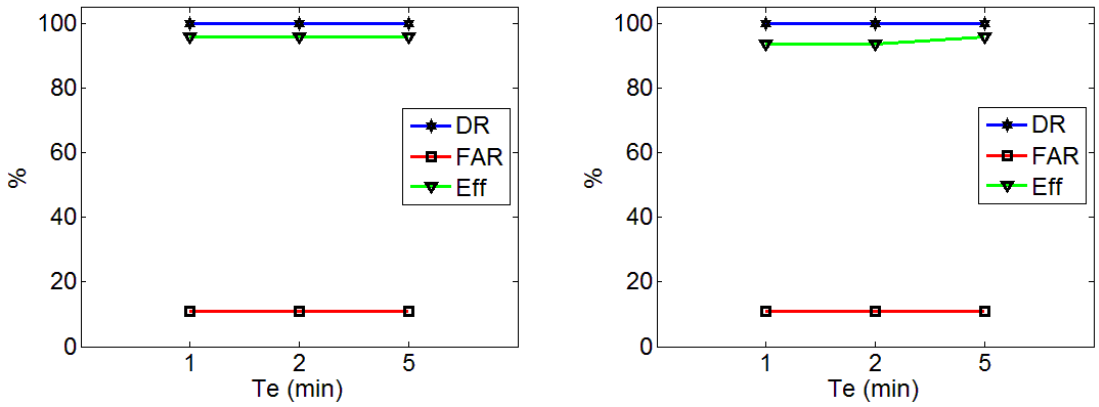


Figure 36 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/2 s, 4σ (à gauche), 5σ (à droite))

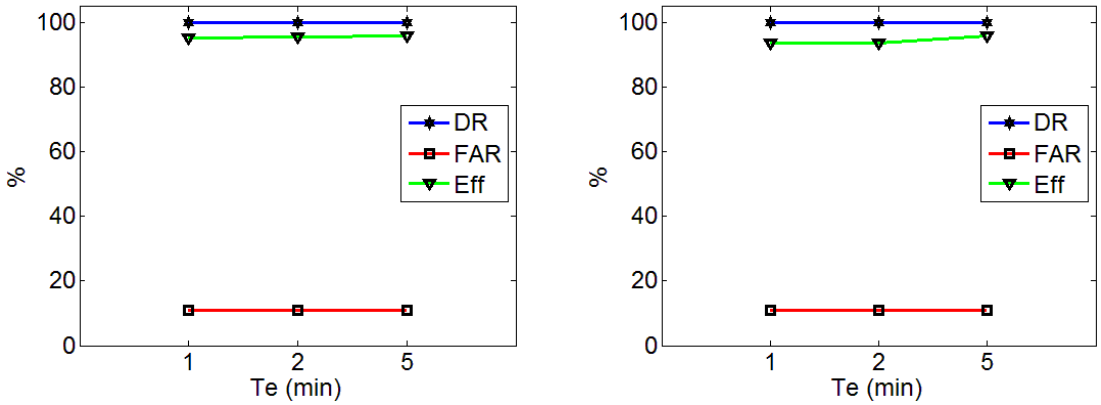


Figure 37 DR, FAR et Efficacité dans le cas (3-paramètres, Débit=1 paquet/2 s, 6σ (à gauche), 7σ (à droite))

Cas	Méthode à 3-paramètres (débit =1 paquet/12 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	98.7	11.2	85.7	97.9	11.3	86.5	96.6	11.4	85.8	96.2	11.2	85.6	93.7	9.3	82.9	92.5	8.6	79.7
Te=2 min	100	11.1	90.83	100	11.1	90.8	100	11.1	90.5	98.3	11.3	89.4	97.5	11.4	88.6	95	11.6	86.1
Te=5 min	100	14.2	93	100	12.7	95.1	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8

Tableau 27 Résultats numériques dans le cas (3-paramètres, débit=1 paquet/12 s)

Cas	Méthode à 3-paramètres (débit =1 paquet/2 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	100	11.7	94.7	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.2	100	11.1	93.8
Te=2 min	100	11.7	95	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.5	100	11.1	93.8
Te=5 min	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8	100	11.1	95.8

Tableau 28 Résultats numériques dans le cas (3-paramètres, débit=1 paquet/2 s)

5.3.3. Détection à 4 paramètres

Figure 38 à Figure 43 présentent le *DR, FAR* et *l'efficacité* pour tous les cas présentés dans le Tableau 24 et cela en utilisant la proposition « détection à 4 paramètres». Dans chacun de ces figures, la courbe en bleu représente le taux de détection, la courbe en rouge représente le taux de fausses alarmes et la courbe en vert représente l'efficacité. Le Tableau 29 et le Tableau 30 résument les résultats numériques obtenus.

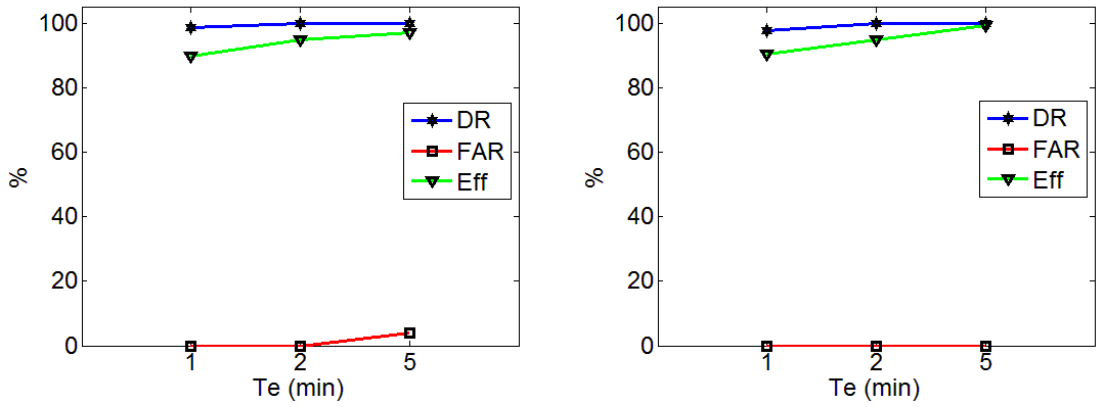


Figure 38 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/12 s, 2σ (à gauche), 3σ (à droite))

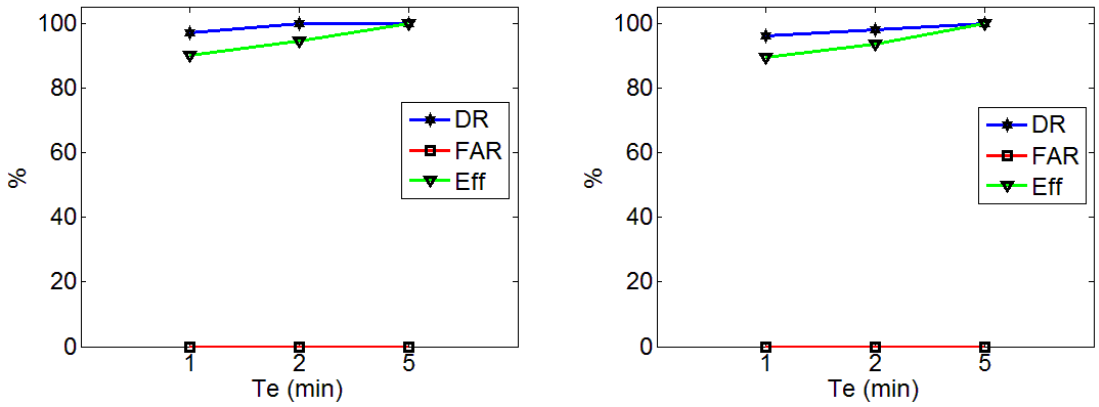


Figure 39 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/12 s, 4σ (à gauche), 5σ (à droite))

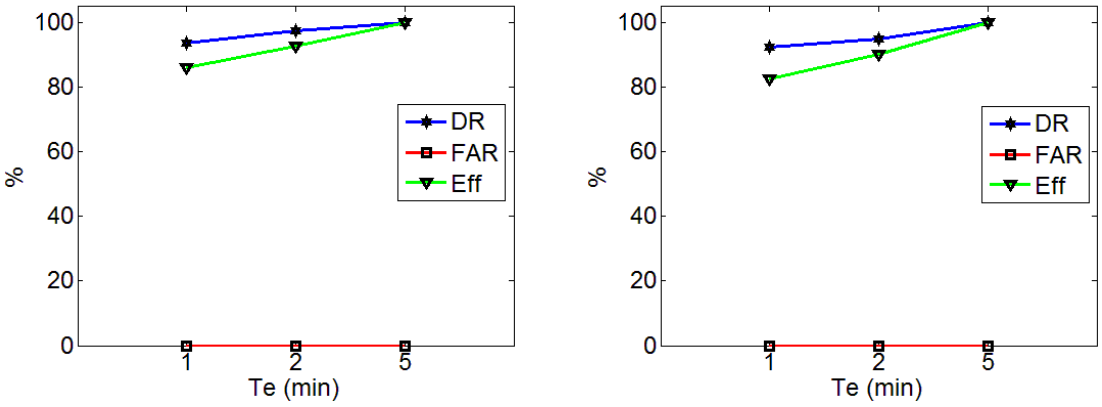


Figure 40 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/12 s, 6σ (à gauche), 7σ (à droite))

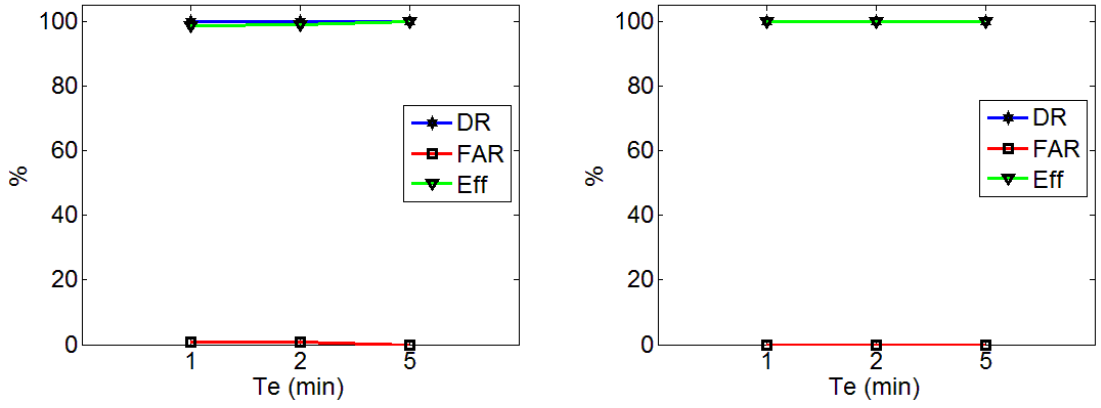


Figure 41 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/2 s, 2σ (à gauche), 3σ (à droite))

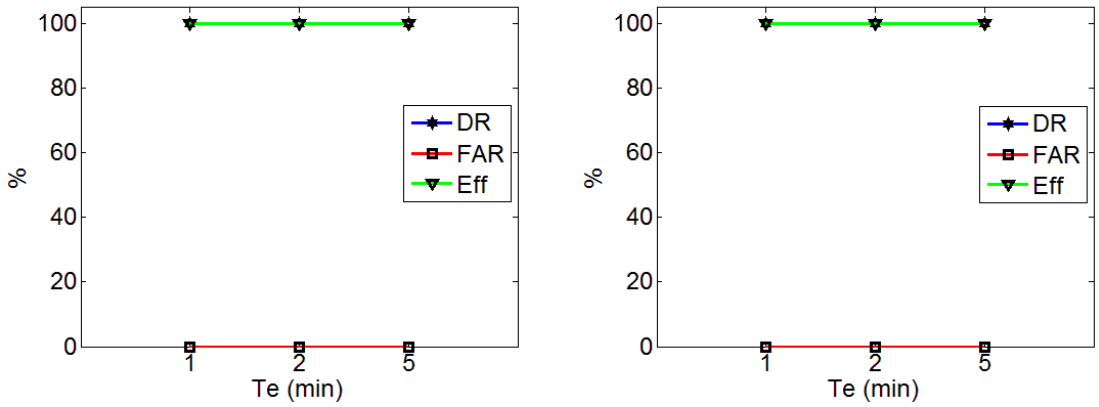


Figure 42 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/2 s, 4σ (à gauche), 5σ (à droite))

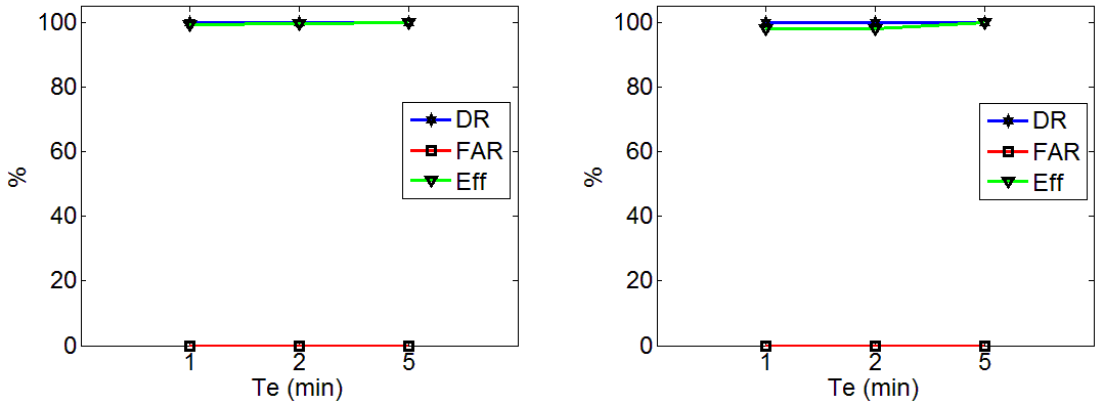


Figure 43 DR, FAR et Efficacité dans le cas (4-paramètres, Débit=1 paquet/2 s, 6σ (à gauche), 7σ (à droite))

Cas	Méthode à 4-paramètres (débit =1 paquet/12 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	98.7	0	89.8	97.9	0	90.7	97.1	0	90.1	96.2	0	89.7	93.7	0	86.1	92.5	0	82.6
Te=2 min	100	0	95	100	0	95	100	0	94.7	98.3	0	93.6	97.5	0	92.7	95	0	90.2
Te=5 min	100	4	97.2	100	2	99.3	100	0	100	100	0	100	100	0	100	100	0	100

Tableau 29 Résultats numériques dans le cas (4-paramètres, débit=1 paquet/12 s)

Cas	Méthode à 4-paramètres (débit =1 paquet/2 s)																	
xσ	2σ			3σ			4σ			5σ			6σ			7σ		
Evaluation	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)	DR (%)	FAR (%)	Eff (%)
Te=1 min	100	0.8	98.8	100	0	100	100	0	100	100	0	100	100	0	99.4	100	0	98
Te=2 min	100	0.8	99.1	100	0	100	100	0	100	100	0	100	100	0	99.7	100	0	98
Te=5 min	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100	100	0	100

Tableau 30 Résultats numériques dans le cas (4-paramètres, débit=1 paquet/2 s)

5.3.4. Discussion

D'après les résultats obtenus, nous pouvons remarquer que :

1-Notre proposition (Détection à 4 paramètres) est plus performante par rapport aux deux autres propositions parce qu'elle a mené à un taux de fausses détections égal à zéro, et elle a présenté une efficacité globale plus élevée par rapport aux deux autres propositions et cela quel que soit le débit, quel que soit la valeur de $\boldsymbol{x}$ et quel que soit la valeur de Te.

2-En appliquant les deux propositions « détection à 2 paramètres » et « détection à 3 paramètres » et pour un DR égal à 100%, la valeur minimale possible de FAR est égale à 11.1%. Par contre, en appliquant notre proposition « détection à 4 paramètres », nous avons obtenu un FAR égale à 0%. Cela s'explique par les faits suivants :

2.1-Dans le cas de la proposition « détection à 3 paramètres » : cette méthode a classifié le scénario où nous avons éloigné le nœud de collecte des quatre capteurs comme une attaque de *jamming* sur le réseau WBAN, parce que dans ce scénario la valeur du PDR est inférieure à PDRth, la valeur de BPR est supérieure à BPRth et la valeur du ECA est inférieure à ECAth. Et comme cette méthode ne tient pas en compte la valeur du niveau de RSSI, donc cette méthode va considérer que ce scénario est une attaque de *jamming* réactif. Par contre, notre méthode a considéré que ce n'est pas une attaque de *jamming* car elle a mesuré le niveau du RSSI qui est inférieure à RSSIth dans ce scénario. Alors la cause de ces valeurs de PDR et de BPR est due au niveau faible de RSSI.

2.2-Dans le cas de la proposition « détection à 2 paramètres » : le nœud de collecte a classifié le scénario où nous avons appliqué un *jamming* aléatoire sur la station de base

comme une attaque de *jamming* qui vise le réseau WBAN. En fait, comme cette méthode n'utilise pas les paramètres BPR et ECA, et comme la valeur du PDR est inférieure à PDRth et la valeur du RSSI est supérieure à RSSIth durant ce scénario, l'algorithme a considéré qu'il y a une attaque de *jamming*. Par contre, notre méthode a considéré que ce n'est pas une attaque de *jamming* car elle a mesuré le taux de BPR qui est inférieur à BPRth et le niveau de l'ECA qui est inférieur à ECAth dans ce scénario. Alors la cause de cette valeur faible de PDR est due au fait que la station de base est mise sous un *jamming* aléatoire, et donc cette station de base ne peut pas envoyer toujours des paquets ACK au nœud de collecte, ce qui diminue le taux des paquets délivrés PDR mesuré au niveau du nœud de collecte. De même, dans un scénario où la station de base tombe en panne et elle ne peut plus envoyer des paquets ACK au point de collecte, la méthode de détection à 2 paramètres va considérer que c'est une attaque de *jamming*, ce qui n'est pas le cas et la valeur faible du PDR est due à un défaut dans la station de base.

3-Dans le cas du débit de données faible (1 paquet/ 12 s), lorsque nous avons augmenté la valeur de Te (Période d'échantillonnage), le taux de détection et l'efficacité globale de l'algorithme augmentent et cela pour les trois propositions et quelle que soit la valeur de x.

4-Dans le cas d'un débit plus élevé (1 paquet/ 2 s), les résultats de DR, FAR et l'efficacité sont presque stables lorsqu'on augmente la valeur de Te.

5.3.5. Récapitulatif

D'après les résultats, nous pouvons conclure que notre méthode « détection à 4 paramètres » est la méthode la plus performante par rapport aux deux autres propositions.

Dans le cas où le débit est faible (1 paquet/ 12 s), il faut choisir une valeur de Te égale à 5 minutes et en utilisant une valeur de $(x = 4, 5, 6\ ou\ 7)$ pour avoir les résultats les plus performants (DR=100%, FAR=0% et une efficacité=100%).

Par contre, dans le deuxième cas où le débit est plus élevé (1 paquet/2 s), nous pouvons choisir pour avoir (DR=100%, FAR=0% et une efficacité=100%) un « Te = 1, 2 ou 5 minutes » avec un $x = 3, 4\ ou\ 5$, mais nous préférons choisir un « Te = 1 minute » afin de détecter l'attaque plus rapidement.

Dans ce chapitre, nous avons proposé une méthode de détection de l'attaque de brouillage radio (*jamming*) dans un réseau de capteurs WBAN. Les principaux avantages qui sont offerts par cette méthode sont :

- Un taux de détection très élevé.

- Un taux de fausses détections très réduit.

- Une capacité à identifier le type de *jamming* et faire la différence entre les quatre types de *jamming* suivants : *jamming* constant, *jamming* réactif, *jamming* aléatoire et *jamming* trompeur.

Le Tableau 31 présente une comparaison entre notre proposition de détection de *jamming* et quelques autres travaux de recherche déjà présentés à la fin du Chapitre III.

Critères de comparaison	Xu et al.	Reyes et al.	Misra et al.	Fragkiadakis et al.	Cakiroglu et al.	Notre proposition
Paramètres mesurés	PDR et RSSI	PDR, BPR, RSSI et CCA	SNR et PDPT	SNR	PDR, BPR et ECA	PDR, BPR, ECA, PSR et RSSI
Détection de l'attaque effectuée par	Nœud individuel	Nœud individuel	Station de base	Nœud individuel	Nœud individuel	Nœud de collecte
Utilisation des seuils	Oui	Non	Non	Oui	Oui	Oui
Complexité de calcul (1:plus simple, 4: plus complexe)	1	4	3	3	2	2
Efficacité de détection (+++: plus efficace, +: moins efficace)	+	++	++	+	++	+++
Obligation de communiquer avec la station de base pour signaler le *jamming*	Oui	Oui	Non	Oui	Oui	Oui
Capable à identifier le type de *jamming*	Non	Non	Oui	Non	Non	Oui
Contexte d'application	Wireless Sensor Network (WSN)	Wireless Network (WN)	WSN	WN	WSN	Wireless Body Area Network (WBAN)
Etudie la relation entre le débit et la période d'échantillonnage « Te »	Non	Non	Non	Non	Non	Oui

Tableau 31 Comparaison entre notre proposition et quelques travaux de recherche

6. Conclusion

Dans ce chapitre, nous avons présenté notre contribution dans la détection des attaques de brouillage radio (*Jamming*) dans un réseau de capteurs médicaux sans fil.

Nous avons commencé par une classification des attaques de brouillage selon le type de brouilleur, et nous avons décrit chaque type de brouilleur et son effet sur la communication des paquets dans le réseau de capteurs sans fil.

Puis nous avons défini plusieurs paramètres réseau qui sont dans la suite utilisés comme critères de détection des attaques de brouillage. Nous avons aussi expliqué l'influence de chaque type de brouillage sur la valeur de ces paramètres.

Ensuite, nous avons présenté notre méthode proposée pour la détection des attaques de brouillage dans un réseau de capteurs sans fil médicaux. Cette méthode est basée sur la mesure des valeurs de plusieurs paramètres du réseau et leur comparaison avec la valeur d'un seuil relatif à chacun de ces paramètres.

Finalement, nous avons appliqué notre méthode proposée. Les résultats de simulation ont bien prouvé que l'utilisation des quatre paramètres ensemble c.à.d. du PDR, BPR, ECA et RSSI augmente le degré de précision dans la détection des attaques de brouillage et diminue le taux de fausses détections.

Chapitre V : Détection des attaques de *flooding* dans les réseaux IP médicaux

1. Introduction

L'utilisation des réseaux de capteurs dans le domaine de la médecine peut apporter une surveillance permanente des patients et une possibilité de collecter des informations physiologiques. Dans un système de surveillance médicale à distance, ces informations peuvent être envoyées à l'équipe médicale via un réseau IP haut débit comme le montre la Figure 44.

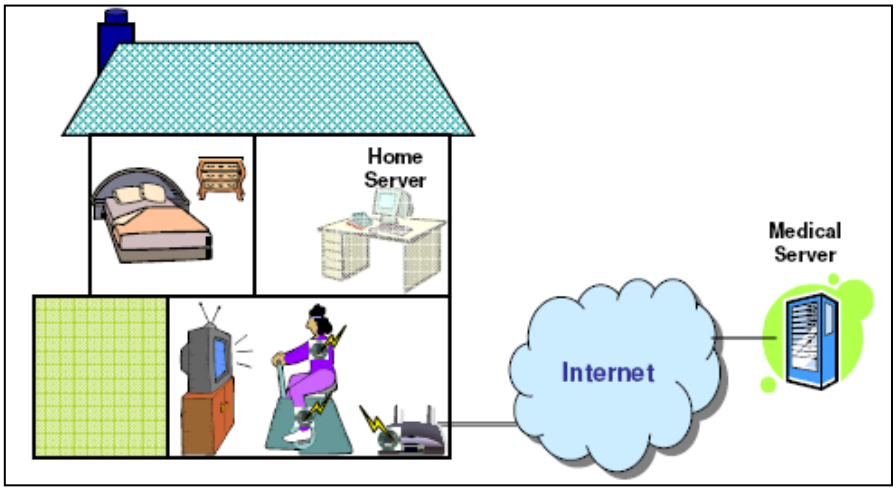


Figure 44 Système de surveillance médicale à distance

En fait, les systèmes d'informations sont aujourd'hui de plus en plus ouverts sur Internet. Cette ouverture, a priori bénéfique, pose néanmoins un problème majeur : il en découle un nombre croissant d'attaques.

Donc, dans les systèmes de surveillance médicale, les données médicales transmises via un réseau IP sont vulnérables aux attaques, ce qui est très dangereux pour la santé des patients, d'où la nécessité d'un système de sécurité et de détection d'attaques.

Dans ce chapitre, nous allons présenter notre contribution au niveau de détection des attaques de type déni de service (DoS: Denial of Service) et plus particulièrement l'attaque de type *SYN Flooding* sur une communication des paquets dans un réseau IP haut débit. Nous allons proposer une méthode de mesure de divergence qui s'appelle Power Divergence et faire une comparaison au niveau de performance avec d'autres méthodes de mesure de divergence que nous allons utiliser pour détecter les attaques *SYN Flooding*.

2. Les attaques DoS dans les réseaux IP

Les attaques par déni de service (DoS : Denial of Service en anglais) sont des attaques qui visent à rendre une machine ou un réseau indisponible durant une certaine période.

En apparence, une telle attaque peut sembler inoffensive si elle vise un réseau ou un ordinateur particulier, mais elle peut s'avérer redoutable lorsqu'elle vise un serveur où des ressources informatiques doivent être délivrées en temps réel.

Cette attaque devient alors très dangereuse dans le cas d'un système de surveillance médicale à distance où l'équipe médicale a besoin d'une communication permanente des informations physiologiques des patients.

En effet, ce genre d'attaque est très répandu dans les réseaux car une telle attaque est assez simple à mettre en œuvre, ce qui peut avoir des conséquences désastreuses. De plus, la détection et la prévention de ces attaques sont difficiles car elles peuvent prendre des formes très variées.

Le principe général des attaques DoS consiste à envoyer des données ou des paquets dont la taille ou le contenu est inhabituel. Ceci a pour effet de provoquer des réactions inattendues du réseau ou de la machine cible, pouvant aller jusqu'à l'interruption du service.

Les attaques DoS prennent de multiples formes et utilisent de nombreuses méthodes différentes pour mettre hors service une ressource réseau. Nous allons définir de manière non exhaustive différentes attaques connues et répandues.

2.1. Les attaques par surcharge

Une des méthodes les plus répandues et une des plus simples à mettre en œuvre est de surcharger complètement la cible de requêtes de toutes sortes. On distingue trois grands types d'attaques par surcharge utilisant différents protocoles et différentes couches réseaux.

2.1.1. Le SYN flood

L'attaque *SYN flood*, représentée dans la Figure 45, utilise des paquets TCP contenant le flag SYN. Ce flag signifie à la cible que l'on veut initier une connexion avec elle. En envoyant un nombre très important de ces paquets, on oblige le serveur à démarrer un socket de connexion pour chaque requête ; il enverra alors des paquets contenant les acquittements SYN ACK pour établir la connexion mais ne recevra jamais de réponses. Le serveur aura donc un grand nombre de connexions en attente et arrivera à saturation jusqu'à ne plus pouvoir répondre aux connexions légitimes des utilisateurs.

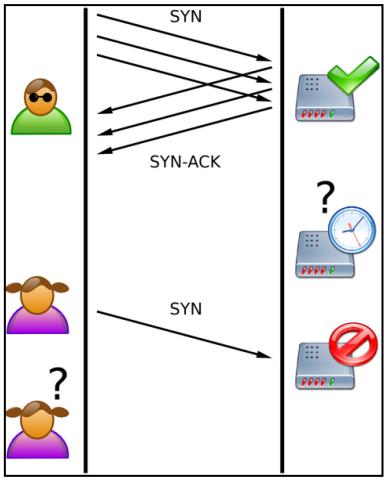


Figure 45 *SYN Flood attack*

Pour éviter de se faire repérer, la source des attaques peut combiner cette attaque avec les changements du champ IP source des paquets envoyés ce qui redirigera les réponses de la cible vers une autre destination. Ce type d'usurpation est aussi appelé attaque en aveugle car les réponses venant de la cible ne pourront être reçues par l'attaquant, Ce dernier lance l'attaque mais ne peut pas vérifier son efficacité autrement qu'en essayant une connexion légitime au serveur.

2.1.2. Le PING flood

Un *ping flood* (ou *ICMP flood*) est une forme simple d'attaque par déni de service, où l'attaquant inonde le serveur cible de requêtes ping. Ce type d'attaque ne réussit que si l'attaquant a plus de bande passante que sa victime.

2.1.3. Le Smurf

Les attaques *Smurf* représentées dans Figure 46 profitent d'une faiblesse du protocole IPv4 et d'une mauvaise configuration des routeurs dans les réseaux permettant l'envoi de paquets à l'adresse de *broadcast*. L'adresse de *broadcast* est une adresse IP qui permet de joindre toutes les machines d'un réseau. L'attaquant envoie à cette adresse de *broadcast* des paquets contenant l'adresse IP source de la victime. Ainsi, chaque machine sur le réseau va répondre à la cible à chaque requête de l'attaquant. On se sert ainsi du réseau comme un amplificateur pour perpétrer l'attaque. Cette méthode porte aussi le nom d'attaque réfléchie permettant à l'attaquant de couvrir ces traces et de rendre l'attaque plus puissante.

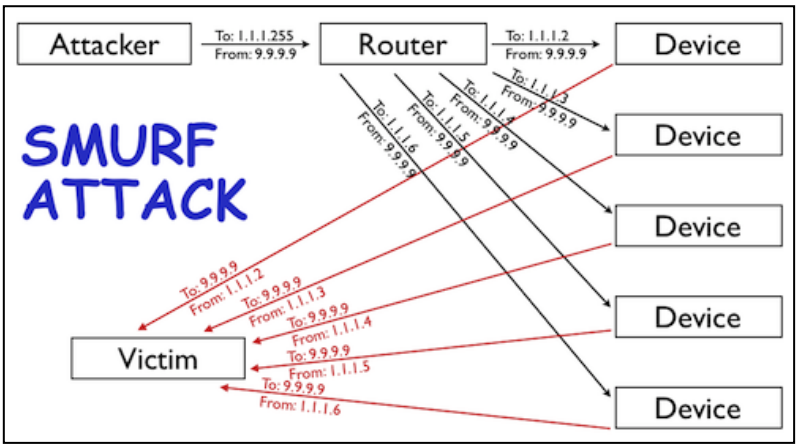


Figure 46 *Smurf attack*

2.2. Les attaques par failles

Un autre moyen de réaliser un DoS consiste à exploiter les nombreuses failles présentes dans les systèmes d'informations. Au lieu de chercher à surcharger la cible, on va simplement la forcer à réagir de façon bien définie en lui soumettant des informations qu'elle ne peut gérer.

Les systèmes Microsoft Windows sont par exemple très vulnérables à ce genre d'attaques. De nombreux moyens existent afin de tromper le système pour l'exploiter. Néanmoins, ces attaques sont de moins en moins nombreuses et de moins en moins efficaces car les systèmes d'exploitation actuels sont de plus en plus sécurisés. Nous décrivons ci-après quelques types d'attaque par faille.

2.2.1. Teardrop Attack

Cette attaque consiste à envoyer des paquets IP invalides à la cible, ces paquets peuvent être fragmentés ou contenir des données corrompues ou qui dépassent la taille réglementaire. Ces paquets ne pouvant être interprétés rendrons la machine inopérante.

2.2.2. Ping of Death

Cette attaque reprend le principe de l'attaque *Teardrop* mais avec des paquets ICMP. Les paquets ICMP possèdent généralement un champ donné de 56 octets. Certains systèmes deviennent vulnérables en envoyant des PING avec un champ de données plus important. Les systèmes en général ne sont pas prévus pour recevoir des paquets ICMP plus gros que les paquets IP traditionnels (64Koctets), mais les PING peuvent être fragmentés. Cependant, une fois rassemblés, ces paquets causeront une saturation de la mémoire tampon. Cette attaque est de nos jours obsolète car la majorité des systèmes ont été corrigés. Elle touchait tous les systèmes d'exploitation et même les équipements réseaux tels que les routeurs et les imprimantes.

2.3. Les attaques distribuées

La plupart des attaques, citées plus haut, peuvent être exécutées de manière distribuée ; On parle alors de DDoS (*Distributed Denial of Service*). Les attaques distribuées se basent sur le fait suivant: attaquer une cible toute seule se traduit souvent par un échec, mais si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir.

Il y a deux façons d'exécuter une attaque DDoS. On peut tout d'abord utiliser un groupe de personnes en connivence et convenir d'un moment et d'une façon bien précise de mener l'attaque. Ce n'est pas la méthode la plus simple et elle nécessite beaucoup d'organisations et de logistiques. L'autre façon est de disposer d'un nombre important de machines corrompues à travers le monde et de les utiliser pour perpétrer l'attaque (voire Figure 47). Ceci nécessite au

préalable une grande préparation pour corrompre les machines et les maintenir sous contrôle, mais présente aussi un avantage certain de pouvoir accomplir l'attaque seul.

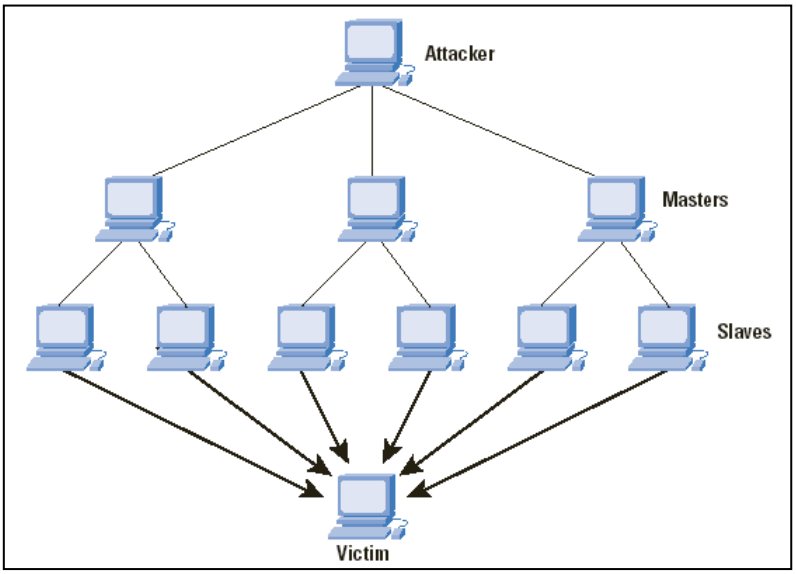


Figure 47 *DDoS attack*

3. Modèles de mesure de divergence

Les modèles de mesure de divergence sont utilisés dans la détection des anomalies. En fait, les approches statistiques établissent un profil du trafic normal pendant une période d'apprentissage, et les écarts par rapport au profil établi sont considérés comme des anomalies. Habituellement, les activités malveillantes provoquent un brusque changement dans les valeurs statistiques des paramètres décrivant le trafic (par exemple: le nombre de paquets, le nombre d'octets, le nombre de SYN, etc.).

Dans cette section, nous allons présenter quatre méthodes de mesure de divergences, ainsi que notre proposition (*Power Divergence*) que nous allons utiliser dans la suite de ce chapitre pour détecter les attaques *SYN flooding*.

3.1. Hellinger Distance (HD)

Hellinger Distance est utilisé pour calculer la divergence entre deux ensembles de valeurs de probabilité. Pour deux distributions de probabilité discrètes $P = (p_0, p_1, \dots, p_{K-1})$ et $Q = (q_0, q_1, \dots, q_{K-1})$, avec $p_i \geq 0$, $q_i \geq 0$ et :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1$$

HD entre la distribution actuelle *P* et la distribution d'avant *Q* est définie comme suit [89] :

$$HD(P,Q) = \frac{1}{2} \sum_{i=0}^{K-1} (\sqrt{p_i} - \sqrt{q_i})^2$$

Où HD vérifie l'inégalité: $0 \leq HD(P,Q) \leq 1$, et $HD(P,Q) = 0$ si et seulement si $P = Q$. HD est une distance symétrique ($HD(P,Q) = HD(Q,P)$), et induit deux pics, l'un au début du changement, et l'autre à la fin du changement.

3.2. Chi-square Divergence (CSD)

Chi-square divergence entre deux distributions de probabilité $P = (p_0, p_1, \dots, p_{K-1})$ et $Q = (q_0, q_1, \dots, q_{K-1})$, avec $p_i \geq 0$, $q_i \geq 0$ est défini par [90]:

$$\chi^2(P||Q) = \sum_{i=0}^{K-1} \frac{(p_i - q_i)^2}{q_i}$$

Avec $p_i \geq 0$, $q_i \geq 0$ et :

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1$$

Où *Q* est la distribution de probabilité d'avant et *P* la distribution actuelle. La divergence de χ^2 peut prendre des valeurs de zéro jusqu'à l'infini.

$\chi^2(P||Q) = 0$ si et seulement si $P = Q$ et sa valeur augmente si les deux distributions deviennent dissemblables, jusqu'à l'infini lorsque les deux distributions sont indépendante. Il est important de noter que la divergence de χ^2est asymétrique, où elle génère un seul pic au début de l'attaque. La division 0 / 0 dans l'équation est considérée comme 0, et la division par zéro est remplacée par une très faible valeur ϵ. La divergence de χ^2 entre deux distributions de probabilité *P* et *Q* doit être proche de zéro avec un trafic normal, et elle doit avoir un pic lorsqu'un changement de distribution de probabilité se produit.

3.3. Kullback-Leibler Divergence (KLD)

Kullback-Leibler Divergence est une équation fondamentale de la théorie de l'information et est utilisée pour calculer la divergence entre deux ensembles de valeurs de probabilité $P = (p_0, p_1, \dots, p_{K-1})$ et $Q = (q_0, q_1, \dots, q_{K-1})$ avec $p_i \geq 0$, $q_i \geq 0$ et:

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1$$

KLD entre P et Q est défini par [91]:

$$KLD(P||Q) = \sum_{i=0}^{K-1} pi\ ln\frac{p_i}{q_i}$$

$KLD(P||Q) \geq 0$, KLD est non symétrique c.à.d. KLD entre P et Q est généralement différent de KLD entre Q et P. *Kullback-Leibler Divergence* est égale à zéro si les deux distributions correspondent exactement.

3.4. Jensen-Shannon Divergence (JSD)

Jensen-Shannon Divergence est utilisée pour calculer la divergence entre deux ensembles de valeurs de probabilité $P = (p_0, p_1, \dots, p_{K-1})$ et $Q = (q_0, q_1, \dots, q_{K-1})$ avec $p_i \geq 0$, $q_i \geq 0$ et:

$$\sum_{i=0}^{K-1} p_i = \sum_{i=0}^{K-1} q_i = 1$$

JSD est une version lissée de *Kullback-Leibler Divergence* [88] et est définie comme suit :

$$JSD(P,Q) = \frac{1}{2}KL(P,M) + \frac{1}{2}KL(Q,M)$$

Avec M est la distribution moyenne de P et Q.

$$M = \frac{P+Q}{2}$$

D'où JSD peut être exprimée sous la forme suivante [91] :

$$JSD(P||Q) = \frac{1}{2}\left[\sum_{i=0}^{K-1} p_i \ln\left(\frac{2p_i}{p_i+q_i}\right) + \sum_{i=0}^{K-1} q_i \ln\left(\frac{2q_i}{p_i+q_i}\right)\right]$$

JSD = 0 si et seulement si P et Q sont identiques ($p_i = q_i$), et JSD > 0 lorsque P ≠Q. Comme nous cherchons à détecter les anomalies grâce à la détection des déviations du trafic normal, JSD détermine la divergence entre deux distributions de probabilité P et Q, qui désignent les distributions avant et après l'attaque. JSD entre P et Q doit être proche de zéro dans le cas de trafic normal, avec une grande déviation (une pointe) lorsque les distributions subissent un changement.

3.5. Notre proposition Power Divergence (PD)

Nous proposons une nouvelle approche de mesure de divergence pour la détection des attaques SYN flooding. L'approche proposée vise à détecter les attaques de faible intensité dans le trafic des réseaux IP. Power Divergence a été défini dans [92], [93], [94] et [100]. Power Divergence généralise les méthodes *Kullback-Leibler Divergence*, *Hellinger Distance* et *Chi-square Divergence* à une large classe de divergence par la variation de la valeur du paramètre β. *Power Divergence* est définie par :

$$PD(P||Q) = \frac{\sum_{i=0}^{K-1} p_i\left({}^{p_i}/_{q_i}\right)^{\beta-1} - 1}{\beta(\beta-1)}$$

PD = 0 si et seulement si P et Q sont identiques ($p_i = q_i$), et PD > 0 lorsque P ≠Q. PD entre P et Q doit être proche de zéro dans le trafic normal, avec une grande déviation (une pointe) lorsque les distributions subissent un changement.

Power Divergence présente quelques cas particuliers intéressants en changeant la valeur du paramètre β, ces cas particulier sont résumés dans le Tableau 32. En effet, pour β=0.5, cette divergence est proportionnelle à *Hellinger Distance* entre P et Q, tandis que pour β = 1, PD est égal à *Kullback-Leibler Divergence*. De plus, pour β = 2, elle est proportionnelle *Chi-square Divergence*. En fait, en changeant la valeur de β, nous pouvons optimiser la détection des attaques par rapport à *Kullback-Leibler Divergence*, *Hellinger Distance* et *Chi-square Divergence*. Dans les résultats expérimentaux, nous montrerons numériquement que pour différentes valeurs de β, l'efficacité de la détection des attaques subit un changement.

β	$PD(P\|\|Q) =$
-1	$\frac{1}{2} \times \chi^2(Q\|\|P)$
0	$KLD(Q\|\|P)$
0.5	$4 \times HD(P,Q)$
1	$KLD(P\|\|Q)$
2	$\frac{1}{2} \times \chi^2(P\|\|Q)$

Tableau 32 Cas particulier de Power Divergence

4. L'attaque SYN *flooding* dans les réseaux IP

Pour défendre contre les attaques de type SYN *flooding* dans un système de surveillance médicale à distance, la première étape consiste à détecter l'existence de cette attaque. La Figure 48 représente le système étudié où nous avons un serveur personnel qui va envoyer les données collectées par les capteurs médicaux à l'équipe médicale via un réseau Internet. Puis nous allons injecter des attaques de type SYN f*looding* sur une communication de paquets dans ce réseau. Par la suite, nous allons détecter ces attaques par les méthodes de mesure de divergence.

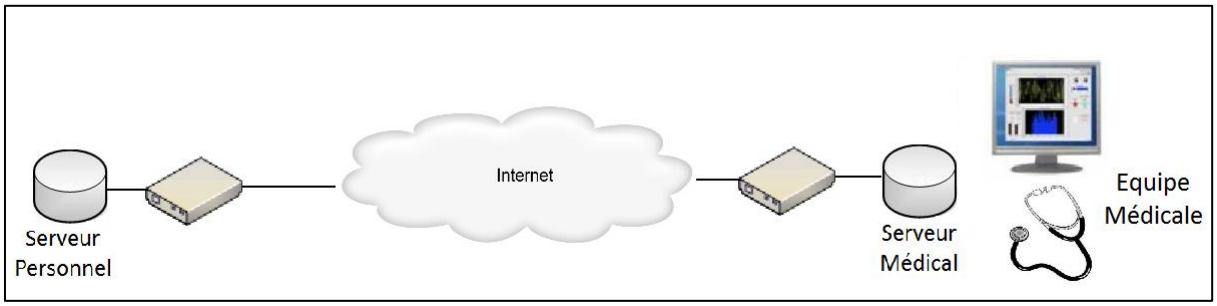


Figure 48 Envoie des données collectées par les capteurs à l'équipe médicale via un réseau Internet

4.1. Détection des attaques *SYN flooding* dans les réseaux IP

La détection des attaques de type déni de service et plus particulièrement le *flooding* a été un travail intéressant pour les chercheurs en sécurité. Les méthodes proposées sont basées sur différentes techniques qui utilisent la détection de déviation. Parmi ces méthodes nous citons : l'analyse par ondelettes [85], la méthode de l'entropie [102], CUmulative SUM (CUSUM) algorithm ([87], [101]), adaptive threshold [103], Exponentially Weighted Moving Average (EWMA) [104] et SNMP (*Simple* Network Management Protocol) MIB *statistical data analysis* [105].

La plupart des travaux de recherche existants qui traitent le sujet de détection des attaques de type *flooding* agrègent l'ensemble du trafic dans une série chronologique, et appliquent des algorithmes de détection de déviation pour détecter l'instant d'apparition de l'anomalie. Ces algorithmes ont une bonne performance en termes de complexité spatiale et temporelle, mais présentent l'inconvénient d'agréger l'ensemble du trafic dans un flux, où les attaques de faible intensité ne peuvent être détectées et les variations normales du trafic soulèvent des fausses alarmes.

En réponse à ces problèmes, la structure de données *Sketch* utilise l'agrégation aléatoire pour une analyse plus efficace que l'agrégation du trafic tout en un seul flux. *Sketch* a été utilisé pour résumer le trafic surveillé dans une mémoire fixe, et pour apporter une contribution évolutive pour l'analyse des séries chronologiques.

Dans la section suivante, nous allons présenter la structure de données Sketch que nous utiliserons dans notre algorithme.

4.2. Structure de données Sketch

La structure de données Sketch ([85], [87], [90]) est utilisée pour la réduction de la dimensionnalité. Elle est basée sur l'agrégation aléatoire du trafic attribut (par exemple nombre de paquets) dans différentes tables de hachage.

Un Sketch S est un tableau à deux dimensions de $H \times K$ cellules (comme le montre la Figure 49), où K est la taille de la table de hachage, et H est le nombre de fonctions de hachage indépendantes (fonctions de hachage universel). Chaque élément est identifié par une clé κ_n et associé à une valeur v_n.

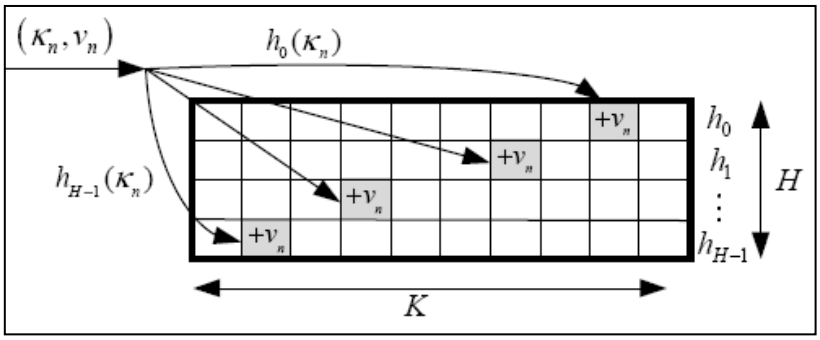


Figure 49 Structure de données Sketch

Pour chaque nouveau élément(κ_n, v_n), la valeur associée sera ajoutée à la cellule $S[i][j]$, où *i* est un indice utilisé pour représenter la fonction de hachage associée à l'*i*ème table de hachage *(0 ≤ i ≤ H-1)* et *j* est la valeur de hachage *(j = $hash_i(\kappa_n)$)* de la clé pour l'*i*ème fonction de hachage. Dans notre application, le couplet (k_n, v_n) = (DIP, 1) où κ_n représente l'adresse IP de destination (DIP : Destination IP) de chaque paquet qui contient un segment SYN.

Les éléments dont les clés sont hachées à la même valeur seront regroupés dans la même cellule dans la table de hachage, et leurs valeurs ($v_n = 1$) seront ajoutées au compteur dans la table de hachage. Chaque table de hachage est utilisée pour calculer la distribution de probabilité dans chaque cellule en divisant le nombre contenu dans la cellule par la somme des nombres contenus dans toutes les cellules de la ligne. Les distributions de probabilité dérivée sont utilisées comme entrées pour les mesures de divergence.

L'algorithme suivant représente la procédure de mise à jour du *Sketch*.

Algorithme 1: Sketch Update procedure.

For all TCP SYN segment received during T **do**
  For $i = 0\ to\ H - 1$ **do**
    $j = univ\_hash_i(DIP)$;
    $S[i][j].counter+ = v_n$;
  End for
End for

4.3. Architecture du système de détection et son fonctionnement

Pour appliquer les mesures de divergence, nous utilisons *K-ary Sketch* afin de tirer les distributions de probabilités. Nous allons décrire dans la suite l'architecture du système utilisé ainsi que son fonctionnement.

Le temps est divisé en des intervalles de temps discrètes (T = 1 minute), l'adresse IP de destination (DIP) pour chaque paquet qui contient un segment SYN est hachée par une fonction de hachage [97] $(j = hash_i(DIP))$. La valeur résultante est utilisée comme indice de la case où il faut incrémenter son compteur. En fait, la case est partagée avec des adresses de destination au hasard, parce que de nombreux DIP peuvent avoir la même valeur de hachage, et de partager la même case dans *Sketch*. Chaque nouveau segment SYN associé à une case incrémente son compteur. A la fin de chaque intervalle T, nous dérivons les distributions de probabilité à partir de *Sketch*. En fait, la distribution de probabilité pour chaque cellule du sketch S_{ij} est calculée en divisant son compteur par la somme de tous les compteurs de la ligne :

$$p_{ij} = S_{ij}.Counter / \sum_{j=0}^{K-1} S_{ij}.Counter$$

Chaque ligne (ou table de hachage) fournit deux distributions de probabilité. La première Q_i est de l'intervalle précédent et est utilisée comme distribution de référence. La deuxième P_i est de l'intervalle courant, et est utilisée pour mesurer la divergence par rapport à la distribution de référence afin de détecter les anomalies. La divergence entre la probabilité de distribution courante (P_i) et la probabilité de référence (Q_i) est calculée pour chaque ligne dans *Sketch* à la fin de chaque intervalle de temps. Au cours d'une attaque, la mesure de la divergence $D(P_i||Q_i)$ produit un pic.

Lorsque $'L'$ valeurs consécutives de la mesure de divergence $D(P_i||Q_i)$ sont plus élevées par rapport à un seuil dynamiquement mis à jour, nous déclenchons une alarme, et cela pour réduire les fausses alarmes. Par conséquence, nous allons déclencher une alarme seulement si l'écart dure plus de η intervalles.

4.4. Calcul du seuil

Pour détecter les déviations dans la série temporelle résultante des mesures de divergence, une phase d'apprentissage est nécessaire dans laquelle nous supposons qu'il n'y a pas une présence d'attaque (condition normale). Nous tirons une suite de série temporelle contenant des valeurs de $D(P_i||Q_i)$ dans ces conditions normales. A partir de cette série, nous définissons un seuil de: $\mu_i + 3\sigma_i$ où 99% des valeurs normales se trouvent au-dessous de ce seuil. Avec $D(P_i||Q_i)$ est la mesure de divergence dans l'intervalle de temps nT pour la ième ligne dans *Sketch*, μ_i et σ_i sont respectivement la valeur moyenne et l'écart type des séries temporelles de $D(P_i||Q_i)$ qui ne contiennent pas d'attaques.

A chaque période T, lorsque la valeur de mesure de divergence dépasse ce seuil ($D(P_i||Q_i) > \mu_i + 3\sigma_i$), cela veut dire qu'on est dans le cas d'une attaque. Les paramètres μ_i et σ_i sont mis à jour dynamiquement en ajoutant les nouvelles valeurs de $D(P_i||Q_i)$ qui sont au-dessous du seuil dans le calcul des nouvelles valeurs de μ_i et σ_i

La valeur de $D(P_i||Q_i)$ est au-dessous du seuil dans le cas du trafic normal tandis qu'elle est au-dessus du seuil dans le cas d'une attaque.

Afin de réduire le nombre des fausses alarmes dues aux variations normales du trafic, $D(P_i||Q_i)$ doit dépasser le seuil dynamique pour η intervalles consécutifs avant de déclencher une alarme. La fonction qui décide le déclenchement des alarmes est donnée par l'équation suivante :

$$d(Alarme_i) = \begin{cases} 1 \; si \; D(P_i||Q_i) \geq \mu_i + 3\sigma_i \; et \; \eta \geq 3 \\ 0 \qquad\qquad\qquad\qquad\qquad ailleurs \end{cases}$$

5. Applications sur des traces d'un trafic Internet

Maintenant, pour appliquer les algorithmes de divergence cités ci-dessus et faire une comparaison au niveau des performances de détection d'anomalies, nous allons utiliser des traces collectées d'un trafic internet entre le Japon et les Etats Unis [96] d'une durée totale de 8h30 (510 minutes) entre 7h30 et 16h00. Nous allons concentrer notre analyse sur la détection des attaques de type TCP *SYN Flooding*, puisque c'est l'attaque de déni de service (DoS) la plus utilisée ces jours-ci.

Nous avons analysé ces traces du réseau internet en utilisant *Sketch* avec $\kappa_n = DIP\ et\ \nu_n = 1$ pour les requêtes SYN seulement. Les paramètres utilisés dans notre mise en œuvre sont: $K = 1024,\ H = 5, \eta = 3\ et\ L = 3$.

L'effet des paramètres de *Sketch* (largeur et profondeur) sur la capacité de détection a été analysé dans [95]. Les auteurs présentent une analyse détaillée de l'impact du nombre de fonctions de hachage (H) et la largeur de *Sketch* (K) sur la précision de la détection. Ils ont constaté que *Sketch* offre une meilleure précision de détection en augmentant H et K, mais cela nécessite une augmentation de la mémoire nécessaire et conduit à une complexité de calcul.

Ensuite, nous avons injecté douze (12) attaques de type DDoS TCP SYN *flooding* avec des intensités différentes. Ces attaques sont insérées toutes les 30 minutes avec une durée de 10 minutes pour chaque attaque. Ces attaques sont représentées sur la Figure 50. La première attaque commence avec une valeur de 10000 SYN/min et diminue d'une façon exponentielle jusqu'à 3200 SYN/min pour la dernière attaque.

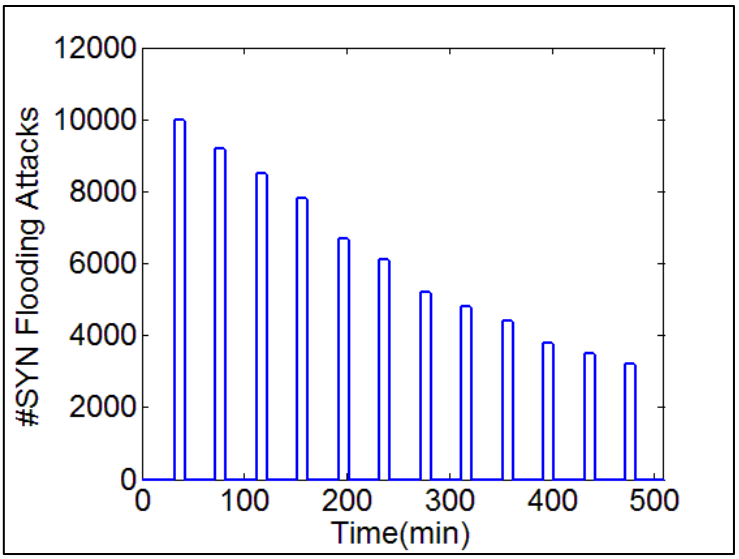


Figure 50 Les attaques injectées

Nous analysons les traces avant et après l'injection des attaques. La Figure 51 montre la variation du nombre total des paquets avant et après l'injection des attaques SYN *flooding*. En comparant ces variations, nous ne trouvons pas de différence entre les deux figures, ce qui signifie que les attaques insérées n'ont pas provoqués des grandes déviations dans la série temporelle du nombre total des paquets.

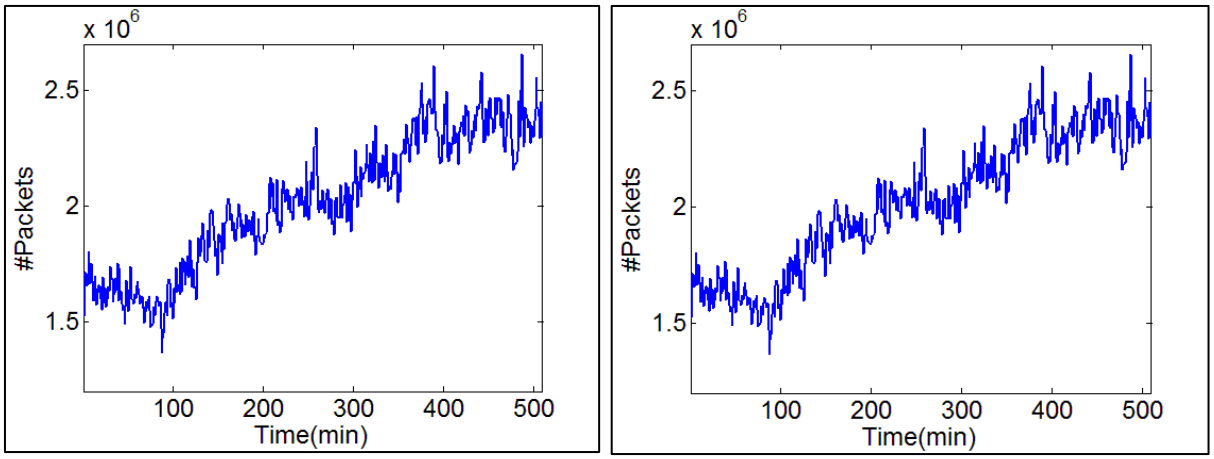


Figure 51 Nombre total de paquets avant l'injection des attaques (à gauche) et après l'injection des attaques (à droite)

La Figure 52 montre la variation du nombre total des segments TCP avant et après les attaques SYN *flooding*. Nous pouvons remarquer que la forme du trafic dans les deux figures est similaire. Cela peut s'expliquer par le fait que l'intensité des attaques SYN *flooding* est beaucoup plus petite par rapport à l'intensité de nombre total des paquets et du nombre total des segments TCP. Dans ce cas, la détection des attaques sera un vrai challenge.

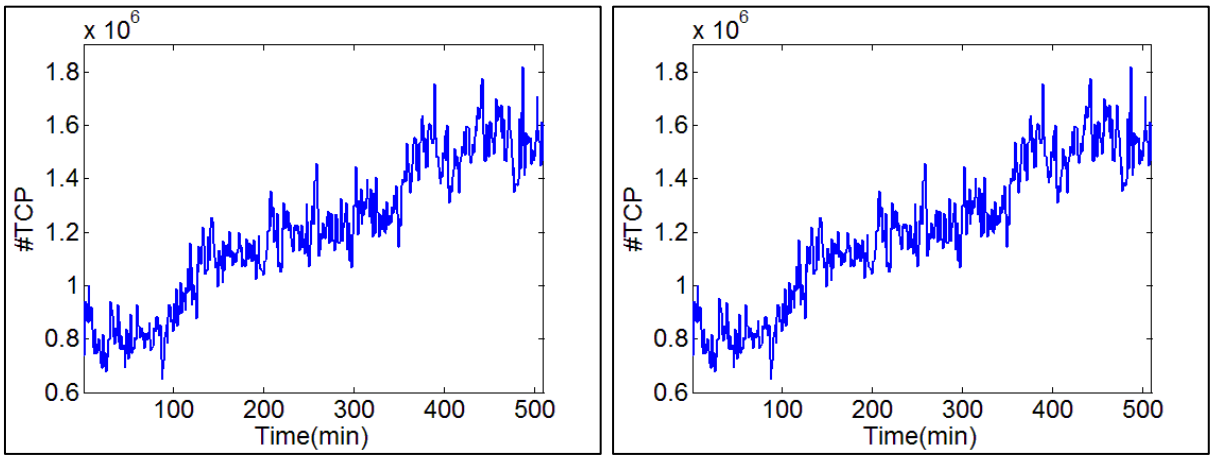


Figure 52 Nombre total de segments TCP avant l'injection des attaques (à gauche) et après l'injection des attaques (à droite)

La Figure 53 montre la variation du nombre de SYN avant et après l'injection des attaques SYN flooding. En fait, nous pouvons remarquer les grandes variations dans le nombre total de SYN avant l'injection des attaques (figure à gauche). Par conséquence, l'agrégation de l'ensemble du trafic dans une série temporelle produit beaucoup de fausses alarmes pour ces

grandes déviations. D'autre part, l'injection des attaques SYN flooding a produit des petites variations dans le nombre de SYN (figure à droite).

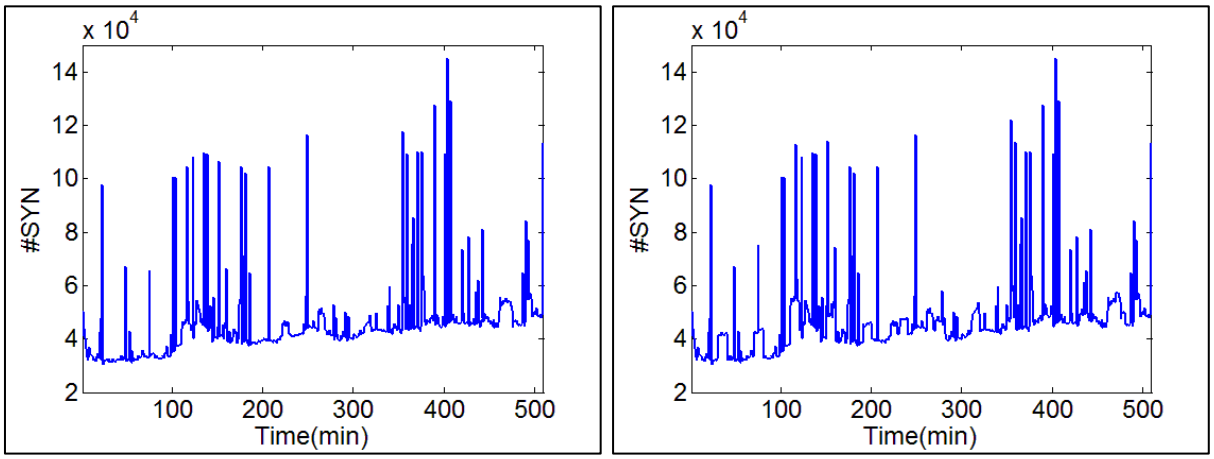


Figure 53 Nombre de SYN avant l'injection des attaques (à gauche) et après l'injection des attaques (à droite)

5.1. Résultats expérimentaux

Nous avons mené de nombreuses expériences en faisant varier la valeur de β afin de prouver que HD, KLD, CSD sont des cas particuliers de PD et pour trouver la valeur optimale de β. Nous présentons la variation de toutes les mesures de divergence citées dans la section 3.2, avec le seuil dynamique sur tout le trafic qui contient des attaques à des intensités variables.

La Figure 54 présente la variation de PD pour β=0.5 (figure à droite) et la variation de HD (figure à gauche). Nous pouvons remarquer en comparant ces deux figures que: $PD = 4 \times HD$.

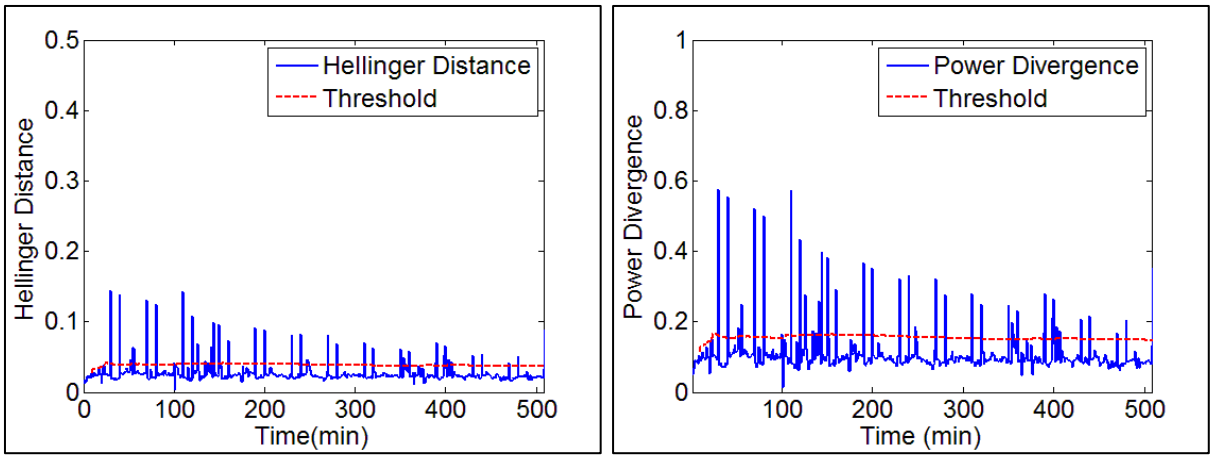


Figure 54 Hellinger Distance (à gauche) et Power Divergence pour β=0.5 (à droite)

La Figure 55 présente la variation de PD pour β=1 (figure à droite) et la variation de KLD (figure à gauche). Nous pouvons remarquer en comparant ces deux figures que: $PD = KLD$.

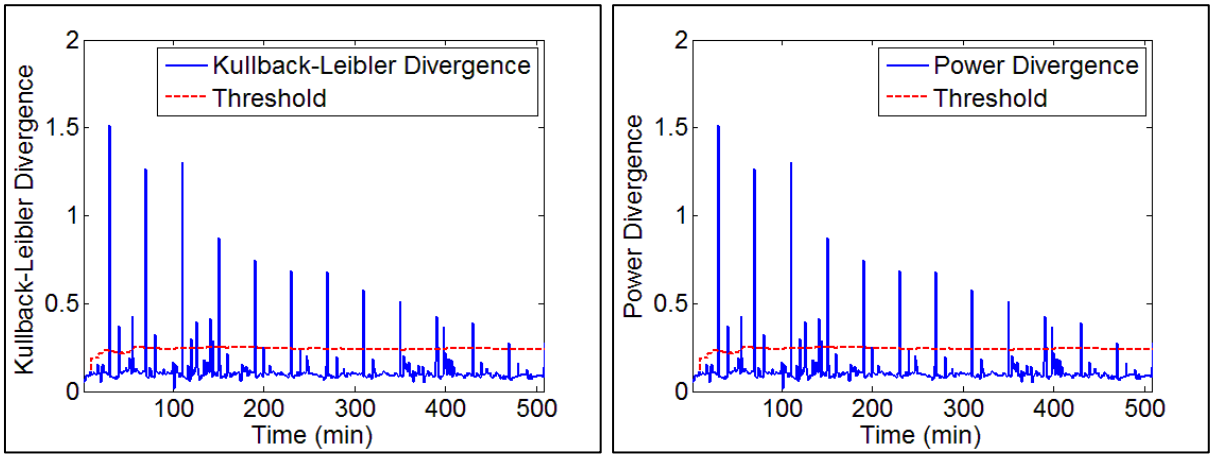


Figure 55 Kullback-Leibler Divergence (à gauche) et Power Divergence pour β=1 (à droite)

La Figure 56 présente la variation de PD pour β=2 (figure à droite) et la variation de CSD (figure à gauche). Nous pouvons remarquer en comparant ces deux figures que: $PD = \frac{1}{2} \times CSD$.

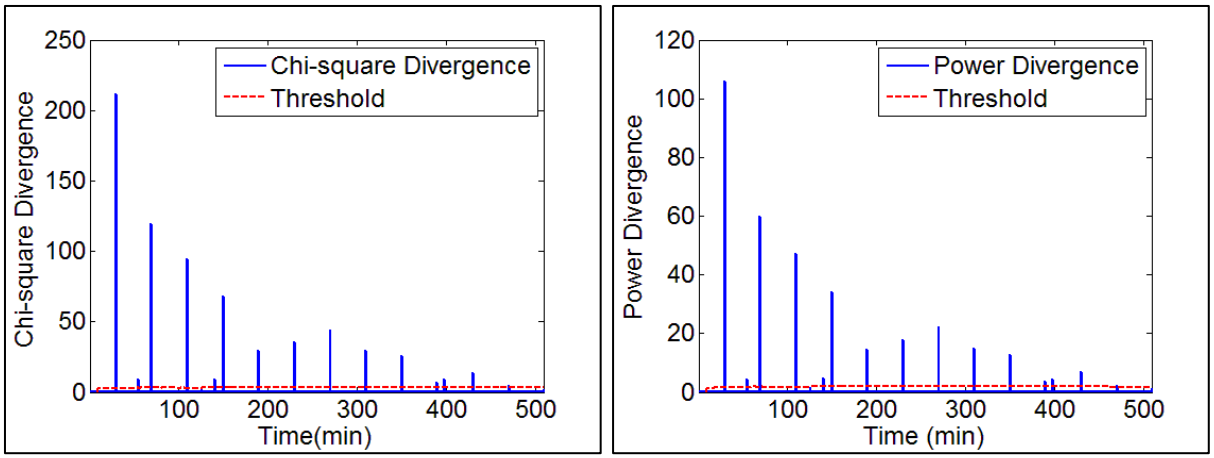


Figure 56 Chi-square Divergence (à gauche) et Power Divergence pour β=2 (à droite)

La Figure 57 présente la variation de PD pour β=1.5 (à gauche) et la variation de PD pour β=2.5 (à droite). Et finalement la Figure 58 présente la variation de JSD.

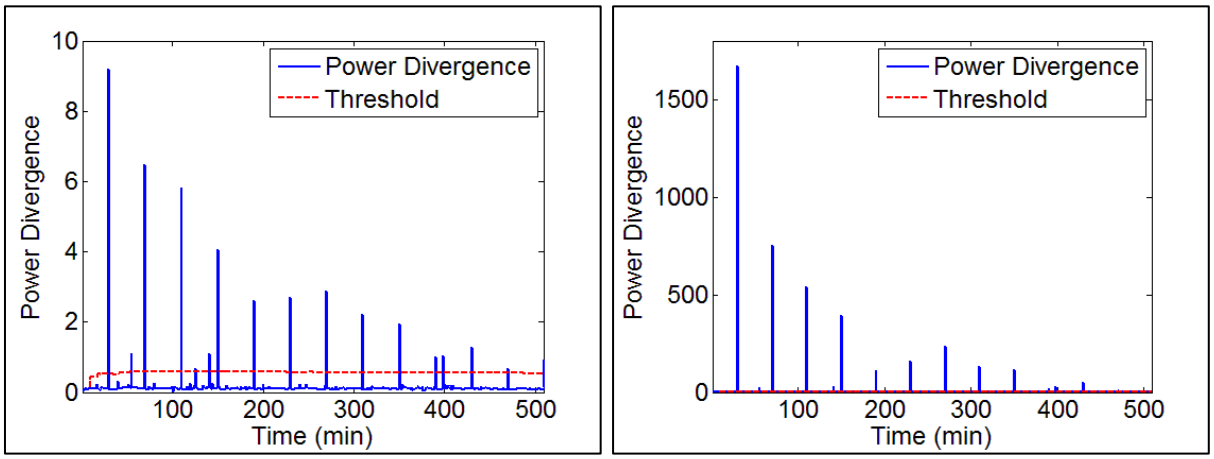


Figure 57 Power Divergence pour β=1.5 (à gauche) et Power Divergence pour β=2.5 (à droite)

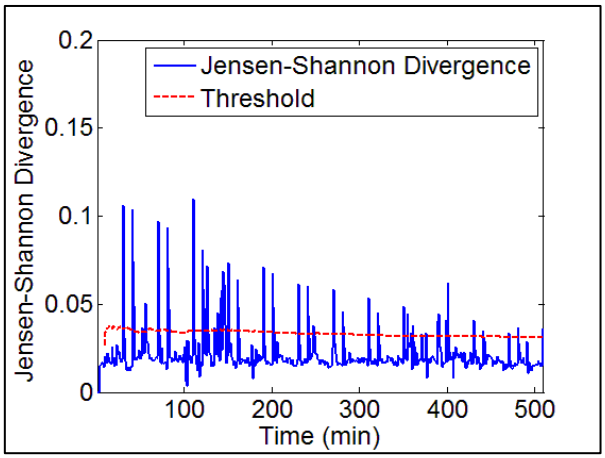


Figure 58 Jensen-Shannon Divergence

Dans toutes les figures, à chaque instant où la valeur de mesure de divergence dépasse le seuil dynamique, une alarme est déclenchée. Il est important de noter la différence d'échelle entre les figures, où l'intensité de pic augmente lorsque nous augmentons la valeur de β. Donc nous n'utilisons pas la même échelle pour des raisons de clarté.

5.2. Evaluation des performances

Pour évaluer les performances et faire une comparaison entre les différentes méthodes de mesure de divergence présentées dans ce chapitre, nous calculons le taux de détection et le taux de fausses alarmes pour analyser la capacité de détection d'attaques pour chacune de ces méthodes.

Afin de présenter les résultats sous forme d'un graphique, nous utilisons la courbe ROC (*Receiver Operating Characteristic*) qui est une mesure de la performance d'un système qui a pour objectif de catégoriser des entités en deux groupes distincts. Graphiquement, on représente la mesure ROC sous la forme d'une courbe qui donne le taux de vrais positifs (dans notre cas, le taux de vrais positifs représente le taux des attaques qui sont détectées correctement) en fonction du taux de faux positifs (dans notre cas, le taux de faux positifs représente le taux de fausses détections).

La courbe ROC va montrer la variation du taux de détection en fonction du taux de fausses alarmes et cela en variant la valeur du seuil.

Le taux de détection (DR : *Detection Rate*) est le rapport entre le nombre des attaques détectées et le nombre total d'attaques existantes, DR est défini comme suit :

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

Par contre, le taux de fausses alarmes ou fausses détections (FAR: *False Alarm Rate*) est le rapport entre le nombre de fausses détections et le nombre total de détections. FAR est défini comme suit :

$$FAR = \frac{Nombre\ de\ fausses\ détections}{Nombre\ total\ de\ détections} \times 100$$

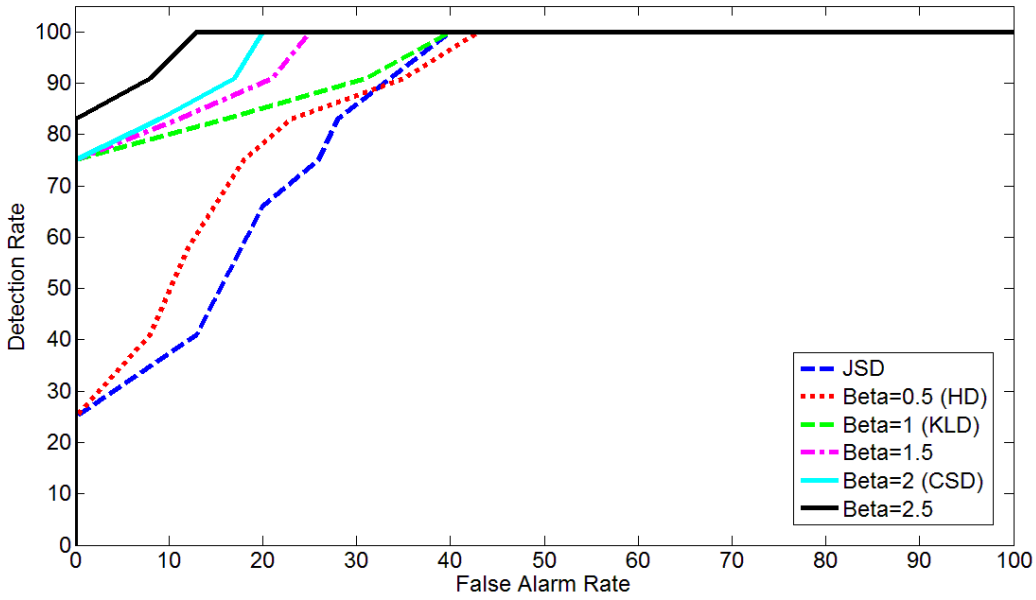


Figure 59 Courbe ROC

Dans la Figure 59, nous présentons la courbe ROC pour les différentes mesures de divergence. Nous pouvons conclure de cette courbe que :

-Pour β=0.5 ($PD = 4 \times HD$) : avec un taux de détection DR=100%, nous avons FAR= 43%. Et pour un FAR=0%, nous avons DR=25%.

-Pour β=1 ($PD = KLD$) : avec un taux de détection DR=100%, nous avons FAR= 40%. Et pour FAR=0%, nous avons DR=75%.

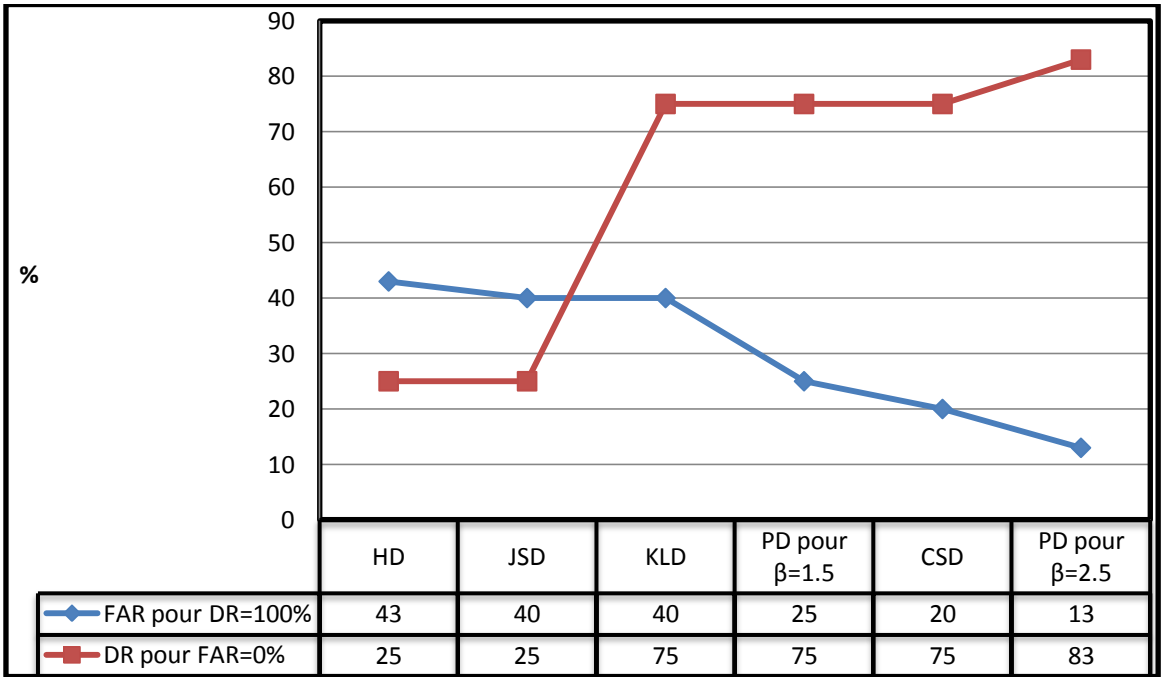
-Pour β=1.5 : avec un taux de détection DR=100%, nous avons FAR= 25%. Et pour FAR=0%, nous avons DR=75%.

-Pour β=2 ($PD = \frac{1}{2} \times CSD$) : avec un taux de détection DR=100%, nous avons FAR= 20%. Et pour FAR=0%, nous avons DR=75%.

-Pour β=2.5 : avec un taux de détection DR=100%, nous avons FAR= 13%. Et pour FAR=0%, nous avons DR=83%.

-Et pour JSD : avec un taux de détection DR=100%, nous avons FAR=40%. Et pour FAR=0%, nous avons DR=25%.

La Figure 60 résume les résultats obtenus :



	HD	JSD	KLD	PD pour β=1.5	CSD	PD pour β=2.5
FAR pour DR=100%	43	40	40	25	20	13
DR pour FAR=0%	25	25	75	75	75	83

Figure 60 Taux de Détection et Taux de Fausse Alarme

5.2.1. Discussion

Nous pouvons conclure des résultats obtenus que pour un taux de détection DR=100%, lorsque nous augmentons la valeur de β, le taux de fausses alarmes (FAR) diminue. Et pour un taux de fausses alarmes FAR=0%, en augmentant la valeur de β, le taux de détection (DR) augmente.

Il est important de noter que nous avons mené de nombreuses expériences avec des valeurs différentes de β, avec un pas de 0.5. Nous avons constaté à travers ces expériences qu'avec une valeur de β ≥2.5, l'intensité de PD pour la détection des attaques augmente

significativement et proportionnellement à l'intensité de l'attaque, mais sans aucun changement dans la courbe ROC.

Par conséquence, la méthode *Power Divergence* avec une valeur de $\beta = 2.5$, surpasse les mesures de divergence existantes et permet d'atteindre des performances optimales. Donc nous recommandons une valeur de $\beta=2.5$ en tant que valeur optimale pour *Power Divergence.*

6. Conclusion

Dans ce chapitre, nous avons traité les attaques de type déni de service qui peuvent être dangereuses pour la communication des informations physiologiques via un réseau IP, dans un système de surveillance médicale à distance.

Nous avons proposé une nouvelle approche basée sur la structure de donnée « *Sketch »* et la méthode de mesure de divergence « *Power Divergence* (PD) » pour la détection des attaques *SYN flooding* (qui sont des attaques de type déni de service) dans les réseaux IP. L'approche proposée a été évaluée sur des traces réelles avec des attaques *SYN flooding*. Les résultats ont montré la capacité du *Power Divergence* dans la détection des attaques de faible intensité. Nous avons présenté les résultats de *Power Divergence* avec différentes valeurs du paramètre β, et nous avons pu montrer les cas spéciaux de Power Divergence présentés dans le Tableau 32.

Enfin, nous avons dessiné la courbe ROC associée à chaque valeur de β lorsqu'on fait varier le seuil. Nous avons prouvé que *Power Divergence* est plus performant par rapport aux mesures existantes (HD, KLD, JSD et χ^2) et cela lorsqu'on augmente la valeur du paramètre β. Finalement, nous avons constaté que pour une valeur de $\beta = 2.5$, PD atteint une performance optimale avec un taux de détection maximal et un taux de fausses alarmes minimal.

Chapitre VI : Conclusion générale et Perspectives

1. Conclusion générale

Les réseaux de capteurs sans fil s'ouvrent à une multitude de domaines d'applications. Chaque application à ses propres contraintes et exigences. Ce travail de thèse avait pour objectif d'apporter des solutions liées à la détection des attaques dans les systèmes WBAN (*Wireless Body Area Networks*) de surveillance médicale à distance.

Cette thèse a débuté par une étude générale sur les réseaux de capteurs sans fils médicaux, en présentant les différents types de capteurs médicaux et leurs fonctions, ainsi que l'architecture des nœuds capteurs, leurs caractéristiques et les systèmes d'exploitation qui gèrent ces capteurs. Ainsi nous avons fait une comparaison entre les réseaux WBAN et les réseaux WSN en termes de déploiement, nombre de capteurs, débit des données, mobilité, etc. Nous avons présenté les sous-systèmes constituant un système WBAN de surveillance médicale à distance et l'architecture des communications dans ce système. Nous avons fait une comparaison entre les protocoles de communications sans fil qui peuvent être utilisés dans les communications intra-BAN et inter-BAN selon plusieurs critères (consommation d'énergie, débit, durée de vie de la pile, la portée maximale, le nombre de nœuds supportés, etc.), et nous avons présenté les topologies les plus utilisées pour le déploiement des réseaux WBAN. Cette partie a compris encore une discussion sur les principaux avantages apportés par les systèmes WBAN dans le domaine médical et leurs applications dans le domaine de la surveillance médicale. Nous avons terminé cette étude générale en présentant les principaux exigences et défis pour les systèmes WBAN.

Dans la deuxième partie, nous avons traité le défi de sécurité dans les systèmes WBAN qui est l'objectif de cette thèse. Nous avons décrit les différents types d'attaques potentielles dans un système WBAN de surveillance médicale à distance et nous les avons classés selon la cible qu'ils visent. Puis, nous avons décrit les anomalies possibles dans les réseaux de capteurs sans fils d'un système WBAN et nous les avons classées en trois classes : anomalies de réseaux,

anomalies des nœuds et anomalies de données. Ensuite, nous avons focalisé notre travail sur l'attaque de brouillage radio (*jamming*) où nous avons fait un état de l'art sur les travaux de recherche concernant la détection de cette attaque dans les réseaux sans fils et nous avons fait une étude comparative entre ces méthodes selon plusieurs critères. Enfin, nous avons présenté quelques solutions proposées pour se défendre contre ce type d'attaque dans les réseaux sans fil.

Ensuite nous avons passé à la partie concernant notre propre contribution, qui est décomposée en deux chapitres.

Dans le premier chapitre, nous avons proposé une méthode pour détecter l'attaque de brouillage radio (*jamming*) dans un réseau de capteurs corporels sans fil (WBAN: *Wireless Body Area Network*). Dans ce chapitre, nous avons présenté quatre types de *jamming* et nous avons décri l'influence de ces types de *jamming* sur les valeurs de plusieurs paramètres réseau (PDR, BPR, ECA, PSR et RSSI) que nous avons utilisés dans notre algorithme pour détecter la présence de *jamming* et pour identifier son type. Nous avons appliqué notre algorithme et nous l'avons comparé avec deux autres propositions. Les résultats obtenus ont montré que notre proposition est plus performante et plus efficace. Nous avons montré aussi la relation entre le débit de données dans le réseau et le choix de la période d'échantillonnage « Te » et l'influence de cette dernière sur le taux de détection et l'efficacité de l'algorithme.

Dans le deuxième chapitre, nous avons proposé une méthode de mesure de divergence pour détecter les attaques de SYN flooding dans le réseau IP qui relie le réseau des capteurs au centre de surveillance. Cette méthode de mesure de divergence « *Power Divergence* » est basée sur une approche statistique. Nous avons utilisé la structure de donnée « *Sketch »* qui a le rôle de l'agrégation aléatoire du trafic attribut (nombre de paquets SYN dans notre cas) dans différentes tables de hachage. L'approche proposée a été évaluée sur des traces réelles avec des attaques *SYN flooding*. Les résultats ont montré la capacité du *Power Divergence* à détecter les attaques de faible intensité. Nous avons présenté les résultats de *Power Divergence* avec différentes valeurs du paramètre β et nous avons pu montrer les cas spéciaux de *Power Divergence*. Enfin, nous avons évalué les performances de *Power Divergence* et nous l'avons comparé aux autres méthodes de mesure de divergence et cela en calculant le taux de détection et le taux de fausses alarme. Nous avons trouvé la valeur optimale de β qui permet à *Power Divergence* d'atteindre des performances optimales avec un taux de détection maximal et un taux de fausses alarmes minimal.

2. Perspectives

Dans cette thèse nous avons proposé une méthode pour détecter l'attaque de brouillage radio (*Jamming*) dans un réseau de capteurs médicaux sans fil. Cette méthode est basée sur la mesure de la valeur de plusieurs paramètres du réseau à chaque période Te. Les valeurs de ces paramètres sont en relation directe avec l'état du réseau. Nous avons appliqué notre méthode proposée sur un réseau simulé, mais la solution idéale reste toujours d'expérimenter ces méthodes sur une plate-forme réelle de capteurs.

La détection de n'importe quel type d'attaque dans le domaine des réseaux est la première étape pour se défendre contre cette attaque. Nous avons proposé dans cette thèse une méthode pour détecter l'attaque de *jamming* dans les réseaux WBAN. Il serait intéressant de travailler à l'élaboration d'une solution pour défendre contre les attaques de *jamming*.

Dans cette thèse, nous avons aussi proposé une méthode de mesure de divergence pour détecter les attaques de type *flooding* dans les réseaux internet d'un système WBAN de surveillance médicale à distance. Nous avons utilisé des traces réelles avec une période d'échantillonnage T = 1 minute. Nous proposons d'étudier l'effet de la période d'échantillonnage sur la précision de la détection des attaques et cela en utilisant plusieurs valeurs pour cette période d'échantillonnage. Cette étude permettra de trouver la valeur optimale de T. Cette valeur optimale est la valeur qui diminue le temps nécessaire pour détecter l'attaque et qui permet d'avoir un taux de détection très élevé et un taux de fausses détections très réduit.

Finalement, Il serait également intéressant de travailler sur d'autres types d'attaques potentielles dans les systèmes WBAN parmi les attaques que nous avons présentées dans la section 2.2 du Chapitre III.

Liste des Acronymes

WSN: Wireless Sensor Network

RCSF: Réseaux de Capteurs Sans Fil

WBAN: Wireless Body Area Network

OS: Operating System

RAM: Random Access Memory

BAN: Body Area Network

PAN: Personal Area Network

WAN: Wide Area Network

RFID: Radio Frequency Identification

PDA: Personal Digital Assistant

UWB: Ultra Wide Band

WMSN: Wireless Multimedia Sensor Networks

DSSS: Direct Sequence Spread Spectrum

FHSS: Frequency Hopping Spread Spectrum

ISM: Industrial Scientific and Medical

NB: Narrow Band

HBC: Human Body Communication

MAC: Medium Access Control

WLAN: Wireless Local Area Network

ECG: ElectroCardioGraphie

EEG: ElectroEncéphaloGraphie

EMG: ElectroMyoGramme

GPRS: General Packet Radio Service

UMTS: Universal Mobile Telecommunications System

CPU: Central Processing Unit

DoS: Denial of Service

PC: Personal Computer

PDR: Packet Delivery Ratio

BPR: Bad Packet Ratio

PSR: Packet Send Ratio

BER: Bit Error Rate

ECA: Energy Consumption Amount

CST: Carrier Sensing Time

CSMA: Carrier Sense Multiple Access

RSSI: Received Signal Strength Indicator

SNR: Signal-to-Noise Ratio

RTS: Request To Send

CTS: Clear To Send

ACK: Acknowledgement

LCL: Lower Control Limit

UCL: Upper Control Limit

DR: Detection Rate

FAR: False Alarm Rate

TCP: Transmission Control Protocol

ICMP: Internet Control Message Protocol

IP: Internet Protocol

DDoS: Distributed Denial of Service

KLD: Kullback-Leibler Divergence

HD: Hellinger Distance

CSD: Chi-Square Divergence

JSD: Jensen-Shannon Divergence

PD: Power Divergence

DIP: Destination IP

ROC: Receiver Operating Characteristic

Bibliographie

[1] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao and Victor C. M. Leung, "Body Area Networks: A Survey", *Mob. Netw. Appl. Journal*, pages: 171-193, April 2011.

[2] P. Johansson, M. Kazantzidis, R. Kapoor and M. Gerla, "Bluetooth: an enabler for personal area networking", *IEEE Network*, Vol. 15, N°.5, pages: 28 – 37, 2001.

[3] Bluetooth Low Energy Technology (Wibree). [En ligne]. Disponible sur: http://en.wikipedia.org/wiki/Bluetooth_low_energy.

[4] B. Allen, T. Brown, K. Schwieger, E. Zimmermann, W. Malik, D. Edwards, L. Ouvry and I. Oppermann, "Ultra Wideband: Applications, Technology and Future perspectives," *International Workshop on Convergent Technologies* (IWCT), 2005.

[5] I.F. Akyildiz, T. Melodia and K. Chowdhury, "A Survey on Wireless Multimedia Sensor Networks," *Computer Networks Journal* (Elsevier), March 2007.

[6] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification for Low Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std. 802.15.4, 2006.[En ligne]. Disponible sur: http://profsite.um.ac.ir/~hyaghmae/ACN/WSNMAC1.pdf.

[7] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta and Y.F. Hu, "Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards," *Computer Communication*, Vol. 30, N°.7, pages: 1655-1695, 2007.

[8] Marek Bykowski, David Tracey, Nick Timmons and Jim Morriso, "A schema for the selection of network topology for Wireless Body Area Networks", *IEEE Radio and Wireless Symposium (RWS)*, pages: 390-393, 2011.

[9] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey», *The International Journal of Computer and Telecommunications Networking*, Volume 54 (Issue 15), pages: 2688–2710, October 2010.

[10] Tsenka Stoyanova and George Papadopoulos, "Wireless Sensor Networks For Medical Service". *In Proceeding of 5th European Symposium on Biomedical Engineering ESBME*, Patras, Greece, 2006.

[11] Paulo Neves, Michal Stachyra and Joel Rodrigues, "Application of Wireless Sensor Networks to Healthcare Promotion", *Journal of Communications Software and Systems (JCOMSS)*, Vol. 4, No. 3, 2008.

[12] Benoît Latré, Bart Braem Ingrid Moerman, Chris Blondia and Piet Demeester. "A Survey on Wireless Body Area Networks", *Wireless Network Journal*, Volume 17, Issue 1, pages: 1-18, January 2011.

[13] JeongGil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Andreas Terzis, and Matt Welsh. "Wireless Sensor Networks for Healthcare", *Proceedings of the IEEE*, Volume 98 (Issue 11), pages: 1947-1960, 2010.

[14] H.-Y. Zhou, K.-M. Hou, J. Ponsonnaille, L. Gineste, J. Coudon, G. De Sousa, C. de Vaulx, J.-J. Li, P. Chainais, R. Aufrère, A. Amamra and J.-P. Chane, "Remote Continuous Cardiac Arrhythmias Detection and Monitoring", *Series: Studies in Health Technology and Informatics, Ebook: Volume 105: Transformation of Healthcare with Information Technologies, IOS Press*, pages: 112-120, 2004.

[15] David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care", *In International Workshop on Wearable and Implantable Body Sensor Networks*, April 2004.

[16] Konrad Lorincz, Bor-rong Chen, Geoffrey Werner Challen, Atanu Roy Chowdhury, Shyamal Patel, Paolo Bonato, and Matt Welsh, "Mercury: a wearable sensor network platform for high-Fidelity motion analysis", *In SenSys '09 : Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pages 183-196, New York, 2009.

[17] D. Konstantas, V.Jones, R. Bults and R.Herzog, "MobiHealth: innovative 2.5 / 3G mobile services and applications for healthcare", *Proceedings of the 11th IST Mobile and Wireless Telecommunications Summit*, Greece, 2002.

[18] Reconnaissance de Signaux de Détresse dans l'Habitat Intelligent Santé. [En ligne]. Disponible sur: http://www-clips.imag.fr/geod/projets/HIS/RESIDE-HIS_7-11-02.pdf.

[19] Jiang S, Cao Y, Lyengar S, Kuryloski P, Jafari R, Xue Y, Bajcsy R and Wicker S, "CareNet: an integrated wireless sensor networking environment for remote healthcare", *BodyNets '08 Proceedings of the ICST 3rd international conference on Body area networks.Tempe*, pages:1-3; Arizona 2008.

[20] G.-Z. Yang, "Body Sensor Networks: Body Sensor Networks: Infrastructure for Life Science Sensing Research", *IEEE Life Science Systems and Applications Workshop*, pages: 1-2, 2006.

[21] Huasong Cao, Victor Leung, Cupid Chow and Henry Chan, "Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook", *IEEE Communications Magazine*, Volume 47, Issue 12, pages: 84-93, December 2009.

[22] Kyung Sup Kwak, Sana Ullah, and Niamat Ulla, "An Overview of IEEE 802.15.6 Standard", *3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, pages: 1-6, 2010.

[23] Jan Magne Tjensvold. "Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards", 2007.

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

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

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

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

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

[29] David Martins and Hervé Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms - A short survey", *In NBiS'10, 13th International Conferenc. on Network-Based Information Systems*, pages: 313-320, Japan, September 2010.

[30] D. Martins, "Sécurité dans les réseaux de capteurs sans fil Stéganographie et réseaux de confiance", Rapport de thèse, 2010.

[31] Youssouf Zatout, "Conception et évaluation de performances d'un réseau de capteurs sans fil hétérogène pour une application domotique", Rapport de thèse, 2011.

[32] Bestoon T. Hussain Jaff, "A Wireless Body Area Network System for Monitoring Physical Activities and Health-Status via the Internet", Thesis report, 2009.

[33] A.D. Wood, J.A. Stankovic, and S.H. Son, "Jam: a jammed-area mapping service for sensor networks*", 24th IEEE Real-Time Systems Symposium (RTSS 2003)*, pages: 286-297, December 2003.

[34] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: attack and defense strategies", *IEEE Network*, Volume 20 (Issue 3), pages: 41-47, June 2006.

[35] Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel, and Paul Havinga, Energy effcient link-layer jamming attacks against wireless sensor network MAC protocols, *ACM Transactions on Sensor Networks (TOSN,)* Journal, Volume 5, Issue 1, pages: 76-88, USA, 2005.

[36] Hang Liu, Hairuo Ma, Magda El Zarki, and Sanjay Gupta, "Error control schemes for networks : An overview", *Mobile Networks and Applications Journal*, Volume 2 (Issue 2) pages: 167-182, USA 1997.

[37] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *IEEE International Workshop on Sensor Network Protocols and Applications*, pages: 113-127, 2003.

[38] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks.", *In Proceedings of the 22th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Volume 3, pages: 1976-1986, 2003.

[39] Srdjan Capkun, Levente Buttyán, and Jean-Pierre Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks", *In SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages: 21-32, New York, USA, 2003.

[40] Lingxuan Hu and David Evans, "Using directional antennas to prevent wormhole attacks", In Proceedings of the Network and Distributed System Security Symposium (NDSS) San Diego, California, USA, 2004.

[41] Wassim Znaidi, Marine Minier, and Jean-Philippe Babau, "Detecting wormhole attacks in wireless networks using local neighborhood information", *In IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages:1-5, France, September 2008.

[42] A.D.Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer Society*, Volume 35, (Issue 10), pages: 54-62, December 2002.

[43] Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo, "DoS-resistant authentication with client puzzles", *8th International Workshop on Security Protocols*, pages: 170-177, 2001.

[44] D. Martins and H. Guyennet, "Etat de l'art - Sécurité dans les réseaux de capteurs sans fil", *The 3rd Conference on Security of Network Architectures and Information Systems SAR/SSI'2008*, October 2008.

[45] T.V. Phuong, H. L. Xuan, S. J. Cho, Y-K Lee, S. Lee, "An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks", *ISI'06 Proceedings of the 4th IEEE international conference on Intelligence and Security Informatics*, pages: 735-736, 2006.

[46] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", *Security in Distributed, Grid, and Pervasive Computing Book: Chapter 17*, 2006.

[47] Chaudhari H.C. and Kadam L.U, "Wireless Sensor Networks: Security, Attacks and Challenges", *International Journal of Networking*, Volume 1, Issue 1, pages: 4-16, 2011.

[48] Jaydip Sen, "A Survey on Wireless Sensor Network Security", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 1, No. 2, pages: 55-78 2010.

[49] M. Somasundaram and R. Sivakumar, "Security in Wireless Body Area Networks: A survey", *International Conference on Advancements in Information Technology*, 2011

[50] Pardeep Kumar and Hoon-Jae Lee., "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", *Sensors 12*, no. 1, pages: 55-91, 2012.

[51] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", *The 8th International Conference Advanced Communication Technology (ICACT 2006)*, Volume 2, 2006.

[52] B. Sheng, Q. Li, W. Mao, and W. Jin, "Outlier Detection in Sensor Networks", *The 8th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc 07)*, pages: 219-228, 2007.

[53]W. Wu, X. Cheng, M. Ding, K. Xing, F. Liu, and P. Deng, "Localized Outlying and Boundary Data Detection in Sensor Networks", *IEEE Transactions on Knowledge and Data Engineering*, Volume 19, Issue 8, pages: 1145-1157, 2007.

[54] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey", *ACM Computing Surveys (CSUR)*, Volume 41 (Issue 3), pages: 1-58, 2009.

[55] Yang Zhang, Nirvana Meratnia, and Paul Havinga, "Detection Techniques for Wireless Sensor Networks: A Survey", *IEEE Communications Surveys and Tutorials*, Volume: 12, Issue: 2, pages: 159 – 170, 2010.

[56] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Distributed Deviation Detection in Sensor Networks", *ACM Special Interest Group on Management of Data (SIGMOD)*, pages: 77-82, 2003.

[57] D. Janakiram, V. Adi Mallikarjuna Reddy, and A.V.U. Phani Kumar, "Outlier detection in wireless sensor networks using Bayesian Belief Networks", *In First International Conference on Communication System Software and Middleware (Comsware06)*, pages: 1-6, 2006.

[58] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks", *International Journal of Distributed Sensor Networks*, Volume 2 (Issue 4), pages: 313-332, 2006.

[59] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Distributed anomaly detection in wireless sensor networks", *In IEEE International Conference on Communication Systems (ICCS06)*, pages: 1 -5, 2006.

[60] Wassim Znaidi. "Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil", Rapport de thèse, 2010.

[61] Wang, Y; Attebury, G.; Ramamurthy, B, "A survey of security issues in wireless sensor networks", IEEE Communications Surveys and Tutorials, Volume 8, pages: 2-23, 2006.

[62] J.-B. Aupet, E. Garcia, H. Guyennet, J.-C. Lapayre, and D. Martins, "Security in Medical Telediagnosis", *In Multimedia Services in Intelligent Environments-Integrated Systems*, Chapter 9, pages: 201-226, 2010.

[63] Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", *Sensors journal*, Volume 11 (Issue 2), pages: 1383-1395, 2011.

[64] Mohamed Mostafa M. Fouad, Nashwa El-Bendary, Rabie A. Ramadan, and Aboul Ella Hassanien, "Wireless Sensor Networks: A Medical Perspective", [En ligne]. Disponible sur: http://scholar.cu.edu.eg/?q=abo/files/k15146_c024.pdf.

[65] Raja Jurdak, X. Rosalind Wang, Oliver Obst, Philip Valencia, "Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies", *Intelligence-Based Systems Engineering* Volume 10, Chapter 12, pages: 309-325, 2011.

[66] Tiong Hoo Lim, "Detecting anomalies in Wireless Sensor Networks", Qualifying Dissertation, August 2010.

[67] Shahriar Mohammadi and Hossein Jadidoleslamy, "A comparison of physical attacks on wireless sensor networks", *International Journal of Peer to Peer Networks*, Volume 2, No. 2, April 2011.

[68] Shahriar Mohammadi and Hossein Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks", *International journal on applications of graph theory in wireless ad hoc networks and sensor network*, Volume 3, No.1, March 2011.

[69] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs", *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 4, Fourth Quarter, 2009.

[70] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", *In MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages: 46-57, 2005.

[71] Y. Law, P. Hartel, J. den Hartog, and P. Havinga, "Linklayer jamming attacks on S-MAC" *In IEEE 2nd European Workshop on Wireless Sensor Networks (EWSN 2005)*, pages: 217-225, 2005.

[72] Anthony D. Wood, John A. Stankovic, and Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks", *4th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07)*, pages: 60-69, 2007.

[73] M. Cakiroglu, A.T. Ozcerit, ”Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks”, *Turkish Journal of Electrical Engineering & Computer Sciences*, Volume 19 Issue 1, 2011.

[74] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, “Denial of Service Attacks in Wireless Networks: The case of Jammers”, *IEEE Communications Surveys & Tutorials*, Volume 13, pages: 245-257, 2011.

[75] Mario Strasser, Boris Danev and Srdjan Capkun, “Detection of Reactive Jamming in Sensor Networks”, *ACM Transactions on Sensor Networks*, Volume 7, Issue 2, August 2010.

[76] Abdulaziz Rashid Alazemi. “Defending WSNs Against Jamming Attacks”, *American Journal of Networks and Communications*. Vol. 2, No. 2, 2013, pp. 28-39.

[77] Sudip Misra , Ranjit Singh and S. V. Rohith Mohan. “Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System”, *Sensors journal*, pages: 3444-3479, 2010.

[78] Héctor Iván Reyes and Naima Kaabouch, “Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic”, *International Journal of Scientific & Engineering Research* Volume 4, Issue 2, February 2013.

[79] Proaño Alejandro and Lazos Loukas, “Selective Jamming Attacks in Wireless Networks”, *IEEE International Conference on Communications (ICC 10)*, pages: 1-6, 2010.

[80] Ali Hamieh and Jalel Ben-Othman, “Detection of jamming attacks in wireless ad hoc networks using error distribution”, *International Conference on Communications (ICC 2009)*, pages: 4831-4836, 2009.

[81] Yu Seung Kim and Heejo Lee, "On Classifying and Evaluating the Effect of Jamming Attacks", *The 24th edition of the International Conference on Information Networking (ICOIN)*, 2010.

[82] Alexandros G. Fragkiadakis, Vasilios A. Siris, Nikolaos E. Petroulakis and Apostolos P. Traganitis, “Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection”, *Wireless Communications and Mobile Computing*, 2013.

[83] Alexandros G. Fragkiadakis, Vasilios A. Siris, Apostolos P. Traganitis, “Effective and Robust Detection of Jamming Attacks”, *Future Network and Mobile Summit*, pages: 1-8, 2010.

[84] Alexandros Fragkiadakis, Sofia Nikitaki and Panagiotis Tsakalides, “Physical-layer Intrusion Detection for Wireless Networks using Compressed Sensing”, *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages: 845-852, Barcelona 2012.

[85] W. Lu and A. A. Ghorbani, “Network Anomaly Detection Based on Wavelet Analysis,” *EURASIP Journal on Advances in Signal Processing*, pages: 1-16, 2009.

[86] S. Siripanadorn, W. Hattagam, and N. Teaumroong, “Anomaly detection using self-organizing map and wavelets in wireless sensor networks,” *in Proceedings of the 10th WSEAS international conference on Applied computer science (ACS’10),* pages: 291–297, 2010.

[87]V. A. Siris and F. Papagalou, “Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks,” *in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM’04)*, Volume 4, pages: 2050-2054, 2004.

[88] M. Deza and E. Deza, Encyclopedia of Distances, *Springer*, 2009.

[89] O. Salem, S. Vaton, and A. Gravey, "A Novel Approach for Anomaly Detection over High-Speed Networks," *in Proceedings of the 3rd European Conference on Computer Network Defense (ECND'07)*, vol. 30, pages: 49-68, 2009.

[90] G. Cormode and S. Muthukrishnan, "An Improved Data Stream Summary: The Count-Min Sketch and its Applications," *Journal of Algorithms*, volume 55, Issue 1, pages: 58-75, April 2005.

[91] Sung-Hyuk Cha, "Comprehensive Survey on Distance/Similarity Measures between Probability Density Functions", *International Journal of Mathematical Models and Methods in Applied Sciences*, Volume 1 (Issue 4), pages: 300-307, 2007.

[92] J. Havrda and F. Chavrat, "Quantification method of classification processes: The concept of structural α-entropy," *Kybernetika*, Volume 3, pages: 30–35, 1967.

[93] P. N. Rathie and P. Kannappan, "A directed-divergence function of type β", *Information and Control*, Volume 20, pages: 38–45, 1972.

[94] D. Haussler and M. Opper, "Mutual information, metric entropy, and cumulative relative entropy risk," Ann. Statist., vol. 25, pp. 2451–2492, 1997.

[95] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, "Sketch-based Change Detection: Methods, Evaluation, and Applications". *In Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement (IMC'03)*, pages: 234–247, 2003.

[96] MAWI working group traffic archive. [En ligne]. Disponible sur : http://mawi.wide.ad.jp/mawi/.

[97] Ali Makke, Osman Salem, Mohamad Assaad, Hassine Moungla, Ahmed Mehaoua, "Flooding Attacks Detection in Backbone Traffic Using Power Divergence", *The 7th ACM International Workshop on Performance Monitoring, Measurement and Evaluation of Heterogeneous Wireless and Wired Networks (PM2HW2N 12)*, Paphos, Cyprus, pages: 15-20, October 2012.

[98] Jean Tajer, Ali Makke, Osman Salem, Ahmed Mehaoua, "A Comparison Between divergence measures for Network Anomaly Detection", *in 7th International Conference on Network and Service Management (CNSM 11)*, Paris, France, pages: 1-5, October 2011.

[99] Osman Salem, Ali Makke, Jean Tajer, Ahmed Mehaoua, "Flooding Attacks Detection in Traffic of Backbone Networks", *in 36th IEEE Local Computer Networks (LCN 11)*, Bonn, Germany, pages: 441-449, October 2011.

[100] Victor Richmond R. Jose, Robert F. Nau, Robert L. Winkler, "Scoring rules, generalized entropy, and utility maximization", *Operations research*, Volume 56, No. 5, pages: 1146–1157, 2008.

[101] H. Wang, D. Zhang, and K. G. Shin, "SYN-dog: Sniffing SYN Flooding Sources", Proceedings 22nd International Conference on Distributed Computing Systems, pages: 421-428, 2002.

[102] A. Lakhina, M. Crovella, and C. Diot, "Mining Anomalies using Traffic Feature Distributions", *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '05)*, Volume 35 (Issue 4), pages: 217–228, 2005.

[103] S. Bu, R. Wang, and H. Zhou, "Anomaly Network Traffic Detection Based on Auto-Adapted Parameters Method", *In Proceedings of the 4th International Conference on*

Wireless Communications, Networking and Mobile Computing (WiCOM'08), pages: 601-607, 2008.

[104] N. Ye, S. Vilbert, and Q. Chen, "Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data", *IEEE Transactions on Reliability*, Volume 51 (Issue 1), pages: 75-82, 2003.

[105] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB using SVM", *Computer Communications*, Volume 31 (Issue 17), pages: 4212-4219, 2008.

[106] http://www.insee.fr/fr/mobile/etudes/document.asp?reg_id=0&id=3806 [En ligne].

[107] Ali Syed Taha, Sivaraman Vijay, Ostry Diethelm and Jha Sanjay, "Securing Data Provenance in Body Area Networks Using Lightweight Wireless Link Fingerprints", Proceedings *of the 3rd International Workshop on Trustworthy Embedded Devices (TrustED '13)*, pages: 65-72, 2013.

[108] Aftab Ali and Farrukh Aslam Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications", *EURASIP Journal on Wireless Communications and Networking*, 2013.

[109] Sarah Irum, Aftab Ali, Farrukh Aslam Khan and Haider Abbas, "A Hybrid Security Mechanism for Intra-WBAN and Inter-WBAN Communications", *International Journal of Distributed Sensor Networks*, 2013.

[110] Lu Shi, Ming Li, Shucheng Yu, Jiawei Yuan, "BANA: Body Area Network Authentication Exploiting Channel Characteristics", *IEEE Journal on Selected Areas in Communications Volume 31 (Issue 9)*, pages: 1803-1816, 2013.

[111] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng and Xiaofeng Liao, "Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme", *IEEE Journal on Selected Areas in Communications, Volume 31 (Issue 9)*, pages: 37-46, 2013.

[112] Hu Chunqiang and Zhang Fan and Cheng Xiuzhen and Liao Xiaofeng and Chen Dechang, "Securing Communications Between External Users and Wireless Body Area Networks", *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec '13)*, pages: 31-36, 2013.

[113] Garth V Crosby, Tirthankar Ghosh, Renita Murimi and Craig A Chin, "Wireless Body Area Networks for Healthcare: A Survey", *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, Volume 3, Issue 3, June 2012.

[114] Haining Wang, Danlu Zhang, Kang G. Shin, "Change-Point Monitoring for the Detection of DoS Attacks", *IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4*, pages: 193-208, Oct.-Dec. 2004.

[115] Lu, Kejie and Wu, Dapeng and Fan, Jieyan and Todorovic, Sinisa and Nucci, Antonio, "Robust and Efficient Detection of DDoS Attacks for Large-scale Internet", *Computer Networks, Volume 51, Issue 18*, pages: 5036-5056, 2007.

[116] Tao Peng and Christopher Leckie and Kotagiri Ramamohanarao, "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring", *In Proceedings of the Third International IFIP-TC6 Networking Conference Networking*, pages:771-782, 2004.

[117] Zargar, Saman Taghavi and Joshi, James and Tipper, David, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Communications Surveys and Tutorials, Volume 15(Issue 4)*, pages: 2046-2069, 2013.

[118] Georgios Loukas and Gülay Öke, "Protection against Denial of Service Attacks: A Survey", *The Computer Journal, Vol.53, No.7*, pages: 1020-1037, 2010.

[119] Peng Tao and Leckie Christopher and Ramamohanarao Kotagiri, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", *ACM Computing Surveys Journal, Volume 39, Issue 1*, 2007.

[120] Matt Beaumont-Gay, "A Comparison of SYN Flood Detection Algorithms", *Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP '07)*, 2007.

[121] Dinil Mon Divakaran, Hema A. Murthy and Timothy A. Gonsalves, "Detection of Syn Flooding Attacks using Linear Prediction Analysis", *14th IEEE International Conference on Networks (ICON '06), Volume 1*, pages: 1-6, 2006.

[122] Rahim Kacimi, "Techniques de conservation d'énergie pour les réseaux de capteurs sans fil", Rapport de thèse, 2009.

[123] Gel De Sousa, "Etude en vue de la réalisation de logiciels bas niveau dédiés aux réseaux de capteurs sans fil : microsystème de fichiers", Rapport de thèse, 2008.

[124] Wassim Drira, "Un système de collecte sécurisé et de gestion des données pour les réseaux de capteurs sans fils", Rapport de thèse, 2012.

[125] Fadila Khadar, "Contrôle de topologie dans les réseaux de capteurs de la théorie à la pratique", Rapport de thèse, 2009.

[126] Kamal Beydoun, "Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs", Rapport de thèse, 2009.

[127] Mohamed Lehsaini, "Diffusion et couverture basées sur le clustering dans les réseaux de capteurs : application à la domotique", Rapport de thèse, 2009.

[128] Hung-Cuong Le, "Optimisation d'accès au médium et stockage de données distribuées dans les réseaux de capteurs", Rapport de thèse, 2008.

[129] Ismail Mansour, "Contribution à la sécurité des communications des réseaux de capteurs sans fil", Rapport de thèse, 2013.

[130] A. Benslimane, A. E. Yakoubi and M. Bouhorma, "Analysis of jamming effects on IEEE 802.11 wireless networks", *in Proceedings of IEEE International Conference on Communications (ICC)*, pages:1-5, 2011.