الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة أبي بكر بلقايد– تلمسان –
Université Aboubakr Belkaïd– Tlemcen –
Faculté des sciences

THESE

Présentée pour l'obtention du **grade** de **DOCTORAT 3ème Cycle**

En : Informatique

Spécialité : Réseaux et Systèmes Distribués

Par : Achour M'hammed

Sujet

Développement d'un mécanisme de détection d'intrusion dans les réseaux de capteurs corporels sans fil (WBANs)

Soutenue publiquement, le 25/05/2022, devant le jury composé de :

M. LEHSAINI Mohamed	Professeur	Univ. UABT	Président
M. MANA Mohammed	MCA	Univ. UABT	Directeur de thèse
M. BENAMAR Abdelkrim	Professeur	Univ. UABT	Examinateur
Mme LABRAOUI Nabila	Professeur	Univ. UABT	Examinateur
M. ADJOUDJ Réda	Professeur	Univ. SBA	Examinateur
M. BOUKLI HACENE Sofiane	Professeur	Univ. SBA	Examinateur

Laboratoire de Systèmes et Technologies de l'Information et de la Communication (STIC)

Remerciements

Mes remerciements vont tout d'abord à **Allah**, Tout-Puissant, pour ces bénédictions, à la fois extérieures et intérieures, et de m'avoir aidé à la réalisation de ce travail, "Tout bienfait qui vous comble ne peut venir que d'Allah, et quand un mal vous atteint, c'est Lui Seul Que vous suppliez à haute voix" An-Nahl-53.

En deuxième lieu je remercie **mes parents**, ils ont toujours été là, pour moi, dès le début, quand j'étais petit et jusqu'à maintenant.

Je remercie monsieur **Mohammed Mana**, mon superviseur, pour son amitié, son ouverture d'esprit, sa patience et pour son encouragement.

Je remercie mes collègues , enseignants et étudiants, dans le laboratoire **STIC**, particulièrement je mentionne, monsieur **Lahsaini Mohamed**, le directeur du laboratoire pour prendre soin de ses étudiants et écouter de leurs préoccupations.

Je suis reconnaissant à **M. BENAMAR Abdelkrim**, **Mme. LABRAOUI Nabila**, **M. ADJOUDJ Réda** et **M. BOUKLI HACENE Sofiane** d'avoir accepté d'être un membre dans le jury de soutenance et de faire partie de cet épisode important de ma vie.

Je remercie mon cher frère **Brahim**, qui n'hésitais pas, à tout moment, de m'aider dans la correction de mes rédactions scientifiques, son aide était précieuse.

Je remercie, également, mes chers frères **Mustefa**, **Abdelkader**, **Saadi**, **Said**, **Ahmed** et **Saleh**, ils sont tous mon trésor, de vrai.

Mes remerciements vont, aussi, à **ma femme** qui m'a supporté durant une grande partie de ce travail, je la remercie pour sa compréhension.

Je vous remercie tous et toutes.

Résumé

Dans ce travail, nous avons choisi la norme IEEE 802.15.4 comme technologie habilitante pour les réseaux corporels sans fil (WBAN). Pour sécuriser ces réseaux, nous avons examiné le mode beacon de la norme du point de vue de sécurité pour trouver les menaces qui visent la disponibilité du réseau. En conséquence, nous avons introduit une nouvelle attaque qui exploite le comportement de la norme dans le cas de trafic périodique pour le détériorer en utilisant le moins de ressources possibles. Pour compléter notre objectif de ce travail, nous avons proposé une contre-mesure dont le but est de diminuer le dommage de cette attaque et de reprendre la majorité des ressources réseau dans le cas d'un attaquant simple.

En deuxième lieu, nous avons proposé un algorithme qui estime le taux naturel d'erreurs de paquets pour détecter les anomalies dans le trafic périodique des réseaux basant sur la norme IEEE 802.15.4. Pour arriver à ce but, nous avons dû transformer les périodes des nœuds afin de capturer la saisonnalité dans le trafic. L'algorithme a bien fait en termes de taux de faux positifs et de détection.

Mot clés: Réseaux corporels sans fil, La norme IEEE 802.15.4, Le mode beacon, Supertame, Trafic périodique, Saisonnalité, Taux de faux positif, Taux de détection.

Abstract

In this work, we chose the IEEE 802.15.4 standard as an enabling technology for wireless body area networks. To secure these networks, we examined the beacon mode of the standard from a security perspective to find threats that target network availability. As a result, we have introduced a new attack that exploits the behavior of the standard in the case of periodic traffic to disturb it using as few resources as possible. To complete our work’s objective, we have proposed a countermeasure whose goal is to reduce the damage of this attack and to take back the majority of network resources in the case of a simple attacker.

Moreover, we have proposed an algorithm that estimates the natural packet error ratio to detect anomalies in the periodic traffic of IEEE 802.15.4 based networks. To achieve this goal, we had to transform the periods of the nodes in order to capture the seasonality in the traffic. The algorithm did well in terms of false positive and detection ratios.

Key words: Wireless Body Area Networks, IEEE 802.15.4 standard, Beacon mode, Superframe, Periodic traffic, Seasonality, False positive ratio, Detection ratio.

ملخص

في هذا العمل، اخترنا المعيار IEEE 802.15.4 كتكنولوجيا تمكين لشبكات الجسم اللاسلكية. من أجل تأمين هذه الشبكات، قمنا بفحص وضع البيكن للمعيار من وجهة نظر أمنية للعثور على التهديدات التي تستهدف توفر الشبكة. ونتيجة لذلك، فقد عرَفنا هجومًا جديدًا يستغل سلوك المعيار في حالة تدفق الحزم الدوري لتشويشه باستخدام أقل قدر ممكن من الموارد. لإكمال هدف عملنا، اقترحنا إجراءً مضادًا يتمثل هدفه في تقليل الضرر الناتج عن هذا الهجوم واستعادة غالبية موارد الشبكة في حالة وجود مهاجم بسيط.

بالإضافة لهذا، اقترحنا خوارزمية تقوم بتقدير المعدل الطبيعي للحزم التالفة لاكتشاف الحالات الشاذة في التدفق الدوري للشبكات التي تعتمد المعيار IEEE 802.15.4. لتحقيق هذا الهدف، كان علينا تحويل أدوار الأجهزة المتصلة من أجل التقاط الموسمية في تدفق الحزم. قامت الخوارزمية بعمل جيد من حيث نسبة الأخطاء الإيجابية وكذا نسبة كشف الهجومات.

كلمات مفتاحية: شبكات الجسم اللاسلكية، معيار IEEE 802.15.4، وضع البيكن، تأطير زمني، تدفق دوري، موسمية، نسبة الأخطاء الإيجابية، نسبة كشف الهجومات.

Table des matières

Table des figures

Liste des tableaux

Liste des algorithmes

Liste des acronymes

ACK	ACKnowledgement
ARIMA	AutoRegressive Integrated Moving Average
BA	Body Aggregator
BAN	Body Area Network
BASN	Body Area Sensor Network
BCU	Body Control Unit
BER	Bit Error Ratio
BI	Beacon Interval
BO	Beacon Order
BSN	Body Sensor Network
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
DDoS	Distributed Denial-of-Service attack
DISH	DIstributed SHuffling
DIV	DIVision
ECG	ElectroCardioGram
ED	Energy Detection
EEG	ElectroEncephaloGram
EMG	ElectroMyoGram
FCFS	First Come First Serve
FFD	Full-Function Device
GPRS	General Packet Radio Service
GTS	Guaranteed Time Slot
IBC	Intra-Body Communication
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter Frame Space
IoT	Internet of Things
LQI	Link Quality Indicator
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Medium Access Control layer
MEMS	MicroElectroMechanical Systems
MITM	Man In The Middle
MOD	MODulo
OIA	One Intelligent Attacker
ORA	One Random Attacker
PC	Personal Computer
PD	Parkinson Disease
PD	Personal Device
PDA	Personal Digital Assistant
PER	Packet Error Ratio
PHY	PHYsical layer
POS	Personal Operating Space
PPCM	Plus Petit Commun Multiple
RCSF	Réseaux de Capteurs Sans Fil
RF	Radio frequency
RFD	Reduced-Function Device
RGTS	Random Guaranteed Time Slot
RPD	Random Packet Departure
SARIMA	Seasonal AutoRegressive Integrated Moving Average
SCADA	Supervisory Control and Data Acquisition
SD	Superframe Duration
SF	SuperFrame
SHJA	Slot-Head Jamming Attack
SHJIA	Slot-Head Jamming Intelligent Attack

SHJRA	Slot-Head Jamming Random Attack
SHJSA	Slot-Head Jamming Sinper Attack
SJRG	Selective Jamming Resistant GTS
SNR	Signal-to-Noise Ratio
SO	Superframe Order
TDMA	Time-Division Multiple Access
TIA	Two Intelligent Attackers
TRA	Two Random Attackers
TSCH	Time Slot Channel Hopping
WAN	Wide Area Network
WBAN	Wireless Body Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
2G/3G/4G	2ème Génération /3ème Génération/ 4ème Génération

Introduction générale

Le progrès technologique dans les domaines de miniaturisation et système sur une puce (system on a chip) ont permis l'apparition des capteurs avec une taille extrêmement réduite. Ces capteurs peuvent être associés par des dispositifs de communication pour la transmission sans fil de l'information capturée.

L'avantage principal des systèmes sans fil c'est la facilité de déploiement et maintenance, par conséquent, l'optimisation en coût et effort. Cette optimisation est donnée par le fait que les réseaux de capteurs sans fil (RCSF) gèrent eux-mêmes de façon une fois automatique et autonome. De cette façon, on peut observer les phénomènes qui arrivent dans les terrains d'applications en temps réel en capturant les paramètres qui reflètent les variations de ceux-ci avec les capteurs correspondants.

Parmi les capteurs développés, on trouve ceux qui surveillent la variation de l'état physiologique de l'être humain. Ces petits appareils collectent la valeur du paramètre contrôlé et la transmettent à travers le réseau local positionné dans/sur le corps humain vers un dispositif ayant plus de capacité en termes d'énergie et puissance appelé le nœud puits. Ce nœud présente le pont entre ce réseau et des réseaux de grandes échelles tel qu'internet et réseaux cellulaires. L'information transportée à travers les WANs (Wide Area Networks) peut être sauvegardée dans une base de données associées à l'utilisateur ou consommée directement par la personne chargée comme un médecin en cas d'application médicale. Nous appelons ce genre de réseaux les réseaux de capteurs corporels sans fil ou Wireless Body Area Networks (WBAN) en anglais.

En raison de la multiplicité des motifs pour lesquels une personne surveille son état physiologique, les WBANs couvrent un large éventail d'applications. À titre d'exemple, un athlète peut utiliser un WBAN pour suivre le taux de réponse de ses organes vitaux comme le cœur et poumons à son effort physique lors de l'entrainement. Les WBANs peuvent être aussi exploités dans le cas des personnes âgées pour la localisation et la détection des postures et gestes corporelles. Le domaine de sécurité bénéfice de ces réseaux pour l'identification des

personnes et l'assurance de la confidentialité et l'intégrité de l'information en exploitant les caractéristiques biométriques des WBANs. Généralement, les domaines pouvant bénéficier de ces réseaux comprennent à la fois des champs sensibles comme le domaine militaire et la santé et d'autres champs moins sensibles comme le divertissement et le sport.

Malgré les nombreux domaines d'application de ces réseaux, la première application qui nous vient à l'esprit lorsqu'on parle de réseaux corporels sans fil est la médecine [6]. Plusieurs cas de crise passent sans enregistrement, ce qui affecte la procédure de diagnostic qui aura lieu après longtemps de l'arrivée de ces cas. En adoptant la surveillance continue que les WBANs nous offrirent, on peut couvrir le moment où ces évènements arrivent de manière inattendue. De plus, la capture simultanée de différents paramètres permet un diagnostic précis vu la corrélation naturelle entre ces paramètres. La délivrance automatique des médicaments, la surveillance à distance et d'autres services fournis par les WBANs contribuent directement et indirectement à réduire la pression sur les hôpitaux, ce qui va réduire le coût et l'effort consacrés au traitement.

La norme IEEE 802.15.4 a été développée pour desservir les réseaux locaux sans fil à faible débit (LR-WPAN : Low Rate WPAN). Par rapport aux autres technologies utilisées dans les réseaux WPAN, l'IEEE 802.15.4 est extrêmement économique en énergie. En pratique, nous entendons normalement par la norme, la pile de protocoles bien connue ZigBee/IEEE 802.15.4. Cependant, en considérant les réseaux WBAN, les chercheurs ne prennent que la partie IEEE 802.15.4. Ceci car ils n'avaient pas besoin des autres fonctionnalités de ZigBee ou ils s'intéressent aux protocoles personnalisés mieux adaptés à l'application cible [2]. Le mode beacon de la norme IEEE 802.15.4 convient les réseaux WBAN en raison de sa faible consommation d'énergie et de sa similitude avec le mode centré des réseaux WBAN, dans lequel les dispositifs terminaux forment une topologie d'étoile avec leur coordinateur.

Afin d'assurer l'adoption des WBANs à grande échelle, ces derniers doivent être acceptés par le grand public. L'une des choses les plus importantes qui rend le public faire confiance dans ce type de réseaux est de garantir leur fiabilité et la protection de la vie privée des utilisateurs. Cependant, la portée des choix de sécurité appropriés pour ces réseaux est étroite à cause du manque de ressources. Par conséquent, parvenir à un bon compromis entre le niveau de sécurité approprié et conserver les ressources disponibles est un véritable défi pour les chercheurs que pour les développeurs.

Les protocoles de sécurité des WBANs doivent satisfaire les exigences de protections de réseaux : l'authentification, intégrité, confidentialité, disponibilité et non-répudiation.

Malgré l'importance de l'ensemble de ces exigences, la disponibilité est considérée au top de celles-ci parce qu'elle affecte l'existence du service réseau à la base d'une part et d'autre part elle peut être détériorée par un intrus sans avoir aucune expérience dans le domaine technologique.

L'attaque la plus courante qui cible la disponibilité dans le réseau est le brouillage (jamming). Le risque de cette attaque augmente lorsque son implémenteur utilise ses connaissances préalables du protocole cible pour dissimuler son attaque en faisant ce qu'on appelle le brouillage sélectif. Dans cette attaque l'adversaire choisit un ensemble de paquets satisfaisant un critère de sélection pour les interrompre soit en prévoyant leur temps de transmission soit en les écoutant.

Comme d'autres normes, L'IEEE 802.15.4 a un nombre considérable d'attaques visant son bon fonctionnement. Certains sont partagés avec d'autres protocoles et d'autres sont spécialement conçues pour lui.

Le mode beacon-enabled de l'IEEE 802.15.4 est considéré comme une cible facile pour le brouillage sélectif puisqu'il inclut le mode de transmission GTS (Guaranteed Time Slot) qui est classé comme un protocole TDMA (Time-Division Multiple Access). La méthode d'accès au médium TDMA est vulnérable au brouillage sélectif vu la facilité de détection du départ et fin du créneau horaire d'un certain nœud une fois que l'adversaire atteindra une synchronisation avec le nœud coordinateur. Ceci fait de cette attaque un véritable souci pour les WBANs, notamment avec l'importance du mode GTS pour le transfert du trafic périodique. Ces attaques qui s'appelles attaques GTS étaient introduites pour la première fois en 2007 [7] [8]. Dans ces attaques le choix de la cible à brouiller peut se baser sur l'identifiant de l'appareil ou sur la longueur du créneau horaire.

Pour assurer le succès de l'attaque l'adversaire doit brouiller l'intégralité du créneau. Ainsi, un attaquant ne peut brouiller qu'un seul créneau à la fois pour conserver de l'énergie. Pour améliorer les performances des attaques GTS, nous avons proposé une autre version qui peut paralyser la totalité du réseau même dans le cas d'un attaquant simple. Notre version exploite le comportement de la norme en cas d'arrivée de paquets en dehors de créneau pour minimiser de maximum les ressources de l'attaque.

Pour éviter les attaques GTS, la randomisation des positions des créneaux horaires est adoptée dans tous les travaux qui s'intéressent dans ce type d'attaques [9] [10] [11]. Cependant, cette approche ne présente aucun effet contre notre version. C'est pour cette raison que nous avons proposé une contre-mesure qui peut récupérer la majorité de la disponibilité réseau.

La robustesse des protocoles de communication et les outils cryptographiques sont la première ligne de défense du réseau qui est nécessaire contre les attaques extérieures. Cependant, la protection du réseau contre les attaques internes est tout aussi importante. À cet effet, les systèmes de détection d'intrusion (IDS : Intrusion Detection System) ont été développés. Les IDS sont considérés comme la deuxième ligne de défense en cas de l'échec de la première. Cependant, il faut adapter les systèmes classiques pour qu'ils soient appropriés au manque de ressources qui caractérise les WBANs et les propriétés techniques unique de ces réseaux.

On trouvent beaucoup de travaux qui adoptent l'analyse de trafic pour détecter les menaces potentielles qui visent la sécurité du système de communication [12] [13] [14] [15]. Cependant, ces travaux ciblent des réseaux qui diffèrent énormément, dans ses natures, des réseaux corporels sans fil. Par conséquent, les techniques utilisées ne seront pas appropriées aux réseaux WBANs. De plus, ils n'ont pas adressé, suffisamment, le facteur de périodicité du trafic pour en profiter à l'amélioration des modèles de communication lors de la modélisation. De ce fait, nous avons analysé l'effet de la norme IEEE 802.15.4 sur le trafic périodique et nous avons proposé une technique qui exploite les propriétés temporelles de la norme pour traiter le signal du trafic a fin de lui rendre modélisable. Ensuite nous avons introduit une approche convenable au mode beacon pour détecter parfaitement les anomalies réseau avec un taux de faux positives minimal.

Notre thèse n'a pas pour but de proposer des moyens complets pour sécuriser complètement les réseaux WBANs, car cela nécessite les efforts cumulés des chercheurs au fil de temps. Notre objectif dans cette thèse, en revanche, est de faire un pas vers la sécurisation des réseaux corporels sans fil, premièrement, en examinant l'une des technologies habilitantes des WBANs pour en extraire des vulnérabilités, et ensuite les fixer en proposant des solutions appropriées. Deuxièmement, en proposant un mécanisme de détection d'anomalies adapté à cette technologie, notamment avec l'absence de recherches authentiquement consacrées à cette section.

On a organisé cette thèse en cinq chapitres avec une introduction et conclusion générales.

Le premier chapitre est consacré à introduire les réseaux WBANs. Dans ce chapitre, nous décrivons généralement les bienfaits des WBANs pour le domaine médical et nous soulignons brièvement les différences principales entre ces réseaux et les réseaux WSNs. Nous abordons dans ce chapitre aussi l'architecture générale de ces réseaux en décrivant les différents niveaux de communication construisant le réseau et en détaillant la fonction de chaque composant physique de communication selon son type. Ensuite, nous présentons les

différentes applications des WBANs en les grouper par domaine et nous introduisons les défis qui font face au large déploiement de ces réseaux en les classifiant selon leurs caractéristiques réseaux associés.

Dans le deuxième chapitre, nous donnons une brève introduction à la norme IEEE 802.15.4. Nous exposons, en particulier, le mode beacon de la norme où nous présentons la structure générale de la supertrame, qui définit la distribution des créneaux de transmission sur les nœuds, et nous donnons les formules et paramètres qui l'introduisent. En deuxième lieu, nous décrivons un état de l'art sur les différentes attaques qui visent le bon fonctionnement du standard en choisissant la classification la mieux appropriée dans la littérature.

Dans le troisième chapitre, nous présentons nos contributions SHJA (Slot-Head Jamming Attack) et RPD (Random Packet Departure).

SHJA est une variante de brouillage sélectif qui exploite une nouvelle vulnérabilité que l'on a introduite et qui vise le trafic périodique servi en mode GTS. Nous exposons le danger apporté par cette attaque vu la facilité d'implémentation et la faible consommation de ressources lors de son exécution.

RPD est une solution d'atténuation qui réduit le dommage de l'attaque apporté au réseau en changeant le temps de transmission des paquets constituant le trafic cible. Nous étudions, au fur et à mesure, l'impact de la structure de la supertrame sur SHJA et RPD en prenant le taux de réception, délai et coût énergétique comme métriques d'évaluation.

Le quatrième chapitre est consacré à la préparation du signal du trafic afin de rendre sa capture réalisable. Dans ce chapitre, nous introduisons l'ajustement multiplication de saison. Cette technique peut réduire la taille du signal d'arrivée de paquets en gardant la configuration réseau la même autant que possible.

Le cinquième chapitre traite la détection des anomalies dans le schéma de trafic périodique de la technologie habilitante. Nous testons et évaluons le modèle résultant dans le contexte des attaques de disponibilité.

Nous tirons nos conclusions concernant la sécurité dans les WBANs qui fonctionnent sur l'IEEE 802.15.4 et nous soulignons nos perspectives de recherche pour le travail futur dans la conclusion générale.

Liste des publications

1. M. Achour, M. Mana, and A. Rachedi, "New slot-head jamming attack and mitigation mechanism for wireless body area networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*, (Abu Dhabi, United Arab Emirates), pp. 1–6, Dec 2018.

2. M. Achour, M. Mana, and A. Rachedi, "On the issues of selective jamming in ieee 802.15. 4-based wireless body area networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 135–150, 2020.

3. M. Achour and M. Mana, "Seasonal adjustment for traffic modeling and analysis in ieee 802.15.4 networks," in *2022 7th International Conference on Image and Signal Processing and their Applications (ISPA)*, (Mostaganem, Algeria), pp. 1–6, may 2022.

4. M. Achour, M. Mana, and S. Achour, "Exploiting traffic seasonality for anomaly detection in IEEE 802.15.4 networks," in *2022 19th International Multi-Conference on Systems, Signals & Devices (SSD)*, (Sétif, Algeria), pp. 1–6, may 2022.

Chapitre 1

Réseaux de Capteurs Corporels Sans Fil et la norme IEEE 802.15.4

Les récents progrès techniques dans les circuits intégrés, la technologie RF (radio fréquence) à ultra faible puissance, communications sans fil et microcapteurs ont permis la réalisation des réseaux corporels sans fil [20].

BAN (Body Area Network), est aussi appelé BSN (Body Sensor Network) et WBAN (Wireless Body Area Network) [21] est formellement défini par l'IEEE 802.15 en tant "Une norme de communication optimisée pour les appareils à faible puissance et fonctionnant sur, dans ou autour du corps humain (mais non limités à l'être-humain) pour servir une variété d'applications, y compris médical, l'électronique grand public, le divertissement personnel et d'autres".

En termes plus communs, un réseau corporel humain est un système d'appareils à proximité du corps d'une personne qui coopèrent pour le bénéfice de l'utilisateur [22]. Il se compose de petits dispositifs intelligents attachés ou implantés dans le corps qui sont capables d'établir un lien de communication sans fil [23] , et dont le but est de fournir une plate-forme de calcul publique intégrée avec matériel, logiciel et la technologie de communication sans fil [24].

Un WBAN présente une surveillance de santé d'un patient à long terme dépourvue de toute restriction à son/ses activités quotidiennes habituelles. Il est le moyen le plus simple et le plus rapide pour surveiller efficacement l'état de santé du patient [25]. La figure 1.1 représente un exemple d'un réseau WBAN.

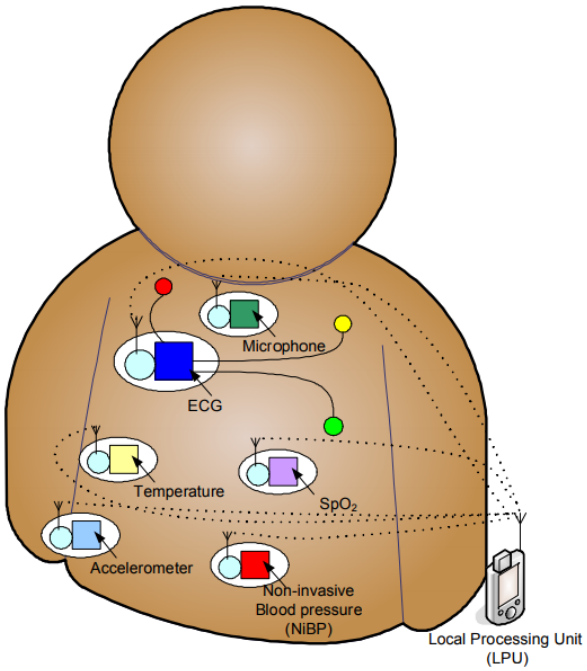


FIGURE 1.1: Un exemple d'un réseau WBAN [1].

Comme la figure montre, un réseau WBAN contient un ensemble de capteurs distribués sur le corps humain et qui peuvent connecter à une unité de traitement locale ayant plus grande capacité en termes de calcul, stockage et énergie.

1.1 Avantages des réseaux de capteurs sans fil

L'exploitation des réseaux WBAN offre plusieurs opportunités pour différents domaines d'application. Cependant, compte tenu de la nature de ces réseaux, le domaine médical est le principal bénéficiaire de cette technologie. Citons quelques avantages médicaux :

(1) **Améliorer la qualité des soins :** En utilisant un réseau corporel sans fil, les résultats des mesures de la santé du patient peuvent être enregistrés sur une période de temps plus longue, améliorant la qualité des données mesurées [26], [25]. De plus, la diversité des paramètres mesurés simultanément donne une vue plus claire notamment qu'il y a une forte corrélation entre les variations des paramètres physiologiques humaines. Par conséquent, avec les réseaux WBANs, les diagnostics seront plus précis.

(2) **Réduction des coûts de soin :** En plus de sauver des vies, l'utilisation répandue de WBANs va réduire les coûts des soins de santé en éliminant la nécessité de coûteuse surveillance hospitalière des patients [27]. L'utilisation d'une connexion filaire dans ce

but se révèle être trop lourde et implique un coût élevé pour le déploiement et la maintenance. En revanche, l'exploit d'une interface sans fil permet une application facile et il est plus rentable [4].

Quelques maladies comme celles cardiaques sont associées aux anomalies épisodiques et l'enregistrement de ces anomalies est important. Cependant, leur calendrier n'est pas prédéfini et beaucoup de temps et d'efforts sont gaspillés en essayant de capturer une "épisode" de ces anomalies.

Dangereux et voire mortels problèmes peuvent passer inaperçus parce qu'ils ne se produisent que rarement et ne peuvent jamais être enregistrés objectivement [1]. En effet, la recherche a montré que la plupart des maladies peuvent être évités si elles ont été détectées à leurs premiers stades [27]. Ainsi, le WBAN offre un changement de paradigme de la gestion de la maladie vers la gestion proactive du bien-être en se concentrant sur la prévention et la détection/traitement précoce des maladies [28].

(3) **Confortabilité des malades :** Avec ce genre de réseaux les malades peuvent rester chez eux et effectuent leurs activités habituelles pendant que leurs paramètres physiologiques soient surveillés à distance à travers d'autres types de réseaux de plus hauts débits comme internet, les réseaux cellulaires ou autres.

Que ce soit le patient est à l'hôpital, à la maison ou en déplacement, le patient n'a plus besoin de rester au lit, il sera plutôt capable de se déplacer librement. De plus, si le réseau est mené par des actionneurs, la prise de médicaments sera faite automatiquement ou même initialisée à distance.

Les chercheurs croient que les systèmes WBAN vont permettre un changement radical de la façon dont les gens pensent et gèrent leur santé de la même manière que l'internet a changé la façon dont les gens communiquent entre eux et recherchent de l'information [29] [30].

1.2 WBAN versus WSN

Les réseaux de capteurs corporels proviennent de réseaux de capteurs, donc il y a beaucoup de similitudes entre eux. Cependant, les caractéristiques sont différentes convenablement en raison de leurs différents buts d'application [31]. De plus, les réseaux de capteurs traditionnels ne relèvent pas les défis spécifiques associés à la surveillance du corps humain.

Le tableau 1.1 résume les principales différences entre ces deux types de réseaux [25] [27] [32] :

TABLEAU 1.1: Les différences principales entre WSN et WBAN [4].

Critère	**WSN**	**WBAN**
Échelle	Environnement surveillé (mètres/kilomètres)	Le corps humain (centimètres/mètres)
Nombre de nœuds	Beaucoup de nœuds redondants pour une couverture étendue	Plus moins, surface limitée
Topologie de réseau	Très susceptibles d'être fixe ou statique	Variable à cause du mouvement du corps
La précision des résultats	Par la redondance de nœuds	A travers la précision et la robustesse de nœud
Tâches de nœuds	Nœud effectue une tâche dédiée	Nœud effectue des tâches multiples
Taille du nœud	Petite est préférable, mais pas de grande importance	Petite est essentielle
Débits de données	Le plus souvent homogènes, trafic événementiel	Le plus souvent hétérogène, trafic événementiel et périodique
Remplacement du nœud	Effectué facilement, des nœuds même jetable	Remplacement difficile des nœuds implantés
Durée de vie du nœud	Plusieurs années/mois	Plusieurs années/mois, plus petite capacité de la batterie
Alimentation électrique	Nœuds accessible et susceptible d'être remplacé plus facilement et fréquemment	Inaccessibles et difficiles à remplacer dans un contexte d'implantation
Demande d'énergie	Susceptible d'être grande, approvisionnement énergétique plus facile	Susceptible d'être inférieure, approvisionnement énergétique plus difficile
Source de récupération d'énergie	Le plus susceptible l'énergie solaire et le vent	Le plus susceptible le mouvement (vibration) et source thermique (chaleur corporelle). Incontournable pour les implants et quelques capteurs externes
Biocompatibilité	Pas une considération dans la plupart des applications	Plus important, afin de protéger la vie du patient
Niveau de sécurité	Plus bas	Plus important, peut exiger des mesures supplémentaires
Impact de la perte de données	Susceptible d'être compensé par des nœuds redondants, dépendra de la situation, le changement de la météo, etc.	L'assurance de la qualité de service est primordiale, transmission de données en temps réel, environnement très non fiable
La technologie sans fil	Bluetooth, ZigBee, GPRS, WLAN, ...	L'exigence d'une technologie de faible puissance
la sensibilité au contexte		Très important, la physiologie du corps est très sensibles au changement du contexte

1.3 Architecture de réseau WBAN

Un WBAN se compose de nœuds situés dans et sur le corps qui surveillent en permanence les informations vitales d'un patient pour le diagnostic et la prescription. Certains nœuds sur-corps peuvent être utilisés pour les applications multimédia et jeux. Ces nœuds peuvent avoir différentes topologies telles qu'étoile, arbre et mesh. Cependant, la plus commune topologie est celle d'étoile dont les nœuds sont reliés directement à un coordinateur central [27] [33].

Généralement, quant à l'architecture du réseau WBAN, il faut prendre en considération deux choses :

- L'architecture considérée c'est l'architecture de communication.
- L'exemple idéal de cette architecture c'est celle exploitée à la télé-médecine à cause de ça bonne représentativité.

La figure 1.2 représente l'architecture générale d'un réseau WBAN.

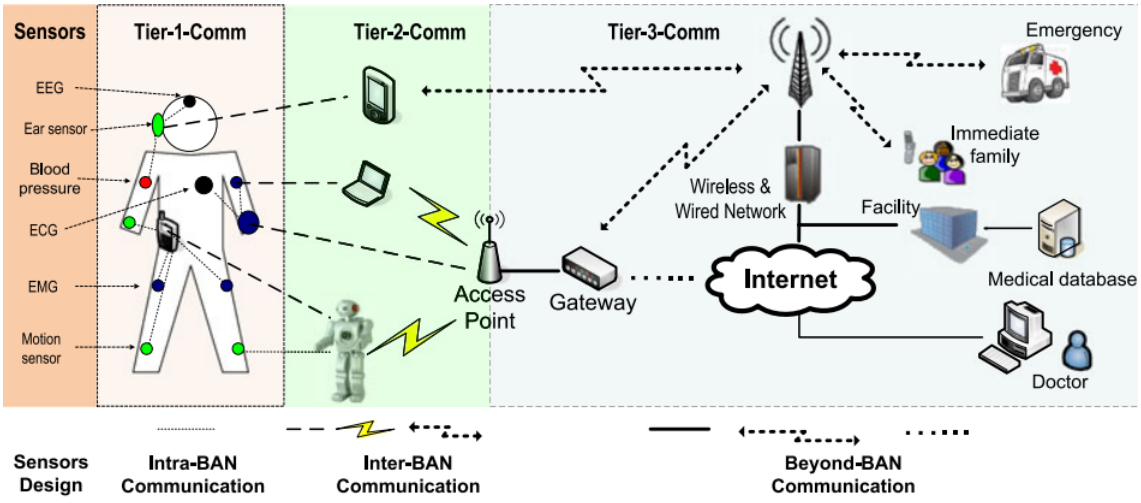


FIGURE 1.2: L'architecture de communication des réseaux WBANs [2].

Comme cette figure montre, l'architecture de communication WBAN peut être divisée en trois niveaux différents comme suit :

- Niveau-1 : la communication Intra-WBAN
- Niveau-2 : la communication Inter-WBAN
- Niveau-3 : la communication Au-delà-WBAN

- Niveau-1 : la communication Intra-WBAN

Niveau-1 représente l'interaction du réseau de nœuds et leurs portées de transmission respectives dans et autour du corps humain ($\sim$ 2 mètres). Un nœud dans un WBAN est défini comme un dispositif indépendant avec possibilité de communication [27].

Dans ce niveau, on distingue deux types de nœuds :

1- **Les nœuds simples :** un nœud simple peut être un capteur qui surveille les variations d'un ou plusieurs paramètres vitaux comme la température, la pression de sang, ECG, etc. Il peut être aussi un actionneur qui acte selon l'ordre d'un agent médical (médecin) ou agit automatiquement si un dépassement d'un seuil prédéfini a été annoncé par un nœud capteur (ex. les pompes d'insuline).

Un nœud est généralement composé de quatre modules. Chaque module est responsable d'une ou plusieurs tâches de préparation de donnée avant qu'elle soit envoyée au nœud coordinateur :

- Le module de capture/action : contient un ou plusieurs capteurs/actionneurs. Prend la responsabilité de collecter les données brutes associées aux paramètres vitaux humaines ou faire une action en cas d'un actionneur.
- Le module de traitement : prépare la donnée avant qu'elle soit émise. La préparation comprend le prétraitement, l'extraction de caractéristiques, la fusion de données et la compression. Finalement le processeur exécute tous les processus protocolaires nécessaires pour envoyer la donnée.
- Le module de communication : responsable de l'émission directe ou indirecte (selon la topologie) des données vers le nœud de coordination.
- Le module d'alimentation : alimente tous les modules précédents.

La figure 1.3 représente la structure générale d'un nœud simple.

2- **Le nœud coordinateur :** c'est le dispositif responsable de la coordination des nœuds simples. Il possède plus grande capacité que les nœuds ordinaires. Il est parfois référencé par le dispositif personnel (PD : Personal Device), l'unité corporelle de contrôle (BCU : Body Control Unit), passerelle corporelle (body gateway), nœud-puits (sink) ou l'agrégateur corporel (BA : Body Aggregator). Il effectue une multitude de fonctions, y compris la détection, la fusion de données des capteurs au long du corps, servant d'interface utilisateur et faire une passerelle de BASNs aux infrastructures de niveau supérieur et donc à d'autres intervenants [34]. Il peut, facilement, être implémenté dans un PDA (Personal Digital Assistant) ou un smartphone.

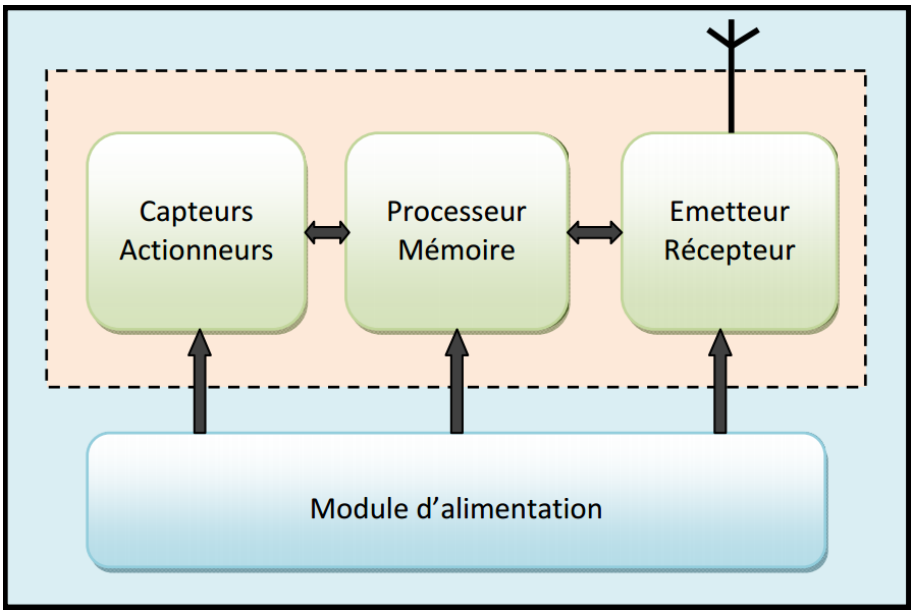


FIGURE 1.3: La structure générale d'un nœud simple.

Les données physiologiques traitées par le coordinateur seront ensuite transmises à un point d'accès dans le Niveau-2 [27]. Le serveur personnel peut être directement implémenté soit dans le coordinateur soit dans le point d'accès.

- Niveau-2 : la communication Inter-WBAN

La communication inter-Ban est la communication entre le serveur personnel et un ou plusieurs points d'accès d'extrémité. L'objectif exclusif du Niveau-2 c'est d'interconnecter le BAN avec les réseaux publics qui sont faciles à accéder dans la vie quotidienne, tels que les réseaux cellulaires et internet [2].

- Niveau-3 : la communication Au-delà-WBAN

Contrairement à la conception communicative de Niveau-2, le design de communication de Niveau-3 est conçu pour être utilisé dans les régions métropolitaines. Afin de relier les deux réseaux de communication inter-Ban et au-delà BAN, une passerelle, comme un PDA peut être utilisé pour créer une liaison sans fil entre eux. Toutefois, en fonction de la demande, le serveur personnel de Niveau-1 peut utiliser GPRS/3G/4G au lieu de passer par un point d'accès [27].

De manière générale les capteurs collectent les données physiologiques et les transmettent au coordinateur qui à son tour les transmet autre fois à travers des réseaux de niveau plus haut vers les serveurs médicaux pour le stockage et le traitement antérieurs.

1.4 Les applications des réseaux WBAN

La nature sans fil du réseau et la grande variété de capteurs offrent de nombreuses applications nouvelles, concrètes et innovantes pour améliorer les soins de santé et la qualité de vie [35]. La technologie BSN devient petit à petit mature et largement utilisée dans de nombreux domaines, y compris la médecine, la protection sociale, le sport, et les interfaces homme-machine [31]. Ces applications peuvent être considérées comme un indicateur de la taille du marché des WBANs. La principale caractéristique de l'ensemble de ces applications est que les WBANs améliorent la qualité de vie de l'utilisateur [4].

Le tableau 1.2 figure quelques exemples d'applications classifiés selon les principaux domaines d'application.

1.5 Les défis des réseaux WBAN

Malgré les progrès importants réalisés dans la technologie sans fil, les WBANs posent des défis techniques uniques principalement en raison de la diversité des applications et de leurs exigences strictes [28]. Pour comprendre les défis qui font face au bon déploiement de ces réseaux, il faut connaitre comment ils sont provoqués. En effet, les défis de déploiement des réseaux WBANs sont une combinaison des caractéristiques restreintes de l'environnement de déploiement avec les besoins de leurs différentes applications.

Dans les paragraphes qui suivent, on va citer les caractéristiques restreintes de déploiement des réseaux WBANs et au fur et à mesure on indique quelques défis associés.

1.5.1 Les caractéristiques environnementales des réseaux WBANs :

L'environnement de déploiement des réseaux WBANs, comme le nom l'indique, est le corps humain. Donc, les caractéristiques en terme technique de ce dernier sont exactement celles du premier :

1- **La valeur importante de la vie humaine**

Puisque les réseaux WBANs sont dirigés principalement aux applications médicales, il faut prendre plus de mesures pour assurer la sécurité des informations médicales des utilisateurs en termes de confidentialité, intégrité, authentification et autres. La deuxième chose qu'il faut prendre en considération c'est la fiabilité et la disponibilité du réseau. En effet, un signal d'urgence manqué pourrait être la différence entre la vie et la mort [36]. Il faut prendre toutes ces mesures sous les contraintes typiques d'énergie et de calcul.

TABLEAU 1.2: Exemples d'application pour les WBANs.

Classe	**Applications**
La surveillance continue : le diagnostic, le suivi et le traitement [2] [4] [20] [27] [31] [37]	- Diagnostic des maladies cardiaques par ECG - Changements de programme de surveillance pour les stimulateurs cardiaques - Défibrillateurs cardiaques implantables - Contrôle de la fonction de la vessie - Surveillance ECG, température, la pression artérielle, respiration - Le diabète, l'asthme - Détection du cancer - La surveillance du stress - Le suivi de la maladie de Parkinson (PD) - Le traitement/réhabilitation des maladies respiratoires - Patients qui se remettent d'une chirurgie - L'administration des médicaments - Prévision d'un œdème pulmonaire (mesurer le volume de liquide pulmonaire) - Intégration de la santé mobile (m-health)
Suite à la page suivante	

TABLEAU 1.2 – Suite de la page précédente

Classe	Applications
Assistance des handicapés [4] [31] [37]	- Assistance de personne aveugle (envoyer des informations auditifs d'emplacement, des portes ou des passages par des capteurs intégrés à l'intérieur des chaussures) - Lunettes IBC supportant (Intra-Body Communication) convertissent les émissions audio en texte pour les personnes sourdes - Un gant basé sur la geste de la main pour faciliter la communication avec les personnes atteintes de la parole et ayant des troubles de malentendants - Malvoyants (rétine artificielle, des capteurs sensibles à la lumière, caméra externe montée sur une paire de lunettes) - La restauration du mouvement du membre (la détermination de la position des jambes, stimuler les muscles) - Pompe d'insuline - Stimulateur de la moelle épinière
Suite à la page suivante	

TABLEAU 1.2 – Suite de la page précédente

Classe	Applications
La sécurité publique [20] [27] [37]	- Les pompiers, les policiers ou dans un environnement militaire (niveau de toxines dans l'air, la reconnaissance chimique) - Explorateurs en eau profonde et de l'espace - L'évaluation de la fatigue des soldats et de la préparation de la bataille - L'uniforme de bataille (capteurs, caméras, RF et PDA personnels) - Surveillance de l'état physiologique d'un soldat - Prévenir les pertes de tirs amis - Appel à soutien - Éviter les embuscades - L'amélioration des soins en cas de blessure
Autres aides sociales [38]	- Réduire les coûts nécessaires pour faire fonctionner un WSN. - Empêcher le vol de câbles et conducteurs (câbles d'alimentation électrique, câbles de lignes de télécommunications et de lignes de chemin de fer)

Suite à la page suivante

TABLEAU 1.2 – Suite de la page précédente

Classe	Applications
Qualité de vie [2] [27] [31] [37] [38]	- La surveillance des choses oubliées - Système de rappel d'actions pour les patients atteints de démence - La création d'un réseau social - Authentification sécurisée (modèles du visage, les empreintes digitales et reconnaissance de l'iris) - Le stockage de l'information privée ou d'affaires dans les capteurs de corps pour de nombreuses applications de la vie quotidienne (courses, échange d'informations, ...) - Prise en charge de navigation dans la voiture ou pendant la marche (un musée ou guide de la ville) - Système de divertissement portable - Le suivi du nourrisson - Carte de paiement sans fil (affichage de transactions récentes et la vérification du solde) - Détection de chute pour déclencher le gonflage de l'airbag gonflable (empêche un dommage grave causé par des chutes) - Les systèmes de surveillance électronique (personnes atteintes de troubles cognitifs) - Rappeler le personnel infirmier pour remplacer les couches (incontinence urinaire) - Mise en scène du sommeil - Détection de l'émotion - Améliorer la santé des animaux et contrôler leurs maladies qui fournissent la nourriture à l'être humain : le lait, les œufs, la viande, etc.
Suite à la page suivante	

TABLEAU 1.2 – Suite de la page précédente

Classe	Applications
sport [2] [27]	- L'entraînement scientifique, la correction de posture et l'amélioration des compétences. - Mesurer le pH de la sueur (détection de l'état physiologique au moment de déplacement) - Prévenir les blessures liées à l'entraînement incorrect - Améliorer la performance humaine - Conserver l'énergie et faire le joueur effectuer son rôle à l'altitude maximale sur une longue période de temps
Divertissement [2] [4] [27]	- Jeux interactifs (interfaces basées sur le mouvement humain) - Appareils : lecteur mp3, visualisation (ordinateur) par tête-monté, un microphone, un appareil photo, etc. - Jeux de réalité virtuelle - Le streaming à temps réel (vidéo/audio en streaming) - Les systèmes de divertissement portables

2- **La confortabilité**

Afin que les réseaux WBANs soient acceptables par le public, il est important qu'ils soient petits et flexibles, ce qui les rend de faible capacité énergétique et calculatrice. L'implémentation des algorithmes de traitement et des protocoles de communication qui satisfirent les besoins multiples de différentes applications sous ces limites représente un grand défi.

La durée de vie de la batterie est proportionnelle à la taille de celle-ci [29] et la taille de celle-là (répondant au besoin énergétique) est dans la plupart des cas, le plus grand

contributeur au capteur en termes de dimensions et poids. Les batteries sont, en conséquence, gardées petites et la consommation d'énergie pour les besoins dispositifs doit être réduite.

En particulier, pour les dispositifs implantés, la durée de vie est cruciale. La nécessité de remplacer ou recharger les capteurs implantés induit une pénalité de coût et commodité qui est indésirable non seulement pour les dispositifs implantés, mais aussi pour ceux qui sont plus grands [4]. Avec une combinaison systématique de protocoles à plus faible énergie et les technologies de récupération d'énergie, la solution optimale pour la réalisation d'un réseau corporel sans fil autonome peut être atteinte [25].

3- **La compatibilité avec le corps humain**

Puisque les capteurs/actionneurs sont en contact direct avec les personnes ou même implantés, leur taille et la compatibilité physique avec les tissus humains sont cruciales. Ce qui motive la recherche et la synthèse de nouveaux matériaux.

Pour les antennes qui sont placés à l'intérieur du corps humain, seuls les matériaux non corrosifs et biocompatibles, tel que le platine ou le titane peuvent être utilisés pour les implants. Cependant, ces matériaux donnent un rendement plus faible par rapport à une antenne de cuivre. La forme et la taille d'une antenne de l'implant dépend de son emplacement à l'intérieur du corps, ce qui limite encore la liberté du constructeur [4].

En outre, les ondes radio provoquent un effet d'échauffement auteur du nœud transmetteur qui fait du mal au tissu ce qui, probablement, va exiger l'application des protocoles de routage qui suivent l'approche basée sur la sensibilisation à la température [37]. De plus, les effets de la température sur la graisse, les muscles et les tissus de la peau, provoquée par le champ électrique, doivent être également considérés lors de la conception des antennes BAN [4].

4- **La mobilité du corps humain**

On peut classifier les mouvements du corps humain en deux catégories :

- Mouvement globale : lors de l'activité habituelle de l'utilisateur. Ce dernier peut entrer dans la portée d'autres WBANs et provoque l'interférence inter-ban, ou passer par d'autres types réseaux sans fil ou machines causant la perturbation (extra-ban interférence).

Le réseau doit assurer la fiabilité de communication même en cas de coexistence avec d'autres réseaux [39]. Cependant, avec l'augmentation du nombre de WBANs qui peuvent coexister chacun à la proximité de l'autre, la liaison de communication peut

souffrir d'une dégradation de performance [27]. En outre, à cause de la nature du réseau WBAN et sa grande mobilité, il est impossible d'attribuer un coordinateur global pour contrôler la coexistence de plusieurs WBANs [39] [40].

- Mouvement partiel : le mouvement des armes lors de la marche par exemple peut entrainer des changements fréquents de la topologie du réseau et les nœuds entrent et sortent de la portée de chacun. La conception d'un protocole robuste contre ces changements avec les caractéristiques uniques des réseaux WBANs porte des grands défis pour les développeurs.

5- **La diversité des valeurs physiologiques humaines**

Les applications des réseaux corporels ont des besoins différents en termes de paramètres de performance réseau à cause de la diversité des paramètres physiologiques associés à ces applications. Comme il est vu dans le tableau 1.3, les différentes applications exigent différents débits, rapports cycliques, topologies et autres spécifications [5].

TABLEAU 1.3: Les exigences technologiques de quelques applications WBAN [5].

Exigences vs. Applications	**ECG**	**EMG**	**EEG**	**Aide auditif**	**Stimulation cérébrale**	**Audio**	**Surveillance de température ou Glycémie**
Durée de vie de pile nécessaire	$>$ 1 semaine	$>$ 1 semaine	$>$ 1 semaine	$>$ 40 heures	$>$ 3 ans	$>$ 24 heures	$>$ 1 semaine
Débit exigé	72 Kbps	1.536 Mbps	86.4 Kbps	200 Kbps	1 Mbps	1 Mbps	$<$ 10 Kbps
Latence toléré	$<$ 250 ms	$<$ 250 ms	$<$ 250 ms	$<$ 250 ms	$<$ 250 ms	$<$ 100 ms	$<$ 250 ms
BER (Bit Error Rate)	10^{-10}	10^{-10}	10^{-10}	10^{-10}	10^{-3}	10^{-5}	10^{-10}
Rapport cyclique	$<$ 10%	$<$ 10%	$<$ 10%	$<$ 10%	$<$ 50%	$<$ 50%	$<$ 1%

Le tableau 1.3 montre la nécessité de garantir la qualité de service dans les réseaux WBANs, ce qui exige le support de différents modes d'opération dans la couche physique implémenté.

6- **La limitation sur le nombre de nœuds**

En raison des limitations de la nature du réseau en termes de protocoles de communication, architecture et techniques de transmission, le nombre de nœuds peuvent être limité dans les scénarios d'application réels [27]. En effet, au contraire de réseaux de capteurs traditionnels, qui assurent la justesse des valeurs mesurées par la redondance des nœuds,

les réseaux WBANs assurent la justesse de celles-ci par la robustesse et la justesse du nœud. En effet, tous les appareils sont tout aussi importants et les dispositifs ne sont ajoutés que lorsqu'ils sont nécessaires pour une nouvelle application [4].

7- **Le corps humain, un support de communication non fiable**

Les WBANs ont, toujours, éprouvés d'une perte de chemin élevée à cause de l'absorption du corps. Par conséquent, la zone environnante du corps humain est considérée comme un support non fiable pour la propagation des ondes.

Différents paramètres de l'utilisateur, tels que la perte de poids/graisse, la posture et le changement de la peau avec l'âge doivent également être pris en considération pour la conception des antennes dans les WBANs [27].

Assurer la fiabilité de communication, surtout en cas de temps réel, dans cette environnement non fiable demande plus de recherches concernant les techniques de routages multi sauts, la technologie radio, la correction d'erreur, gestion d'énergie de transmission, etc.

1.6 Conclusion

La technologie des réseaux corporels sans fil va permettre d'ouvrir de grands horizons aux applications télé-médecine et à la qualité de vie de manière générale. Elle va changer radicalement le mode de vie quotidienne et ajouter une autre dimension au systèmes IoT (Internet Of Things) lors de l'adoption répandue de ces derniers. Cependant, pour bénéficier du plein potentiel de ces réseaux, il faut surmonter quelques difficultés techniques et éthiques. La protection de la vie humaine représente le cœur de ces difficultés.

Les défis introduits par ces réseaux viennent de ces caractéristiques distinguées par rapport aux réseaux de capteurs sans fil classiques. Ils sont liés principalement à la nature et au comportement du corps humain.

Beaucoup de facteurs importants doivent être pris en considération lors du déploiement des ces réseaux dont la compatibilité avec le corps humain, la confortabilité de ses porteurs et la protection de la vie privée représentent la première priorité [41] [42].

Pour que ces réseaux soient adoptés à grande échelle, ce domaine nécessite la collaboration des efforts des chercheurs et fabricants pour accélérer la procédure d'amélioration de ce qui existe et développer des nouvelles solutions afin d'arriver finalement à la normalisation de ces réseaux.

Dans le chapitre suivant nous allons introduire une technologie qui a pu, avec ses améliorations continues, prouver sa éligibilité à héberger les réseaux corporels sans fil. Cette

technologie introduit différents modes de communication et adopte, continuellement, des nouvelles technologies radio pour couvrir les différentes manières d'exploitation des réseaux hébergés.

Chapitre 2

La norme IEEE 802.15.4 et les menaces existantes

La technologie IEEE 802.15.4 a été développée pour desservir les réseaux locaux sans fil à faible débit (LR-WPAN). Cette technologie est extrêmement économique en énergie en comparaison avec d'autres technologies utilisées dans les réseaux WPAN. Elle comprend le mode beacon qui convient les réseaux WBAN en raison de sa faible consommation d'énergie et de sa similitude avec le mode centré des réseaux WBAN, où les nœuds capteurs forment une topologie d'étoile avec le nœud puits.

Dans les sections qui suivent, nous donnons une introduction sur la norme IEEE 802.15.4 et les menaces potentielles pouvant affecter sa fonctionnalité en se concentrant sur le mode beacon et sur les notions les plus pertinentes pour notre travail [3].

2.1 Aperçu général de l'IEEE 802.15.4

Un réseau IEEE 802.15.4 est un réseau de communication simple et économique qui permet une connectivité sans fil dans des applications avec une puissance limitée et des exigences de débit assouplies. Les principaux objectifs de ce réseau sont la facilité d'installation, la fiabilité du transfert de données, un coût extrêmement bas et une durée de vie raisonnable de la batterie, tout en conservant un protocole simple et flexible.

2.1.1 Composants du réseau IEEE 802.15.4

Deux types d'appareils différents peuvent participer à un réseau IEEE 802.15.4 : un appareil à fonction complète (FFD : Full-Function Device) et un appareil à fonction réduite

(RFD : Reduced-Function Device). Un FFD est un appareil capable de servir de coordinateur de réseau personnel (PAN) tandis que un RFD ne peut pas servir de coordinateur.

Le composant le plus élémentaire est l'appareil. Deux ou plusieurs appareils communiquant sur le même canal physique constituent un réseau. Cependant, ce réseau doit comprendre au moins un FFD, qui joue le rôle de coordinateur PAN.

2.1.2 Topologies de réseau

En fonction des exigences de l'application, un réseau IEEE 802.15.4 fonctionne dans l'une des deux topologies : la topologie en étoile ou la topologie pair à pair. Dans la topologie en étoile, la communication est établie entre les appareils et un seul contrôleur central, appelé coordinateur PAN. Le coordinateur PAN est le contrôleur principal du réseau.

Les applications qui bénéficient d'une topologie en étoile comprennent la domotique, les périphériques d'ordinateurs personnels (PC), les jeux et les soins de santé personnels.

La topologie pair à pair a également un coordinateur PAN ; cependant, elle diffère de la topologie en étoile en ce que tout appareil est capable de communiquer avec n'importe quel autre appareil tant qu'ils sont à portée l'un de l'autre. La topologie pair à pair permet la mise en œuvre de formations réseau plus complexes, telles que la topologie de réseau maillé. Des applications telles que le contrôle et la surveillance industriels, les réseaux de capteurs sans fil, le suivi des actifs et des stocks, l'agriculture intelligente et la sécurité bénéficieraient d'une telle topologie de réseau.

Chaque PAN indépendant sélectionne un identifiant unique. Cet identifiant PAN permet la communication entre les appareils au sein d'un réseau et permet les transmissions entre les appareils sur des réseaux indépendants.

2.1.3 Architecture

La norme IEEE 802.15.4 définit les couches PHY et MAC et s'appuie sur d'autres technologies pour les couches supérieures (Figure 2.1).

Les caractéristiques de PHY sont l'activation et la désactivation de l'émetteur-récepteur radio, la détection d'énergie (ED : Energy Detection) , l'indicateur de qualité de lien (LQI : Link Quality Indicator), la sélection du canal, l'évaluation du canal (CCA : Clear Channel Assessment) et la transmission et la réception des paquets sur le support physique.

La sous-couche MAC comprend la gestion des balises, l'accès au canal, la gestion GTS, la validation de trame, livraison accusée de trame, l'association et la dissociation.

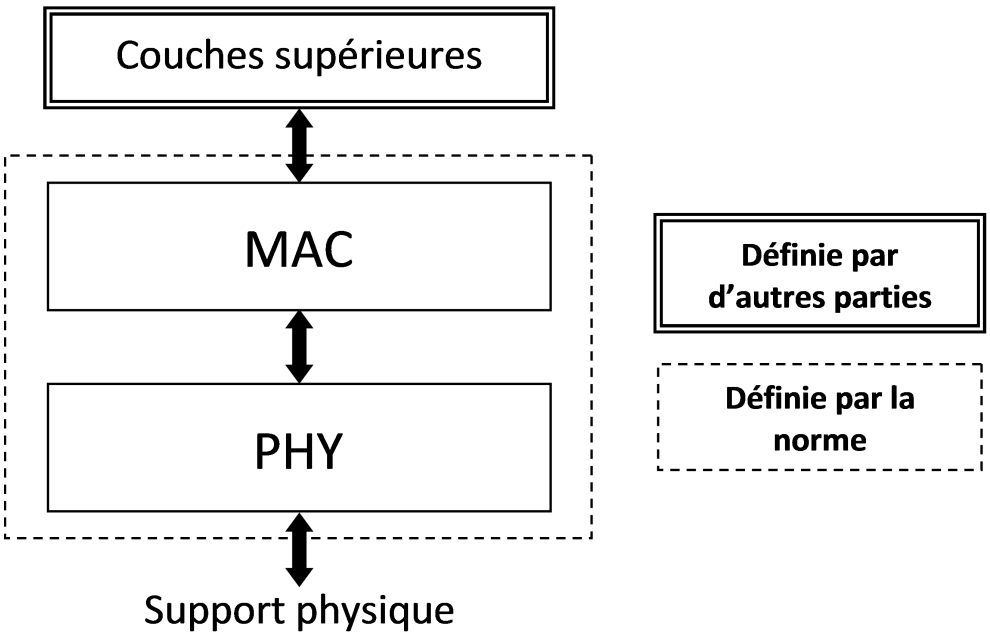


FIGURE 2.1: Architecture de la norme IEEE 802.15.4 [3]

2.1.4 Modes de communication

Il existe deux modes au choix lors de l'établissement d'un réseau : le mode avec balise activé (beacon-enabled mode) et le mode avec balise non activé (non-beacon enabled mode). Les réseaux qui nécessitent une structure de supertrame de synchronisation doivent utiliser le premier mode et ceux qui ne le font pas doivent utiliser le second.

Nous adopterons le terme beacon au lieu de balise dans le reste de cette thèse.

Le mode beacon de l'IEEE 802.15.4

Ce mode est également appelé mode fendu (slotted mode).

En mode beacon, les appareils doivent suivre une structure de supertrame et communiquer uniquement avec le coordinateur. Il n'y a pas de transactions pair à pair.

Le coordinateur transmet périodiquement des trames beacon pour définir les limites de la supertrame et se synchroniser avec les dispositifs du réseau. La supertrame est l'incarnation réelle du mode beacon.

Structure de la supertrame

La supertrame présente le temps écoulé entre deux transmissions de trames beacon et nous nous référons à sa longueur par l'intervalle beacon (BI : Beacon Interval). L'intervalle

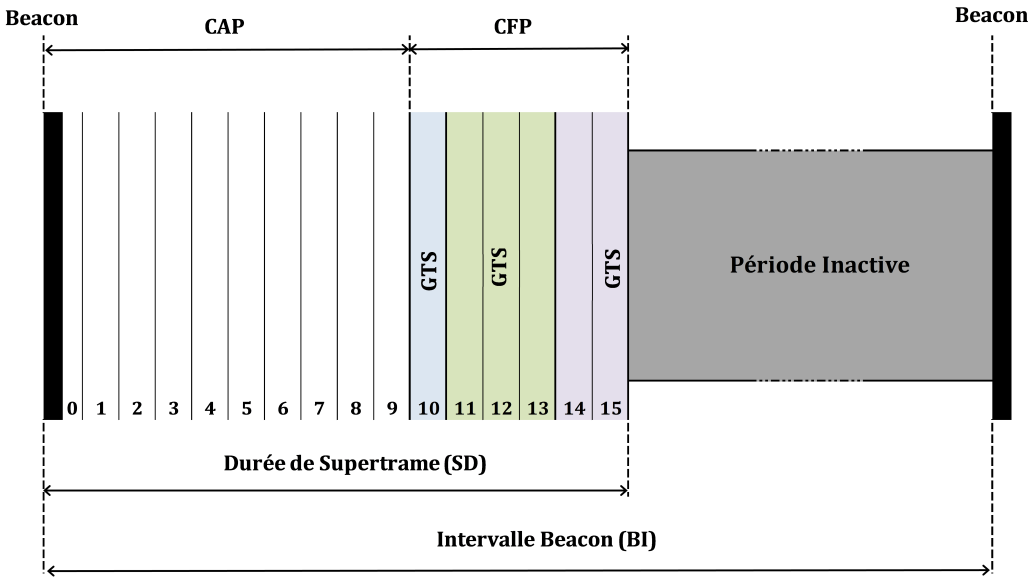


FIGURE 2.2: Un exemple de structure de supertrame

beacon comprend une période active (Active Period) et une période facultative dite inactive (Inactive Period). Pendant la période inactive, tous les appareils, y compris le coordinateur, entrent dans un état de faible puissance pour économiser de l'énergie. Dans la période active, l'appareil peut entrer dans un état actif selon les besoins et la configuration. La longueur de la période active est appelée durée de supertrame (SD : Superframe Duration) et divisée en 16 tranches de temps de taille égale (time slots).

Ces tranches sont appelées : emplacements, plages horaires, intervalles temporelles, laps de temps, section ou le plus souvent créneaux horaire (ou tout simplement créneaux). Cependant, nous allons les appelées slots tout au long de la thèse.

La durée de la supertrame comprend deux parties : la période d'accès avec contention (CAP : Contention Access Period) et la période sans contention (CFP : Contention Free Period). Les appareils suivent la CSMA/CA fendue pour accéder au support dans la CAP et poursuivent la méthode TDMA avec une taille maximale de 7 slots dans la CFP. Les slots CFP, également appelés slots horaires garantis (GTS : Guaranteed Time Slot), pourraient être réservés de manière FCFS par les dispositifs qui ont besoin d'une bande passante dédiée.

Figure 2.2 montre un exemple de la structure de la supertrame.

La durée de supertrame (SD) et l'intervalle beacon (BI) dans un PAN sont caractérisés respectivement par l'ordre de la supertrame (SO : Superframe Order) et l'ordre de beacon (BO : Beacon Order). En substance, la paire (SO, BO) résume les caractéristiques tem-

porelles de la supertrame. Les équations (2.1) et (2.2) décrivent la durée de supertrame et l'intervalle de beacon en fonction de ces deux paramètres.

$$BI = aBaseSuperframeDuration \times 2^{BO} \tag{2.1}$$

$$SD = aBaseSuperframeDuration \times 2^{SO} \tag{2.2}$$

Où $0 \leq SO \leq BO \leq 14$.

aBaseSuperframeDuration correspond à une durée de 960 symboles, ce qui équivaut à $15,36$ ms pour la bande de fréquences $2,4$ GHz, ce qui sera considérée tout au long de ce travail.

En 2012, une amélioration de la norme [43] a défini d'autres modes MAC, dont l'un prend en charge une structure de supertrame modifiée similaire à celle du MAC IEEE 802.15.4. Cependant, le nouveau mode introduit une complexité de mise en œuvre et souffre de l'absence de périodes inactives. De plus, de nombreuses technologies ont implémenté commercialement le MAC IEEE 802.15.4 comme norme sous-jacente et ont conservé leur implémentation de l'IEEE 802.15.4 pour sa faible complexité [44]. Par conséquent, nous adopterons le MAC IEEE 802.15.4 dans ce travail.

Le mode sans beacon de l'IEEE 802.15.4

Également appelé mode non fendu (unslotted mode) dans lequel les nœuds effectuent un CSMA/CA non fendue pour communiquer de manière distribuée.

Dans ce cas, un coordinateur ne doit pas transmettre de beacons, sauf à la réception d'une requête de demande de beacon, et BO avec SO sont tous les deux mis à 15. En outre, les GTS ne sont pas autorisés.

2.2 Vue d'ensemble des attaques de couche MAC ciblant le mode beacon de la norme IEEE 802.15.4

Étant donné les composants du réseau, on retrouve les attaques orientées vers les appareils ordinaires et celles ciblant le coordinateur de réseau :

2.2.1 Attaques visant les appareils ordinaires

Dans la période CAP

Ces attaques ont tendance à altérer le bon fonctionnement de la CSMA-CA non fendue en appliquant ce que nous appelons les attaques d'injustice [45].

Un nœud malveillant peut effectuer une attaque de manipulation du temps d'attente (back-off) dans laquelle il choisit une courte durée au lieu de sélectionner une période d'attente aléatoire dans sa fenêtre de contention. L'adversaire peut aller plus loin en omettant entièrement le compte à rebours du back-off, ce qui signifie en fait quitter le protocole CSMA-CA. Ce faisant, l'adversaire détourne l'accès au canal en s'assurant qu'il soit toujours accordé une priorité plus élevée pour accéder au canal que les nœuds légitimes. Cette attaque augmente à la fois le temps d'attente des nœuds légitimes lors de l'accès au canal et la consommation énergétique des nœuds lors de la réception des données de l'adversaire.

Dans le but d'obtenir plus de privilèges que les nœuds légitimes, un adversaire peut effectuer la manipulation de la procédure d'évaluation du canal (CCA : Clear Channel Assessment) en écoutant la liberté du canal pendant une seule période d'attente plutôt que deux périodes comme le protocole le spécifie, ou même sauter complètement la procédure CCA afin de commencer immédiatement la transmission à la fin du compte à rebours aléatoire. Cela pourrait potentiellement provoquer des collisions si le canal n'est pas libre [46][47].

Dans la période CFP

Les attaques les plus populaires qui visent à perturber les communications sur la CFP sont les attaques dites GTS. Ces attaques relèvent de deux catégories d'attaques ; épuisement et collision.

Après avoir réalisé la synchronisation avec le coordinateur de réseau, au moyen de la réception de trames de balise, l'adversaire vérifie le début et la longueur du slot dans le descripteur GTS de la victime. Ces informations sont présentes dans la trame beacon une fois que la victime est un nœud associé légitime. L'adversaire peut donc brouiller le slot de la victime et corrompre toute la communication en cours [48].

Les attaques GTS sont considérées comme une forme de brouillage sélectif dans les réseaux IEEE 802.15.4. Un brouillage sélectif où la sélection du slot cible est basée sur sa longueur ou son ID de propriétaire.

Collision avec les trames de contrôle

Le but de l'adversaire en heurtant les trames de contrôle pourrait être d'épuiser la victime comme dans le cas d'une collision avec les acquittements (ACKs) où la victime est épuisée par les retransmissions de trames. Les attaques MITM (Man In The Middle) bénéficient de la collision des trames de contrôle pour usurper les ACKs et injecter des données.

Un adversaire dans la portée radio du coordinateur peut brouiller les demandes d'association ou d'allocation GTS d'un certain nœud pour contrecarrer sa disponibilité de réseau. Si la portée radio de l'adversaire couvre également la cible, celui-là peut aller plus loin en brouillant les trames beacon et rend la victime orpheline [45].

2.2.2 Attaques visant le coordinateur

Dans les réseaux de capteurs sans fil de l'IEEE 802.15.4, chaque coordinateur personnel possède un identifiant (PANid) connu de tous les membres du réseau personnel. S'il existe plus d'un coordinateur PAN fonctionnant dans le même espace opérationnel personnel (POS : Personal Operating Space), un conflit PANId peut se produire. Si un tel conflit PANId se produit, le coordinateur PAN peut détecter le conflit via les trames beacon reçues ou l'un des nœuds membres peut notifier le coordinateur PAN lors de la réception du signal de deux coordinateurs PAN avec le même PANId. En cas de notification, le coordinateur PAN exécute la procédure de résolution de conflit. Ce mécanisme couvre principalement les balayages de canaux et la procédure de réalignement du coordinateur qui comprend le choix d'un nouveau PANId et sa diffusion à tous les nœuds membres. Après la resynchronisation avec les trames beacon, le réseau est prêt à communiquer de manière stable, ce qui implique que la résolution du conflit est terminée.

Un dispositif adverse peut fréquemment envoyer de faux messages de notification de conflit au coordinateur et obliger ce dernier à exécuter la procédure de résolution de conflit. De cette façon, l'attaquant peut utiliser ces faux messages pour épuiser le coordinateur ou empêcher/retarder la communication entre les appareils et le coordinateur. Cette attaque est typiquement appelée attaque de conflit de PANId [48].

2.2.3 Attaques visant le réseau en général

La stéganographie est utilisée pour cacher l'existence de données. Ceci est accompli en incorporant des données secrètes dans des données existantes, appelées données de couverture. Les destinataires non concernés passeront le message car ils ne sont pas conscients de

l'existence du message secret. Une fois que le destinataire final aura reçu l'ensemble complet des messages, il composera le message caché et exécutera son contenu.

Dans l'IEEE 802.15.4, il existe de nombreux bits réservés dans les trames MAC et PHY qui peuvent prendre en charge un message masqué. Ce dernier pourrait être une heure d'exécution d'une DDoS ou un avertissement sur le soupçon d'une attaque en cours [49].

2.3 Conclusion

La technologie IEEE 802.15.4 se distingue par sa faible puissance énergétique et sa mode de communication garantie GTS. Ces qualités répondent aux contraintes de performance et énergétique caractérisant les réseaux corporels sans fil et convient leur modèle centré. Cependant, comme n'importe quelle technologie TDMA, le mode beacon de l'IEEE 802.15.4 souffre des attaques de disponibilité, ce qui aura un impact négatif sur l'acceptabilité dans les divers champs d'application, y compris les WBANs.

Par conséquent, la sécurisation de l'IEEE 802.15.4 présente une tâche primordiale et contribue de manière directe ou indirecte à la sécurisation des WBANs. De ce fait, nous consacrons les trois prochains chapitres à la protection active et pro-active des réseaux corporels qui exploitent le mode beacon de la technologie concernée pour procéder à la communication.

Chapitre 3

Une nouvelle GTS attaque avec une méthode d'atténuation pour les réseaux corporels basés sur l'IEEE 802.15.4

Les énormes progrès des systèmes microélectromécaniques (MEMS) et de la miniaturisation en général, ainsi que la nécessité urgente de réduire les coûts de soins de santé et d'assistance aux personnes âgées, sont les principaux contributeurs à l'émergence d'une nouvelle catégorie de réseau ; les réseaux corporels sans fil (WBAN).

Compte tenu de l'exigence de faible puissance des WBANs, l'IEEE 802.15.4 a prouvé son avantage économique parmi les technologies médicales précédemment adoptées telles que Bluetooth et Wi-Fi.

Les implémentations existantes reposent sur le mode non-beacon de l'IEEE 802.15.4 pour poursuivre les communications, même si le mode beacon est plus économe en énergie. La nature centralisée du mode beacon aide les nœuds à se mettre en état de veille lorsqu'il n'y a pas de communication courante et correspond bien au modèle centré du WBAN.

Le brouillage sélectif est une attaque réactive qui exploite la connaissance du protocole et la nature partagée du support pour contrecarrer la communication dans les réseaux sans fil. Dans cette attaque, l'adversaire effectue des interférences intentionnelles tout en économisant de l'énergie en exécutant l'attaque de manière sélective pendant de courtes périodes de temps. Ces périodes sont choisies en fonction de la connaissance préalable de la fonctionnalité du protocole [50].

En mode beacon de l'IEEE 802.15.4, un brouilleur sélectif choisit un slot de la période sans conflit (CFP) pour corrompre sa communication et passe à l'état inactif le reste du

temps. Cette forme de brouillage sélectif, ciblant exclusivement le mode beacon de la norme, est appelée attaque GTS [7]. Cette attaque est, à la fois, facile à exécuter et cause des dommages considérables.

Les attaques GTS peuvent être classées en fonction de critère de sélection des cibles et les solutions sont soit centralisées, soit distribuées.

Dans [7], les auteurs ont identifié une nouvelle attaque qui vise à corrompre la communication GTS entre les appareils simples et le coordinateur du réseau.

Après avoir atteint la synchronisation avec le coordinateur, en écoutant les trames beacon, l'attaquant peut intercepter le descripteur GTS dans ces trames pour connaître exactement le début et la longueur d'un slot GTS pour un certain nœud. L'attaquant dirigera alors une attaque de brouillage sélectif vers le slot sélectionné afin de dégrader la qualité de la liaison. Dans ce travail, aucun critère de sélection n'a été défini pour le prélèvement du slot de temps cible.

Un travail étendu prenant en compte le nombre d'attaquants et adoptant la longueur des slots des nœuds comme critère de sélection [8] a été introduit par les mêmes auteurs. Ils ont défini quatre scénarios possibles : un attaquant intelligent (OIA : One Intelligent Attacker), un attaquant aléatoire (ORA : One Random Attacker), deux attaquants intelligents (TIA : Two Intelligent Attackers) et deux attaquants aléatoires (TRA : Two Random Attackers). Dans les cas intelligents, l'attaquant sélectionne le plus long slot temporel dans la CFP pour le brouiller. Dans le cas de TIA, les deux attaquants collaborent pour sélectionner le plus long et le deuxième plus long slots dans le but de réduire, autant que possible, l'utilisation de la bande passante du réseau. Dans les cas aléatoires, l'attaquant choisit le slot au hasard. Il n'y a pas de collaboration entre les attaquants dans TRA, ce qui conduit à un possible chevauchement de brouillage. Les attaques ont été évaluées en termes de rapport de slots corrompus et de consommation énergétique de l'attaquant. Comme prévu, les attaques intelligentes ont surpassé les attaques aléatoires dans les deux métriques.

Même si les auteurs ont défini une nouvelle attaque avec quatre scénarios différents, l'évaluation était médiocre et limitée. Par exemple, le taux de slots corrompus pour OIA était de 50,48%, ce qui est loin d'être un scénario réaliste. Dans un réseau réel avec de nombreux nœuds, la probabilité qu'un nœud soit seul dans la CFP est très faible. La raison derrière la valeur élevée ci-dessus est la jointure progressive au réseau, effectuée par les nœuds, et un temps de simulation très court par rapport à la durée de la supertrame. Un autre exemple, qui illustre la subjectivité des résultats, est que l'OIA a surpassé le TRA dans les deux mesures d'évaluation. Théoriquement, deux attaquants aléatoires faites brouiller

presque le double de la longueur moyenne de tous les slots. Si la longueur du slot le plus long dans la CFP est supérieure au double du moyen, ce qui était le cas dans les données d'évaluation, TRA suivra à peine le rythme du OIA.

R. Daidone et al. [9] ont introduit une nouvelle attaque GTS avec un schéma GTS résistant au brouillage sélectif (SJRG : Selective Jamming Resistant GTS scheme). En adoptant l'ID du nœud comme critère de sélection, Sniper Attack cible sélectivement certains slots dans la CFP.

Dans le but de réduire le dommage de Sniper Attack et d'autres attaques GTS, les auteurs ont suggéré un nouveau schéma d'allocation GTS, censé être résistant à de telles attaques. L'objectif principal de SJRG est de répartir le dommage subi par une victime sur tous les nœuds actifs dans la CFP. À cette fin, SJRG force l'attaquant à passer à une attaque de brouillage aléatoire.

SJRG consiste en deux étapes : (1) la sécurisation des informations d'allocation GTS dans les trames beacon ; et (2) de randomiser l'allocation de slots en modifiant l'ordre de ceux-ci dans chaque supertrame. La première étape a été réalisée en déplaçant les informations liées au GTS vers la partie donnée de la trame beacon pour qu'elles soient cryptées et authentifiées par les services de sécurité IEEE 802.15.4. La dernière étape est le cœur de SJRG qui rend l'attaquant aveugle dans son activité.

Le travail a été évalué dans un scénario réel à l'aide des appareils Tmote Sky. Les considérations comprenaient le taux de livraison de paquets, empreinte mémoire, délai et la consommation supplémentaire d'énergie par paquet. Le taux de livraison de paquets en présence de SJRG était proche de celui analytique, et toutes les autres mesures étaient raisonnables. Le principal inconvénient de ce travail était de modifier l'allocation GTS et les fonctionnalités du service de sécurité de l'IEEE 802.15.4. De plus, SJRG améliore le taux de livraison de la victime, cependant, le nombre de nœuds attaqués par supertrame s'augmentera considérablement. En fait, la durée du brouillage peut couvrir de nombreuses parties de différents slots en raison de la nature aveugle de l'attaque.

JAMMY [10] est une solution distribuée et dynamique pour les attaques de brouillage sélectif dans les WSN basés sur TDMA.

Afin d'éviter l'exposition continue aux signaux de brouillage, JAMMY utilise le même principe de SJRG pour modifier l'ordre des slots, mais cette fois, de manière distribuée. Contrairement à SJRG, dans lequel les nœuds s'appuient sur les informations de la trame beacon pour connaître leur ordre de slot, les nœuds de JAMMY génèrent indépendamment la même séquence de slots de manière cohérente. Les auteurs ont affirmé que l'utilisation d'un

générateur de séquences pseudo-aléatoires localement dans chaque nœud, pour connaître la position du slot suivant, est plus économe en énergie que de le recevoir à l'arrivée de chaque supertrame.

Même si les deux approches centralisées et distribuées fournissaient le même taux de paquets corrompus, l'évaluation analytique de l'approche centralisée, en termes de consommation d'énergie, a révélé une surcharge supplémentaire.

JAMMY peut être plus économe en énergie dans le cas de TDMA. Cependant, dans le scénario de transmission GTS de l'IEEE 802.15.4, les trames beacon sont transmises dans tous les cas. Par conséquent, la surcharge de communication dans l'approche distribuée sera la même que celle centralisée. En fait, il y aura une surcharge de traitement supplémentaire pour chaque nœud dans le cas distribué. De plus, pour générer la même séquence dans tous les nœuds, une phase d'initialisation est nécessaire afin d'échanger les paramètres initiaux. Cela peut être vulnérable du point de vue de sécurité. Par conséquent, l'utilisation de JAMMY dans un schéma d'allocation GTS est non seulement inutile et inefficace sur le plan énergétique, mais c'est également plus menaçant pour la sécurité.

M. Tiloka et al. [11] ont introduit le mélange distribué (DISH : DIstributed SHuffling) pour faire face aux attaques de brouillage sélectif dans les réseaux TSCH IEEE 802.15.4e. Les réseaux de saut de canal à slot temporel (TSCH : Time Slot Channel Hopping) combinent un accès temporisé de l'IEEE 802.15.4 avec une possibilité de saut de canal. Cette combinaison offre une grande capacité réseau et garantit une latence prévisible. DISH change l'ordre des slots et l'utilisation des canaux de manière aléatoire, distribuée et par supertrame. L'analyse quantitative de DISH a montré son efficacité contre le brouillage sélectif pour différentes configurations de réseau.

À partir de la littérature revue, nous concluons que l'idée principale des solutions proposées pour les attaques de brouillage ciblant le modèle TDMA est la randomisation des positions des slots.

3.1 Motivation et faits saillants

La sécurité est l'un des aspects les plus importants à prendre en compte dans le déploiement d'un réseau. Elle englobe l'adoption de techniques de protection pour les violations connues et la découverte d'éventuelles vulnérabilités inconnues. Par mesure de sécurité, les entreprises recrutent même des experts en sécurité pour évaluer la robustesse de la sécurité de leurs réseaux et systèmes d'information.

La faible consommation d'énergie et le modèle centré du mode beacon de l'IEEE 802.15.4 font de cette technologie un choix potentiel pour déployer les réseaux corporels sans fil. Par conséquent, la sécurisation du premier aboutit, directement ou indirectement, à la sécurisation du second.

Dans le but d'augmenter la sécurité du mode beacon de l'IEEE 802.15.4, nous avons analysé les fonctionnalités du protocole et la structure de la supertrame pour extraire les éventuelles faiblesses qu'un intrus peut exploiter pour perturber la communication de l'utilisateur. En conséquence, nous avons introduit une version optimisée d'une attaque introduite précédemment qui cible la disponibilité du réseau. De plus, on a proposé une contre-mesure d'atténuation afin d'atteindre notre objectif dans ce travail.

Nous avons soutenu notre travail avec une simulation extensive prenant presque toutes les configurations de réseau possibles et nous avons fourni quelques preuves mathématiques nécessaires.

3.2 Modèle et analyse du réseau

Pour comprendre la logique derrière l'attaque proposée et sa contre-mesure associée, une vue claire du modèle de réseau et du schéma de communication est nécessaire.

Dans ce travail, on considère un réseau corporel sans fil, constitué d'un ensemble de dispositifs capteurs qui transmettent périodiquement leurs mesures physiologiques à une entité centrale appelée coordinateur. Ce réseau forme une topologie en étoile et utilise le schéma GTS de l'IEEE 802.15.4 pour la livraison des paquets (Figure 3.1).

Soit N le nombre de nœuds (appareils) dans le réseau. Pour un nœud i ($1 \leq i \leq N$), on note par D_i, P_i et S_i, l'heure d'arrivée du premier paquet, la période d'inter-départ des paquets (le temps entre deux arrivées successives de paquets) et la durée du slot de nœud, respectivement. Par conséquent, le premier paquet sera généré dans la couche application à D_i, le deuxième à $D_i + P_i$ et le troisième à $D_i + 2 \times P_i$, et ainsi de suite. Nous nous référons à la durée de l'intervalle de beacon par la notation BI.

Théoriquement, un nœud i transmettra sa j^{me} trame à $D_i + (j-1) \times P_i$. Cependant, le temps réel de transmission du paquet pourrait être différent en raison de la structure limitante de la supertrame IEEE 802.15.4. En fait, si un paquet arrive à la couche MAC lorsque l'appareil est hors de son slot ; la transmission sera reportée à la prochaine arrivée du slot du nœud.

Ce délai introduit dépend de trois facteurs :

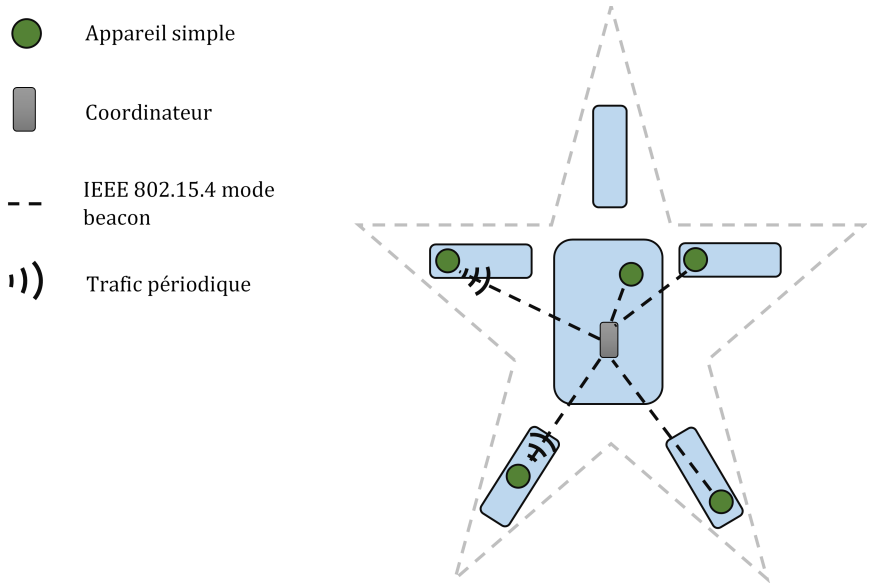


FIGURE 3.1: Réseau corporel sans fil à topologie en étoile

(1) La paire $(D_i \ mod_{réel} \ BI, P_i \ mod_{réel} \ BI)$

(2) Les caractéristiques temporelles de la supertrame (SO, BO)

(3) La longueur du slot de l'appareil en slots GTS

Lorsque $mod_{réel}$ est le dernier reste positif après avoir effectué des soustractions successives. Algorithme 1 montre comment $mod_{réel}$ et $div_{réel}$ sont calculés.

Algorithme 1 Calcul de $A \, mod_{réel} \, B$ et $A \, div_{réel} \, B$

```
1: lire (A, B)                          ▷ deux nombres réels
2: mod ← A
3: div ← 0
4: tant que A − B > 0 faire
5:     mod ← A − B
6:     div + +
7: fin tant que
8: afficher (mod, div)
```

Ces délais s'accompagnent d'un certain comportement qui révèle une vulnérabilité sérieuse en mode de transmission GTS.

Dans les sections suivantes, nous présentons nos principales contributions, à savoir, le brouillage en tête de slot (SHJA : Slot-Head Jamming Attack) et le départ aléatoire de paquets (RPD : Random Packet Departure) [16] et nous étudierons l'effet des facteurs ci-dessus tout au long de ce chapitre [17].

3.3 Brouillage en tête de slot (SHJA : Slot-Head Jamming Attack)

SHJA est une version efficace de l'attaque GTS qui, étant donné la version classique, produit presque le même dommage avec une activité d'attaque minimale.

Cette attaque repose sur deux aspects fondamentaux : une vulnérabilité facilement exploitable dans la fonctionnalité de base du mode GTS de l'IEEE 802.15.4 , et le chevauchement de la supertrame avec le temps d'inter-départ d'un certain nœud.

Fondamentalement, le mode GTS de l'IEEE 802.15.4 a deux effets sur le trafic périodique transporté :

(1) Effet supertrame : effet de la structure supertrame sur le modèle inter-arrivées des paquets.

(2) Effet du protocole : résultant du comportement de l'IEEE 802.15.4 lors de la transmission du trafic affecté par l'effet supertrame.

3.3.1 Vulnérabilité du mode de transmission GTS

Le protocole MAC de l'IEEE 802.15.4 transmet une trame au début du slot, intentionnellement, dans deux cas : (on entend par intentionnellement, que la trame n'était pas censée être envoyée au début du slot)

(1) Retransmission de trame

(2) Lorsqu'un paquet arrive à la couche MAC avant le démarrage du slot de l'appareil

Ce comportement introduit une sérieuse vulnérabilité pour un brouilleur sélectif à exploiter, car l'attaquant ne sera pas obligé de brouiller l'intégralité du slot pour garantir le succès de son attaque. Il lui suffira de ne brouiller que le début du slot.

Néanmoins, si le taux de trames MAC différées est faible, cette vulnérabilité ne présentera pas une menace de sécurité considérable. Dans le cas contraire, cela donnera aux adversaires la possibilité de causer presque autant de mal qu'un brouillage complet avec beaucoup moins d'épuisement des ressources.

Supposons que $P_i \; mod_{réel} \; BI \neq \; 0$ (l'autre cas sera discuté dans la sous-section suivante).

Il y a deux cas :

- Lorsque $P_i mod_{réel} BI > durée\_slot$:

Soit t_j le temps d'arrivée du paquet $j^{ème}$ qui s'est produite à l'intérieur du slot, donc :

$$\begin{aligned} t_{j+1} &= t_j + P_i \\ &= t_j + N \times BI + P_i mod_{réel} BI \end{aligned}$$

Où $N = P_i div_{réel} BI$.

Il est clair que $t_j + N \times BI$ arriverait dans la même position à l'intérieur du slot que t_j.

Puisque $durée\_slot < P_i mod_{réel} BI < BI$, t_{j+1} arrivera, certainement, au-delà du slot.

Nous concluons que quelle que soit l'heure d'arrivée du paquet, si cela se produit à l'intérieur du slot, la prochaine arrivée aura lieu en dehors du slot. Cela se traduit par au moins 50% des arrivées au-delà des slots.

- Quand $P_i mod_{réel} BI \leq durée\_slot$:

  Dans ce cas, le nombre d'arrivées au-delà des slots est proportionnel à $\frac{BI - durée\_slot}{BI}$.

  En prenant le pire scénario (quand BI prend sa plus petite valeur et $durée\_slot$ prend sa plus grande valeur en termes de nombre de slots GTS) ce devrait être $\frac{16-7}{16} = 56.25\%$.

Même si nous avons envisagé le pire scénario dans les deux cas, le nombre d'arrivées au-delà des slots reste élevé et représente au moins la moitié du volume de trafic. Endommager cette quantité de trafic est très nocif et n'est pas tolérable.

3.3.2 L'algorithme de SHJA

En exploitant la vulnérabilité mentionnée ci-dessus, l'adversaire peut corrompre la majorité du trafic d'un nœud spécifique.

Dans SHJA, l'adversaire brouille régulièrement la tête de slot du nœud victime et arête le brouillage dans le reste de celui-ci. Cela ferait l'attaquant gagner des ressources supplémentaires pour effectuer l'attaque pendant la plus longue période. Algorithme 2 montre comment le brouilleur effectue l'attaque.

Le seul moyen d'éviter le brouillage est d'éviter le report de transmission lui-même. Ceci peut être réalisé en faisant que D_i se produise à l'intérieur du slot et en choisissant une période inter-départ qui soit un multiple de l'intervalle de beacon, c'est-à-dire ($S_i\_début + N \times BI \leq D_i < S_i\_début + S_i + N \times BI$) et ($P_i mod_{réel} BI = 0$), où $S_i\_début$ est la différence entre l'heure de début du slot et celle de sa supertrame englobante. Cependant, en choisissant D_i et P_i satisfaisant les conditions ci-dessus, l'attaque sera encore plus réussie et plus facile qu'avant.

Algorithme 2 Brouillage en tête de slot (SHJA)

```
1: ▷ Phase d'initialisation
2: selectSlot()                          ▷ à base du nœud ID où de la taille du slot
3: attendreArrivée(début_slot)           ▷ dans la supertrame actuelle ou suivante
4: établir (Temporisateur, durée_intervalle_beacon)▷ quand l'attente se termine
5: ▷ Procédure de brouillage périodique
6: procédure EXPIRÉ(Temporisateur)▷ exécuté à l'expiration de la temporisateur
7:     établir (Temporisateur, durée_intervalle_beacon)
8:     seRéveiller()
9:     Brouiller_Tête_Slot()
10:    sommeiller()
11: fin procédure
```

Puisque $P_i mod_{réel} BI = 0$, l'arrivée du paquet prendra la même position dans le slot tout le temps. Par conséquent, l'adversaire peut atteindre un taux de corruption de 100% en brouillant régulièrement la même partie du slot.

On note que SHJA ne prend aucun critère de sélection pour choisir sa cible. SHJA, en fait, est une version améliorée des attaques GTS. À cet égard, nous introduisons trois nouvelles versions de l'attaque de brouillage GTS, à savoir, le brouillage intelligent en tête de slot (SHJIA : Slot-Head Jamming Intelligent Attack), le brouillage aléatoire en tête de slot (SHJRA : Slot-Head Jamming Random Attack) et l'attaque Sniper en tête de slot (SHJSA : Slot-Head Jamming Sinper Attack). La figure 3.2 illustre ces nouvelles attaques dans le contexte globale.

3.3.3 Exploitation du modèle de transmission déterministe pour augmenter l'efficacité de SHJA

SHJA exploite le comportement de la norme en cas d'arrivée au-delà slot pour diminuer la durée du brouillage. Cependant, le modèle de transmission déterministe imposé par la structure de la supertrame n'était pas encore exploité puisque l'attaque doit être effectuée dans chaque supertrame.

Un attaquant peut se servir de certaines propriétés mathématiques pour éviter le brouillage continu et effectue l'attaque dans un nombre limité de supertrames.

Étant donné que les transmissions sont effectuées exclusivement dans le slot du noeud, l'attaquant peut exploiter les caractéristiques du nombre de supertrames séparant deux émissions de trames successives afin de réaliser des attaques plus sophistiquées.

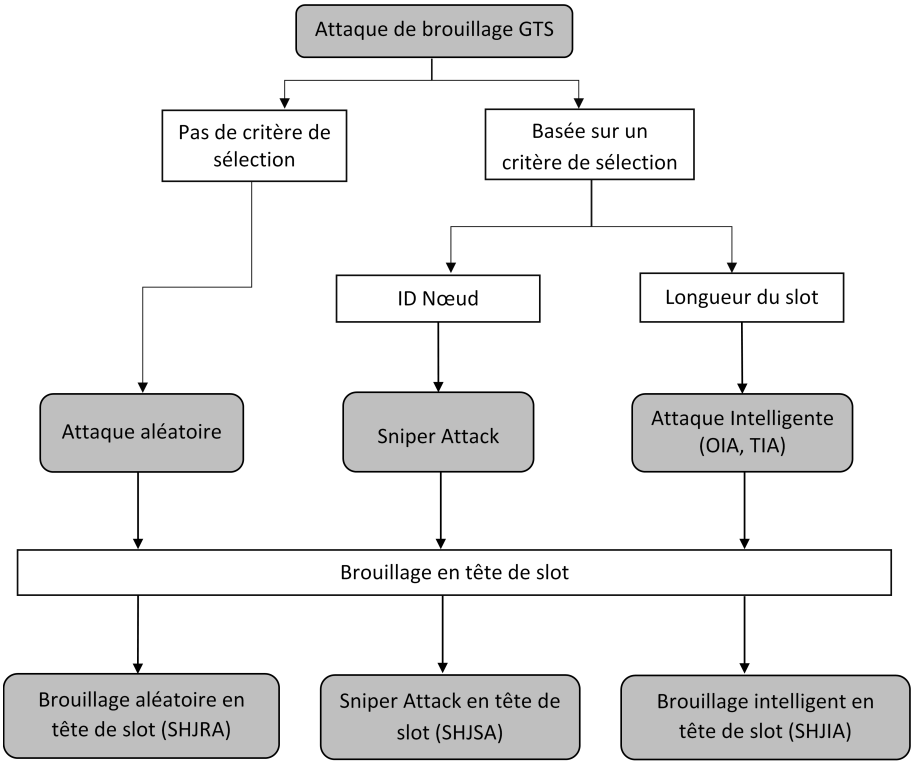


FIGURE 3.2: Nouvelles versions de brouillage GTS

Par exemple, on peut démontrer que ce nombre ne prend que deux valeurs : $P_i div_{réel} BI$ et $P_i div_{réel} BI+1$ (voir l'annexe A). Par conséquent, en écoutant deux transmissions successives, nous pouvons obtenir un encadrement de la valeur de $P_i div_{réel} BI$.

Soit N le nombre de supertrames séparant deux transmissions successives et N_i le nombre de supertrames correspondant au $i^{ème}$ arrivée de paquet ($N_0 = N$).

Étant donné les deux valeurs que N peut prendre, la valeur N_1 est $N_0 + N - 1$, $N_0 + N$ ou $N_0 + N + 1$ et N_2 peut prendre les valeurs $N_1 + N - 1$, $N_1 + N$ ou $N_1 + N + 1$ et ainsi de suite. Donc, N_1 prendra $2 \times N - 1$, $2 \times N$ ou $2 \times N + 1$ et N_2 prend $3 \times N - 2$, $3 \times N - 1$, $3 \times N$, $3 \times N + 1$ ou $3 \times N + 2$.

La formule généralisée des valeurs possibles que N_i peut prendre est de la forme :

$$N_i = (i + 1) \times N - i + k \tag{3.1}$$

Où $0 \leq k \leq 2i$.

Après avoir trouvé N en écoutant le support, un attaquant peut brouiller toutes les supertrames d'ordre $(i + 1) \times N - i + k$ pour garantir 100% de corruption jusqu'à ce que l'attaque se transforme en une attaque continue (le nombre de supertrames brouillées couvre

N). Ensuite, l'attaquant ne doit traquer qu'une seule transmission pour répéter la procédure puisqu'il fait déjà obtenir N. Algorithme 3 décrit la procédure de l'attaque.

Algorithme 3 Brouillage en tête de slot optimisé

```
1: trouver (N)                                  ▷ deux arrivées successives de paquets
2: i ← 0
3: tant que 2 * i ≤ N faire ▷ nous n'avons pas encore atteint le brouillage continu
4:     brouillePaquetsOrdre( (i + 1) × N − i + k )    ∀k ≤ 2 * i
5:     i + +
6: fin tant que
7: écouterUnPaquet()
8: goto(2 :)
```

Algorithme 3 exploite une propriété mathématique simple pour optimiser les dépenses en ressources tout en exécutant l'attaque efficacement. Un attaquant peut exploiter d'autres propriétés complexes pour produire des attaques encore plus économiques. À titre d'exemple, le nombre de supertrames entre deux transmissions successives suit une séquence bien définie dans laquelle l'une des valeurs possibles, $P_i div_{réel} BI$ où $P_i div_{réel} BI + 1$, ne peut pas arriver deux fois successives. Par conséquent, N_i aura moins de valeurs possibles à prendre, ce qui va sûrement affecter le nombre de paquets de brouillage.

Une approche totalement différente consiste à traquer les variations de N_i jusqu'à ce qu'on soit sûr d'avoir un modèle répétitif. L'attaquant peut alors corrompre tout le trafic sans aucune autre écoute ultérieure. Cependant, il est difficile de déterminer si on a atteint un modèle fermé. De plus, la procédure d'écoute continue peut prendre beaucoup de temps en raison de la relation arbitraire entre BI et P_i.

Le principal inconvénient des algorithme de suivi du modèle de communication est la nécessité d'être à l'intérieur de la portée de communication du coordinateur et celle de la victime à la fois. En revanche, en SHJA continue, l'attaquant n'a qu'à se trouver dans la portée du coordinateur, ce qui est relativement large par rapport à l'intersection des deux portée. La figure 3.3 montre les emplacements possibles de l'attaquant dans le contexte de brouillage continu et optimisé.

La figure 3.3 montre que l'amélioration de l'efficacité de l'attaque coûte à l'attaquant une partie de sa flexibilité de localisation.

Nous notons que les travaux antérieurs ont simulé le brouillage de slot complet en (1) envoyant un paquet dans la tête du slot de la victime ; (2) faire coïncider l'heure du premier

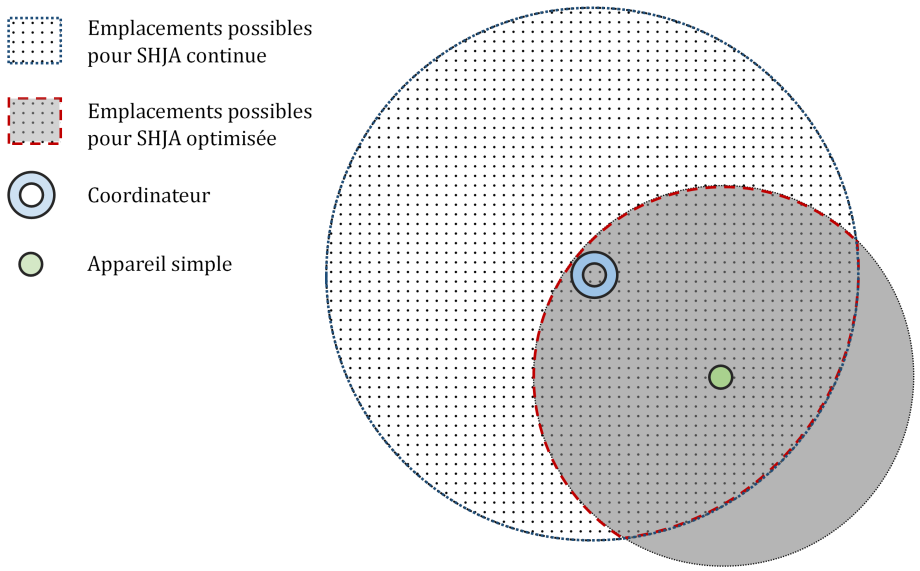


FIGURE 3.3: Emplacements possibles de l'attaquant pour SHJA continue et optimisée

paquet avec l'heure d'arrivée de la trame beacon ; et (3) choisir une période d'inter-départ égale à l'intervalle de beacon.

En faisant cela, ils garantissaient un brouillage complet sans utiliser de paquets extra-larges. Par conséquent, leur action se fait dans le cadre de faciliter l'évaluation des performances et non pas comme une technique d'attaque comme nous l'avons fait. Cela explique pourquoi ils prennent la configuration $D_i mod_{réel} BI = 0$ et $P_i mod_{réel} BI = 0$ dans la procédure d'évaluation. Il est important de faire la distinction entre le premier cas, qui est un acte de facilitation, et le second cas, qui est une technique intentionnellement proposée dans laquelle nous avons également considéré la relation arbitraire entre P_i et BI.

Dans la section suivante, nous présentons notre contre-mesure qui atténue les dommages SHJA à $\frac{durée\_brouillage}{durée\_slot}$, théoriquement.

3.4 Départ aléatoire de paquet (RPD : Random Packet Departure)

La transmission intentionnelle au début de slot aura lieu en deux cas : la retransmission et l'arrivée au-delà du slot. Par conséquent, pour éviter les tirs SHJA, un appareil peut suivre l'occurrence de ces deux événements dans le but d'envoyer le paquet à un moment différent dans le slot.

Un nœud i peut effectuer en continu une simple comparaison entre la prochaine arrivée P_i (de la forme $D_i + N \times P_i$) et le début/fin du slot de la supertrame courante pour évaluer si elle aura lieu ou non à l'intérieur du slot.

Soit M et N les compteurs des arrivées de supertrame et de P_i, respectivement, et Délai une durée aléatoire :

- Si $D_i + N \times P_i \leq S_i\_début + M \times BI$ alors le paquet sera transmis à $S_i\_début + M \times BI + Délai$

- Si $D_i + N \times P_i > S_i\_début + S_i + M \times BI$ alors le paquet sera transmis à $S_i\_début + (M + 1) \times BI + Délai$

Nous pouvons simplifier la procédure en randomisant tous les départs de paquets, qu'ils aient été différés, retransmis ou non.

RPD peut être implémenté dans la couche application ou directement intégré dans les fonctionnalités de la couche MAC. Cette flexibilité fait de RPD une solution très pratique.

L'algorithme 4 résume la procédure RPD de transmission de paquets dans le cas d'une implémentation en couche application.

Dans cet algorithme, *dur_transm_paquet* est le temps suffisant pour envoyer tous les bits d'un paquet avec son ACK associé incluant tout le matériel IFS. *ST* réfère à Super-Trame.

Algorithme 4 Départ aléatoire de paquet (couche application)

```
1: si expiré (TemporisateurInterDépart) alors▷ arrivée de temps de transmission
2:     T ← heure_actuelle()
3:     générer (temps_aléatoire)
4:     ▷ temps_aléatoire < dur_slot − dur_transm_paquet
5:     si T < début_slot_ST_courante alors
6:         attendreArrivée(début_slot_ST_courante + temps_aléatoire)
7:     fin si
8:     si T > fin_slot_ST_courante − dur_transm_paquet alors
9:         attendreArrivée(début_slot_ST_suivante + temps_aléatoire)
10:    fin si
11:    transmettrePaquetCoucheInférieur()     ▷ quand l'attente est terminée
12: fin si
```

Dans ce cas, la couche application doit émuler la supertrame de la couche MAC afin de savoir si elle doit envoyer immédiatement le paquet (nous sommes au milieu de notre slot) ou le conserver jusqu'au prochain slot (paquet différé). Dans ce dernier cas, on attend un temps supplémentaire aléatoire avant d'envoyer le paquet vers le bas.

Parallèlement à cela, la couche application doit savoir ce qu'il faut, pour un paquet, pour atteindre la couche physique. Ce peu de temps est de la plus haute importance. Il englobe le temps de propagation inter-couches et le temps de construction des en-têtes dans toutes les couches intermédiaires. Ignorer ce temps lors du calcul de l'heure de départ dans la couche application peut provoquer une arrivée au-delà slot dans la couche MAC. Ceci conduit ce dernier à reporter à nouveau la transmission à la supertrame suivante. Cependant, cette fois, la transmission aura lieu au début du slot car la couche MAC n'a pas connaissance du protocole RPD.

Le deuxième problème avec le RPD en couche application est la retransmission des paquets. Pour permettre à RPD de randomiser les retransmissions de paquets, une approche inter-couche (cross-layer) doit être activée. À cet égard, la retransmission de la couche MAC doit être désactivée et un processus de déclenchement de retransmission doit être émulé par la couche application. Ces détails ne sont pas pris en compte dans l'algorithme 4.

Nous pouvons éviter tous ces soucis en intégrant RPD directement dans la couche MAC (Algorithm 5). La procédure RPD sera beaucoup plus simple dans ce cas puisque RPD a une synchronisation fine avec la couche MAC. De plus, les informations qui déterminent si un paquet doit être soumis à RPD ou pas sont déjà disponibles.

Le seul problème avec RPD en couche MAC c'est qu'il modifie la fonctionnalité de la norme. Cependant, nous pensons que RPD n'apporte pas une énorme modification à la norme et qu'il est abordable voire même indispensable.

3.5 Évaluation des performances

Dans cette section, nous évaluons notre travail en prenant différentes métriques en considération. À cette fin, on a envisagé différents scénarios de simulation et les résultats étaient cohérents avec nos prévisions analytiques.

3.5.1 Configuration de la simulation

Nous avons simulé SHJA et RPD dans l'implémentation IEEE 802.15.4 [51], qui est incluse dans le framework INETMANET 2.0 [1]. Cette implémentation prend en charge le mode beacon avec pleine GTS fonctionnalité. On a importé le framework ci-dessus dans OMNet ++ [2] pour procéder à nos simulations.

1. http ://github.com/aarizaq/inetmanet-2.0
2. https ://www.omnetpp.org

Algorithme 5 Départ aléatoire de paquet (couche MAC)

```
1: si expiré (temporisateurDébutSlot) alors          ▷ mon slot vient de commencer
2:     T ← heure_actuelle()
3:     fini ← faux
4:     tant que NON fini faire          ▷ la tâche RPD n'est pas encore terminée
5:         paquet ← tête(MAC_QUEUE)
6:         si paquet ≠ NUL alors
7:             si retransmis(paquet) ou tempsArrivée(paquet) < T alors
8:                 générer (temps_aléatoire)
9:                 attendreArrivée(T + temps_aléatoire)
10:            fin si
11:            seRéveiller()
12:            transmettrePaquetCoucheInférieur()
13:            sommeiller()                  ▷ quand la transmission se termine
14:            fini ← vrai
15:        fin si
16:        si expiré (temporisateurFinSlot) alors                ▷ la fin du slot
17:            fini ← vrai
18:        fin si
19:    fin tant que
20: fin si
```

Nous considérons sept nœuds qui, avec un coordinateur, forment une topologie en étoile. Chaque nœud du réseau occupe un slot des sept slot GTS. le Tableau 4.1 décrit les paramètres choisis pour toutes les simulations.

On a considéré quatre métriques d'évaluation :

- **Taux de paquets corrompus :** c'est le nombre de paquets corrompus par rapport au nombre total de paquets transmis.

- **Taux de Livraison de Paquets (PDR : Packet Delivery Ratio) :** c'est le nombre de transmissions réussies par rapport au nombre total de paquets.

- **Délai :** c'est la différence entre le moment où un paquet quitte réellement la couche MAC et son temps de départ supposé.

- **Consommation d'énergie par paquet :** la consommation d'énergie moyenne pour toutes les transmissions de paquets réussies obtenue en divisant la capacité totale de la batterie par le nombre de paquets transmis avec succès pendant toute la durée de vie du nœud.

Étant donné que la supertrame se caractérise par sa taille d'une part et par le rapport de durées active-inactive d'autre part, nous avons considéré BO et $BO-SO$ comme paramètres

TABLEAU 3.1: Paramètres de simulation

Paramètre	**Valeur**
Taille de paquet de nœud	121 B (taille maximale autorisée)
Capacité résiduelle d'énergie évaluation (nœuds ordinaires)	capacité = 25 mAh
Limite de temps de simulation	100 h (pour chaque simulation)
Bande radio de transmission	2,4 GHz (250 kbps débit de données)

variables lors de l'évaluation. On a utilisé ces deux paramètres pour évaluer l'effet de la structure de la supertrame sur les résultats.

Nous supposons que les nœuds établissent le temporisateur de transmission périodique immédiatement après avoir reçu un slot du coordinateur. L'affectation de slot se produit dès la réception de la deuxième beacon après qu'une demande d'association est envoyée d'un nœud au coordinateur.

Puisque seulement $P_i mod_{réel} BI$ affecte la position d'arrivée de paquet dans la supertrame, on a choisi P_i où $P_i div_{réel} BI = 1$. Cela garantit que P_i tourne suffisamment de fois pendant la simulation, ce qui rend les résultats plus cohérents.

Pour chaque paire (SO, BO), nous prenons toutes les valeurs possibles que $P_i mod_{réel} BI$ peut prendre tout en considérant les secondes comme unité de temps et $P_i div_{réel} BI = 1$. Par exemple, pour la paire $(7, 8)$, la durée de l'intervalle beacon (BI) est $3,93216\,s$. Par conséquent, toutes les valeurs possibles que P_i peut prendre sont 4, 5, 6 et $7\,s$.

3.5.2 Analyse des résultats

Dans les simulations, l'attaquant est l'un des nœuds associés et il effectue l'attaque en envoyant un paquet dans la tête du slot de la victime dans chaque supertrame.

Brouillage en tête de slot

Pour évaluer les dommages que SHJA peut infliger au réseau, nous avons effectué une longue séquence de simulations de 100 heures, dans lesquelles nous avons considéré toutes les valeurs possibles de (SO, BO). Pour chaque instance de paire, on a couvert l'ensemble des valeurs que $P_i mod_{réel} BI$ peut prendre en considérant les secondes comme l'unité de temps. Les résultats sont ensuite moyennés sur chaque série de valeurs.

La figure 3.4 montre l'effet de la structure de la supertrame sur la moyenne de taux de livraison de paquets en présence de SHJA.

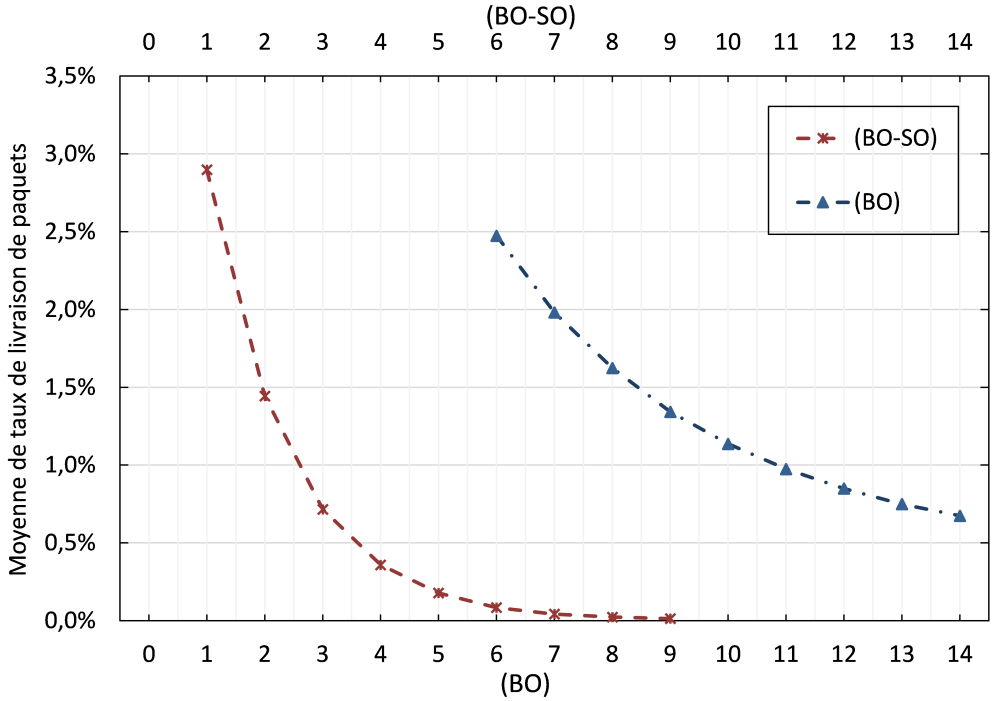


FIGURE 3.4: Brouillage en tête de slot vs brouillage complet du slot

Puisque nous avons considéré les secondes comme une unité de temps, nous avons dû éliminer toutes les paires (SO, BO) qui aboutissaient à une période P inférieure à $1\,s$. Par conséquent, la valeur de BO devrait être au moins 6.

Pour montrer l'efficacité de SHJA, on a dû prendre la plus petite fraction $\frac{durée\_brouillage}{durée\_slot}$ tout en prenant autant de valeurs SO que possible. Cependant, puisque la taille des en-têtes MAC et PHY est fixe, nous avons dû ignorer les courtes durées de slots qui ne conservent pas cette fraction. La plus petite fraction conservable qui donne le plus grand nombre de valeurs SO est $\frac{1}{30}$. Par conséquent, SO ne peut pas être inférieur à 5.

Il est important de mentionner que l'implémentation IEEE 802.15.4 n'est pas testée dans le cas où $SO = BO$, nous n'avons donc pas considéré ce cas dans les simulations.

À partir de la figure 3.4, on peut voir que SHJA a atteint au moins 97% de corruption en n'effectuant que 3,33% de brouillage complet de slot. Par conséquent, il y avait une différence significative en terme d'efficacité par rapport au brouillage classique. Cette efficacité est donnée par le fait que la majeure partie du trafic a été livrée dans la tête de slot cible.

En général, on remarque que la moyenne du taux de livraison des paquets diminue à mesure que BO et $BO - SO$ augmentent dans les deux courbes. Ceci est évident dans le cas

de $BO - SO$ puisqu'il y a une relation inverse entre $BO - SO$ et $\frac{durée\_slot}{BI}$. En fait, lorsque $BO - SO$ augmente ($\frac{durée\_slot}{BI}$ diminue), la probabilité d'arrivée au-delà des slots augmente.

Dans le cas des variations BO, la diminution du PDR est due à l'effet de l'établissement de la moyenne sur l'ensemble de toutes les valeurs SO correspondant à chaque valeur BO. Par exemple, lorsque $BO = 14$, il y a neuf valeurs SO avec lesquelles on fait la moyenne. En revanche, il n'y a que deux valeurs dans le cas où $BO = 7$.

La figure 3.5 représente les performances de SHJA optimisée résumée dans l'algorithme 3 en comparaison avec la SHJA continue. Les résultats ont été moyennés sur l'ensemble de la paire instance $(7, 8)$.

D'après la figure, nous remarquons que lorsque $P_i div_{réel} BI$ augmente, le taux de corruption de paquets de SHJA optimisée se rapproche de celui de l'attaque continue alors que le taux de paquets de brouillage diminue. Il s'avère que l'exploitation d'une propriété mathématique simple a économisé la moitié des ressources de l'attaquant. Il suffit de voir la figure pour réaliser que les taux de paquets de brouillage et de corruption convergent vers 100% et 50%, respectivement.

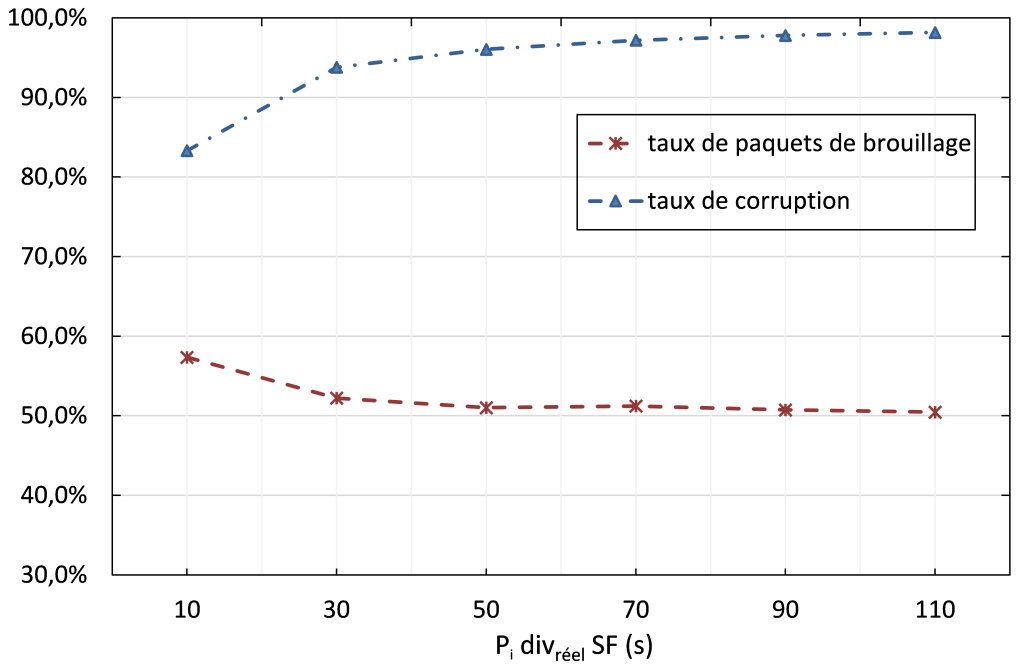


FIGURE 3.5: Brouillage optimisé vs brouillage continu

Au fur et à mesure que $P_i div_{réel} BI$ augmente, le rapport $\frac{nombre\_paquets\_écoute}{nombre\_paquets\_brouillage}$ et l'interférence entre les phases d'écoute/brouillage diminuent. Cela augmenterait le taux de

corruption de paquets d'une part et diminuerait le nombre de paquets de brouillage d'autre part.

Départ aléatoire de paquet

Pour évaluer les performances de notre solution dans différentes configurations de réseau, nous avons évalué le taux de livraison de paquets en présence et en absence de RPD.

On a utilisé une distribution uniforme pour générer les délais aléatoires ajoutés par RPD et on a changé la graine du générateur de manière par paire pour que RPD se comporte différemment à chaque fois.

D'après la figure 3.6, on voit que RPD a considérablement amélioré le débit du réseau. En fait, en moyenne, RPD a augmenté le PDR de 1% à 96%, faisant passer l'état de la liaison de paralysé à actif.

La figure révèle que le taux de livraison des paquets était presque constant et proche de $\frac{durée\_slot - durée\_brouillage}{durée\_slot}$. Cela est dû au grand nombre d'arrivées de paquets au-delà des slots.

Nous avons choisi une distribution uniforme plutôt qu'une distribution à base de moyenne afin d'éviter la situation où l'attaquant concentre ces attaques sur la proximité de la moyenne.

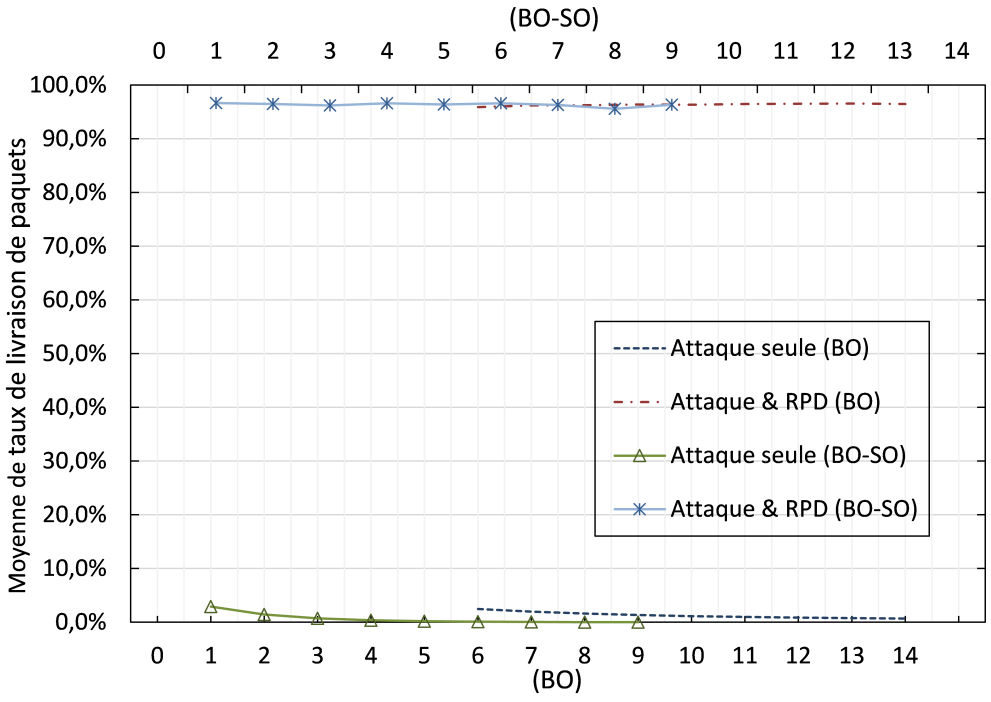


FIGURE 3.6: Évaluation de départ aléatoire de paquets (RPD)

Puisque notre protocole introduit une surcharge de délai supplémentaire, nous avons étudié les délais de livraison dans les deux cas : lorsque RPD est activé et lorsque seule la structure de la supertrame IEEE 802.15.4 est suivie.

Le mode GTS de l'IEEE 802.15.4 envoie les paquets différés par la supertrame au début du slot. Donc, tout paquet différé par la structure de la supertrame impliquera également un report RPD. Par conséquent, le délai RPD va inclure le délai résultant de l'effet de la structure de la supertrame. La figure 3.7 montre les changements de la moyenne du rapport $\frac{délai\_RPD}{délai\_supertrame}$ dans différentes configurations de supertrame.

Comme nous pouvons le voir, RPD a ajouté un délai négligeable au celui précédent qui est relativement plus important. En fait, il a fallu considérer le rapport pour éviter le chevauchement des courbes causé par la convergence des résultats.

Les mêmes facteurs influençant le taux de livraison des paquets dans l'évaluation de SHJA affectent le rapport de délais lorsque BO et $BO - SO$ augmentent. En général, nous pensons que cette surcharge de délai est raisonnable, en particulier lorsque P prend de grandes valeurs par rapport à la durée de l'intervalle beacon.

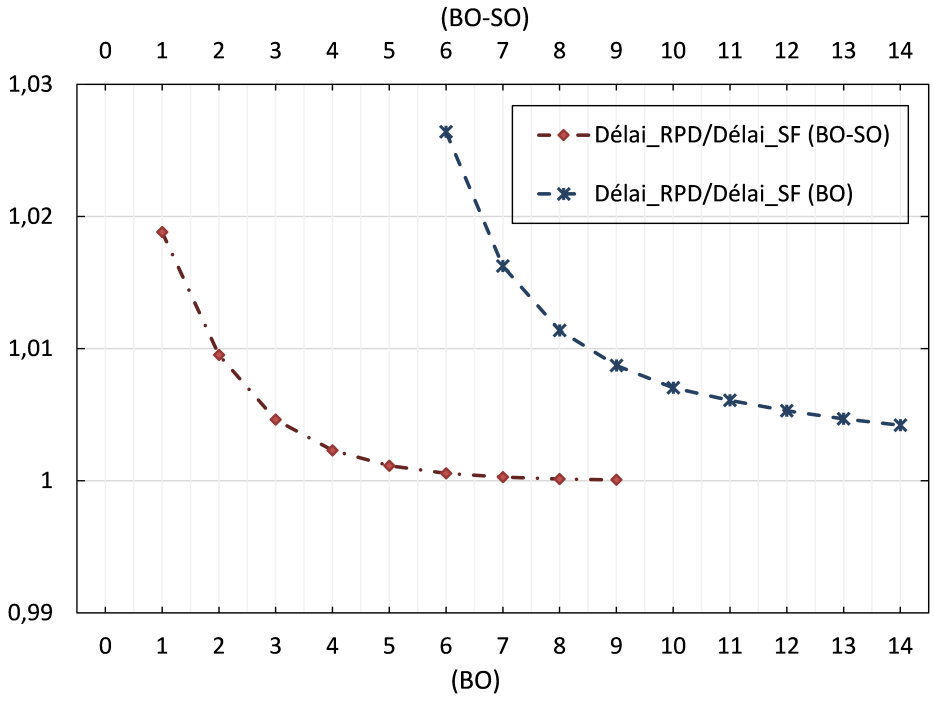


FIGURE 3.7: Évaluation de délai RPD

La variation de la consommation d'énergie par paquet en fonction de la durée de brouillage pour l'instance de paire $(7, 8)$ est représentée sur la figure 3.8. On a considéré trois cas : pas d'attaque, présence d'une attaque et scénario RPD (la courbe «attaque seule» est présentée

sur l'axe gauche et les deux autres courbes sur l'axe droit). Cette fois, nous avons poursuivi la simulation jusqu'à l'épuisement de la batterie de la victime.

En considérant la consommation d'énergie dans le cas de «sans attaque» comme métrique d'évaluation, en moyenne, un paquet dans le scénario RPD correspond à 4,3 paquets de «sans attaque». En revanche, le paquet dans le cas «attaque seule» correspond à 137,7 paquets. Par conséquent, la différence entre le cas «sans attaque» et le scénario RPD était négligeable par rapport aux valeurs élevées observées dans le cas «attaque seule».

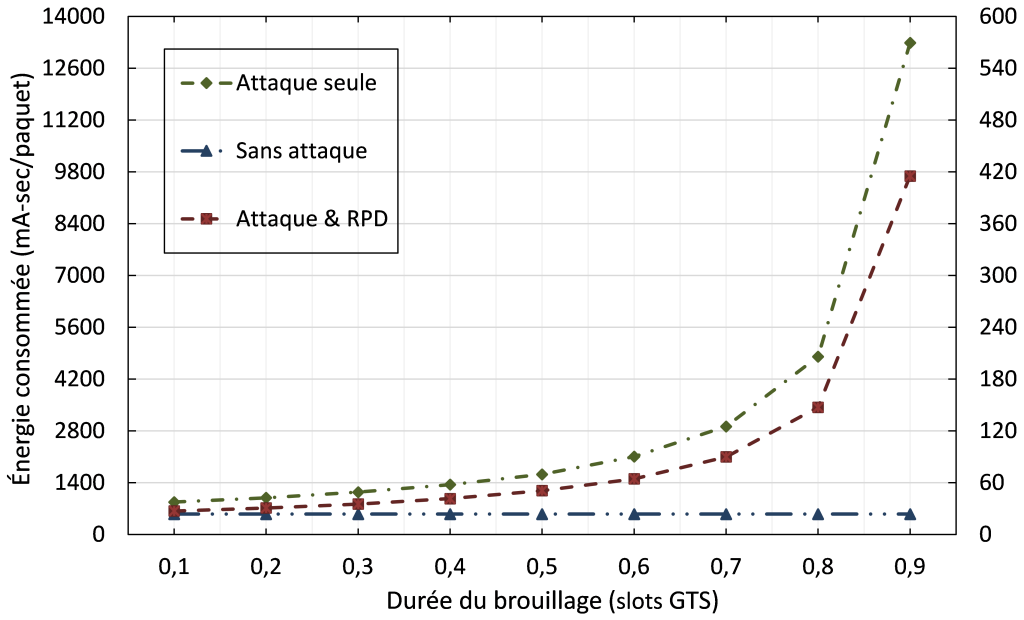


FIGURE 3.8: Évaluation de consommation d'énergie

Afin de montrer clairement les dommages résultant de SHJA et le débit du réseau que RPD peut récupérer, nous avons comparé notre travail avec l'allocation aléatoire de slots, proposée dans [9] et adoptée par [10] et [11]. Les auteurs ont affirmé que l'attaquant s'appuie probablement sur de simples nœuds de capteurs et vise à économiser l'énergie en n'attaquant qu'un seul slot de nœud.

En supposant les mêmes limitations sur l'attaquant, nous avons effectué un brouillage en tête de slot et brouillé tous les slots GTS, chacun avec un septième de la durée totale du brouillage ($\frac{1}{7}$ durée du slot GTS). La figure 3.9 montre la moyenne du taux de livraison de paquets dans RPD et l'allocation GTS aléatoire (RGTS : random GTS allocation) pour un nœud du réseau. Le PDR est moyenné sur l'ensemble de périodes de l'instance de paire $(7, 8)$.

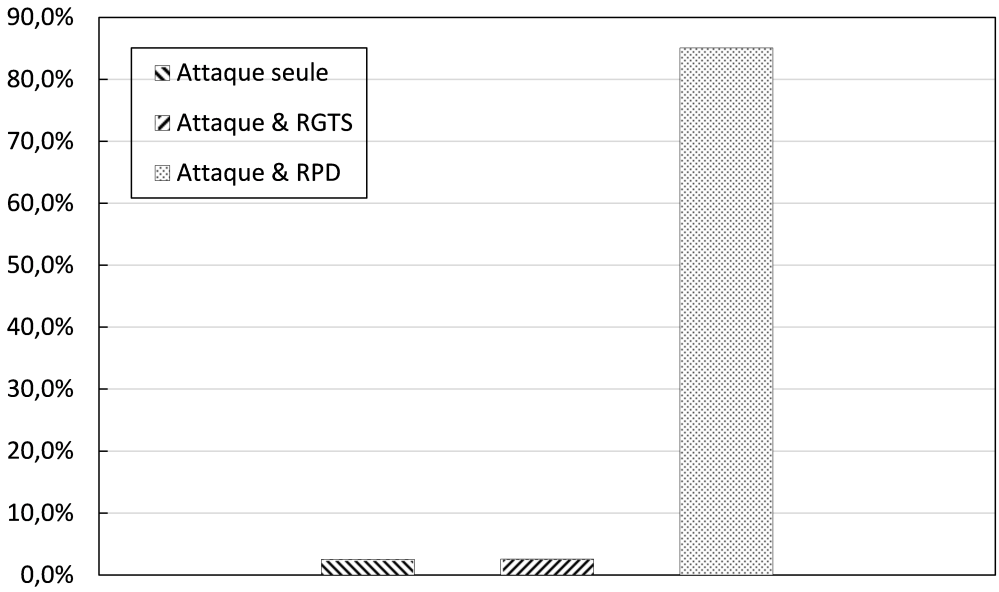


FIGURE 3.9: Taux de livraison de paquets de RPD et RTGS

À partir de la figure 3.9, on note que l'attaque a causé des dommages importants à l'ensemble du trafic même si celle-ci a dépensé les mêmes ressources que la Sniper Attack classique. Cependant, dans ce cas, l'allocation GTS aléatoire était inutile. Puisque tous les slots seront brouillés par $\frac{1}{7}$ durée de slot, changer l'ordre des slots ne sert pas à éviter l'attaque.

La raison sous-jacente de cette simulation, même si l'allocation GTS aléatoire n'était pas conçue pour contrer de telles attaques, est de montrer qu'il existe un moyen pour l'attaquant de poursuivre l'attaque et d'éviter RGTS, tout en évitant de consommer de ressources supplémentaires.

Il convient de noter que SHJA n'a pas seulement fait en sorte que le GTS aléatoire n'exerce aucun effet, il a également paralysé l'ensemble du trafic réseau, contrairement aux Sniper Attack qui ne visent qu'un seul nœud.

D'après les simulations effectuées dans ce travail, on peut voir que les principaux facteurs affectant le modèle de communication de l'IEEE 802.15.4 dans le cas d'un trafic périodique sont la structure de la supertrame et la politique de transmission de la norme.

Après avoir considéré presque toutes les configurations réseau ainsi que toutes les valeurs discrètes possibles de la période inter-départs, nous pouvons voir qu'une grande partie du trafic est livrée dans la tête de slot du nœud. C'est ce qui a rendu SHJA aussi destructeur pour les informations communiquées.

En effectuant seulement 3,33% de brouillage complet de slot, SHJA a atteint de 99% à 97% de corruption, conformément à la configuration du réseau. Par conséquent, l'effet de la supertrame sur les dommages SHJA est négligeable, ce qui nécessite, à notre avis, de reconsidérer certaines des fonctionnalités de la norme. La situation peut être pire si l'attaquant a tendance à limiter son attaque aux supertrames qui auront très probablement une communication courante.

Une solution possible pour SHJA est de randomiser le départ des paquets à l'intérieur du slot. Ce faisant, RPD pourrait réduire la corruption de SHJA à 4,3% conformément aux nos entrées de simulation.

De plus, les résultats montrent que la supertrame modifie le schéma horaire de la communication à tel point que le délai introduit par RPD était négligeable. Notablement, ce dernier présente au plus 3% du délai de la supertrame.

L'évaluation énergétique montre que la randomisation des départs de paquets améliore l'efficacité énergétique de la victime, ce qui se traduit par une durée de vie du réseau plus longue. En fait, RPD sauve les nœuds de l'épuisement de la batterie résultant des retransmissions de trames d'une part et assure une disponibilité maximale du réseau en sauvant la majeure partie du trafic ciblé d'autre part.

3.6 Conclusion

Dans ce chapitre, nous avons présenté une nouvelle version de l'attaque GTS avec une contre-mesure atténuante. L'application cible est le trafic périodique dans les réseaux corporels sans fil basés sur l'IEEE 802.15.4.

À partir des simulations réalisées, nous concluons que les attaques de brouillage sélectif peuvent être facilement effectuées sans dépenser beaucoup de ressources. Cette facilité est donnée par le fait que la structure de la supertrame modifie, de manière déterministe, le schéma de transmission du nœud habilitant.

SHJA peut faire tomber l'ensemble du réseau en ne dépensant que ce dont une attaque GTS classique a besoin pour cibler un seul nœud du réseau.

RPD peut réduire les dommages causés par SHJA à $\frac{durée\_brouillage}{durée\_slot}$ sans introduire de gros délais.

Dans futures travaux, nous avons l'intention d'améliorer SHJA pour qu'il soit plus économique en adoptant des algorithmes plus sophistiqués pour traquer le schéma de communication cible. La prochaine étape de notre travail peut éventuellement être un système de

détection d'intrusion qui exploite l'altération déterministe en mode GTS pour détecter les anomalies dans le comportement de l'appareil.

Chapitre 4

Ajustement multiplicatif de saison

Le trafic périodique dans les réseaux IEEE 802.15.4 comme dans tout autre réseau a un modèle déterministe, et puisque la période de l'appareil est une durée finie, le modèle peut être, certainement, capturé et sa durée est appelée une saison.

Malgré ses multiples avantages, la structure de la supertrame IEEE 802.15.4 modifie fortement le trafic périodique en raison des slots dédiés fixes où les appareils gèrent exclusivement leur communication garantie. En effet, lorsqu'un paquet applicatif atteint la couche MAC d'un équipement où ce n'est pas l'heure de son slot, la transmission de la trame sera retardée jusqu'à son prochain slot dans la supertrame courante ou suivante. Ces retards rendent la fermeture du modèle plus difficile et donc la saison sera plus longue. Les changements de périodicité dépendent des périodes des dispositifs d'une part et de la structure temporelle de la supertrame d'autre part.

Étant donné que le comportement temporel du trafic agrégé n'est pas complètement prédit à moins que nous ne capturons son modèle, il est primordial d'extraire la saison qui intègre tous les scénarios possibles, que ce soit pour construire un modèle ou analyser les performances du système.

En fait, il est clair que la modélisation de toute métrique de réseau diffère dans le cas de la présence de saisonalité. Par exemple, pour modéliser un certain signal continu en tant que série temporelle, les modèles ARIMA saisonniers (SARIMA [52]) prennent comme entrée la taille de la saison, et l'utilisation d'ARIMA non saisonnier dans de tels cas donne des estimations biaisées.

Dans la littérature, on trouve trois directions principales adoptées dans la prévision agrégée du trafic : les approches statistiques [53] [54], l'apprentissage automatique [55][56] et les processus stochastiques [57] [58]. Les deux premières approches ne supposent aucune

hypothèse avant de construire le modèle. Cela les rend plus dépendantes de l'ensemble de données. Par conséquent, la capture de la saisonnalité constitue une étape primordiale dans ces approches. D'autre part, la dernière approche considère principalement un modèle prédéfini avec des paramètres connus préfixés où le processus de Poisson fait le modèle choisi le plus fréquemment. Cependant, pour évaluer authentiquement le modèle, la saison complète doit être considérée avant de tirer des conclusions définitives à son sujet. De plus, des études empiriques montrent que l'hypothèse du processus de Poisson ne tient pas lorsque le réseau est de taille petite ou modérée, ni pour le trafic périodique [57] ni pour le trafic événementiel [58].

Dans ce chapitre, nous visons à fournir une technique pratique qui aide à extraire la saisonnalité du trafic, qui peut ensuite être exploitée pour modéliser authentiquement le trafic. Cette technique vise essentiellement à réduire les tailles de saison irrationnelles qui caractérisent le trafic périodique de l'IEEE 802.15.4 tout en gardant la même configuration de réseau autant que possible.

4.1 La capture du signal

La première étape à effectuer dans la modélisation du schéma de communication, est la préparation d'un log qui enregistre l'historique des arrivées des paquets. Cet log ne doit nécessairement pas avoir un format spécifique pour jouer le rôle attendu. Un simple tableaux contenant le nombre d'arrivée de paquets associé d'une estampille temporelle est suffisant. Le point de log le plus raisonnable c'est le coordinateur puisqu'il présente un point de passage impératif pour le trafic d'une part et il a plus de capacité mémoire et énergétique d'autre part.

Après avoir préparé le log nous devons être capables d'en extraire le signal du trafic. La figure 4.1 présente un exemple de signal.

Les observations (nombre d'arrivées) sont enregistrées dans des intervalles de tailles égales. Le choix de la taille de ces intervalles affecte directement la taille d'espace mémoire nécessaire pour sauvegarder le signal complet. De ce fait, ce n'est pas nécessaire de gaspiller l'espace mémoire en conservant une estampille de chaque observation du signal. Il faut juste adopter un certain pas et construire le log en enregistrant seulement les observations dans des intervalles de taille égale au pas choisi. Cependant, nous, absolument, déconseillons de choisir un pas de taille supérieure à BI pour ne pas perdre des détails importants comme les retransmissions qui portent une information sur la qualité du lien de communication.

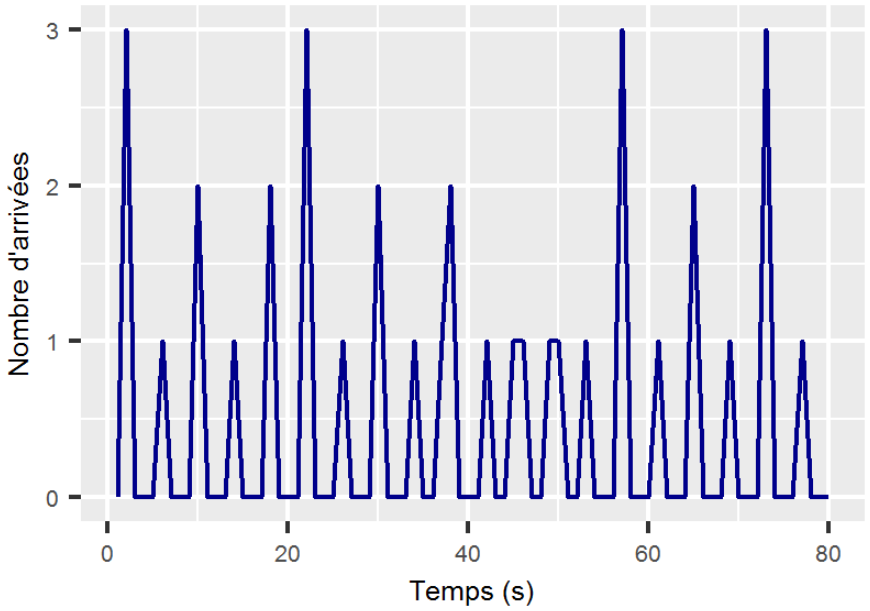


FIGURE 4.1: Une extraction du signal du trafic pour trois noeuds (périodes : $5\,s$, $7\,s$, $9\,s$)

Dans la figure, on note quatre observations typiques (détails) dans le signal. C'est raisonnable car le nombre de nœuds est trois dans cet scénario, donc, on peut avoir 1, 2, 3 ou rien comme nombre d'arrivées. De manière générale, il y a $N+1$ observations typiques pour N nœuds communiquant [1].

4.2 Énoncé du problème et motivation

Pour modéliser le schéma de communication il faut avoir suffisamment d'observations afin de terminer les deux phases de modélisation ; formation et test du modèle. Par conséquent, il nous faut au moins trois saisons ; deux pour la phase de formation (on a besoin de deux saisons pour faire la différence saisonnière), et une saison pour la phase de test (afin de tester toutes les possibilités qui peuvent arriver dans une saison).

Considérons un réseau avec N nœuds et soit P_i la période entre les arrivées de paquets du nœud i $(1 \leq i \leq N)$.

Soit S la saison qui capture tous les changements dans le schéma d'arrivée des paquets. S couvre tous les décalages possibles entre les répétitions périodiques des facteurs horaires en interaction, y compris la supertrame.

1. Cela reste vrai en excluant l'effet de la supertrame. Dans le cas contraire, on peut parfois avoir plus que $N+1$ observations typiques produites par les reports inter-pas des paquets.

En conditions naturelles et sans adopter de structure de supertrame, la saison n'est autre que le plus petit commun multiple (PPCM) de l'ensemble de périodes des nœuds :

$$S = PPCM(P_i, 1 \leq i \leq N)$$

Cependant, on sait que la structure de la supertrame modifie le schéma d'arrivée des paquets et déforme son ordonnancement. Par conséquent, nous devons considérer la durée de la supertrame pour extraire la saison.

Puisque BI est flottant, l'entier minimum qui est un multiple de BI est ce qui chevauche réellement avec les périodes des appareils. On note cet entier par BI_{nat}. Par conséquent, BI_{nat} est l'entier minimum où $BI_{nat} mod_{réel} BI = 0$.

Pour la bande de fréquence $2,4$ GHz et le débit $62,5$ ksymbole/s, BI en secondes peut s'écrire :

$$\begin{aligned} BI &= 0.01536 \times 2^{BO} \\ &= 3 \times 2^9 \times 10^{-5} \times 2^{BO} \\ &= 3 \times 2^9 \times 2^{-5} \times 5^{-5} \times 2^{BO} \\ &= 3 \times 2^{BO+4} \times 5^{-5} \end{aligned}$$

Puisque les nombres 2, 3 et 5 sont premiers entre eux, le nombre minimum que nous pouvons multiplier par BI pour en faire un entier est 5^5.

Ainsi, nous obtenons :

$$BI_{nat} = 3 \times 2^{BO+4}$$

$$BI = BI_{nat} \times 5^{-5}$$

Donc, on peut écrire S, la saison, comme suit :

$$S = PPCM(3 \times 2^{BO+4}, PPCM(P_i, 1 \leq i \leq N)) \tag{4.1}$$

L'équation (4.1) est la formule générale de la saison naturelle qui doit être prise en compte lors de la modélisation ou de l'analyse du trafic.

Prenons l'exemple figuré dans 4.1. Cet exemple prend la configuration de 3 nœuds avec 5, 7 et 9 s comme temps inter-départs et $BO = 8$. La taille de la saison pour cet exemple est 1290240 s, ce qui compte en heures $358,4\,h$. Pour le modélisation on a besoin de 3 saisons, donc, les deux phases vont prendre $1075,2\,h$ ($\approx 1,5$ mois). Cette durée est immense et malgré la configuration simple choisie et avec seulement trois nœuds c'est encore n'est pas pratique.

Une solution possible c'est de faire la modélisation par simulation, et après avoir obtenir le modèle, on l'intègre dans les nœuds réels. Cette solution semble être appropriée, surtout avec la rapidité des simulateur réseaux qui ignorent les périodes qui n'est témoin d'aucune évènement. À titre d'exemple, OMNeT++ en mode express prend environ $5\,min$ en simulant les premières 100 heures de la configuration précédente, donnant une efficacité temporelle de $\frac{1}{1200}$.

Cependant, lors de l'utilisation des simulateurs de réseau, nous pourrions être confrontés à des problèmes d'échelle de précision du temps en raison des saisons énormes. Dans OMNeT++ par exemple, le type $simtime\_t$ supportant les valeurs temporelles ne peut prendre que les valeurs dans la gamme $\pm 9,22 \times 10^{18-e}$, où e présente l'échelle de précision qui prend les valeurs entre 0 et 18. En considérons l'échelle de précision par défaut (12), nous pouvions à peine simuler trois saisons de la configuration précédente (c'est pour ça qu'on n'a pris que les 100 premières heures et pas la saison complète pour estimer l'efficacité temporelle). Il nous coûterait plusieurs ordres de précision de plus pour simuler des configuration réalistes, ce qui va probablement manquer les petits temps de propagation qui caractérisent les réseaux de nœuds contigus comme les WBANs.

En cas du choix de petites échelles de précision, il ne faut, surtout, pas prendre une échelle moins que la précision de la supertrame ($= 5$) pour ne pas perdre les détails de celle-ci.

Même si nous parvenons à ignorer les minuscules temps de propagation des paquets et à fixer $simtime\_t$ sur la précision de la supertrame, le temps de simulation pourrait prendre des jours dans le cas d'une configuration réaliste avec de nombreux nœuds. De plus, dans ce cas, la simulation peut effectivement capturer la saisonnalité mais elle ne peut pas considérer les facteurs contextuels, qui dépendent fortement de l'environnement cible. Dans le scénario d'évaluation de performance, on ne peut pas compter seulement sur les simulations. Selon l'objectif ciblé, un montage concret peut être obligatoire.

Une solution de contournement c'est d'enregistrer l'état du trafic quand le temps de simulation approche de la taille de type $simtime\_t$ et reprendre la simulation de nouveau en adoptant des décalages périodiques qui conviennent l'état enregistré. Cette solution peut être très gênante si on doit le reprendre à plusieurs reprises en cas d'immenses saisons.

En outre, dans de nombreux cas, nous devons répéter l'évaluation plusieurs fois afin de renforcer sa crédibilité. Travailler avec une longue saison peut parfois être possible ; cependant, répéter la procédure peut ne pas être confortable. Il est toujours avantageux d'avoir plus de flexibilité même dans les scénarios réguliers.

La meilleure solution qui est, dans beaucoup de cas, toute seule satisfaisante ou moins gênante si combiner avec l'enregistrement d'état dans les cas extrêmes, c'est ce que nous l'avons appelée **l'ajustement multiplicatif de saison**.

4.3 Ajustement multiplicatif de saison

L'ajustement multiplicatif exploite la partie exponentielle de la supertrame pour créer des points communs partiels entre les périodes et la supertrame.

Dans cette approche on change légèrement les périodes des nœuds en les transformant de nombres entiers (secondes : l'unité naturelle saisie manuellement) aux nombres réels pour des raisons de simplification.

Prenons la convention suivante :

$$2^{10\alpha} = 10^{3\alpha}$$

Où α est un entier positif strictement supérieur à 1 ($\alpha \geq 2$).

Avec cette convention on peut écrire :

$$P_i = \frac{2^{10\alpha}}{10^{3\alpha}} \times P_i$$

α est dit l'ordre d'ajustement multiplicatif. Nous appelons l'ajustement d'ordre 2 le méga-ajustement, l'ajustement d'ordre 3 le giga-ajustement, l'ajustement d'ordre 4 le téra-ajustement, etc.

Nous effectuons l'ajustement multiplicatif d'ordre α en changeant la valeur de toute période P_i par $\frac{2^{10\alpha}}{10^{3\alpha}} \times P_i$. En faisant ceci, on donne au P_i la chance d'avoir plus de diviseurs communs avec la durée de supertrame BI.

La fraction $\frac{S_{ajt}}{S}$ représente l'efficacité de l'ajustement, où S et S_{ajt} sont les durées de la saison avant et après avoir effectué l'ajustement, respectivement. Trouvons S et S_{ajt}.

En excluant l'effet de supertrame, la durée minimale qui capture toutes les inter-arrivées entre les périodes est $PPCM(P_i, 1 \leq i \leq N)$.

Écrivons le $PPCM$ sous la forme :

$$PPCM(P_i, 1 \leq i \leq N) = 2^n \times 3^k \times 5^m \times P^*$$

Où P^* est le produit des facteurs premiers constituant le $PPCM$ autres que 2, 3 et 5 [2]. n, m et k sont des nombres entiers.

2. Le choix de ces facteurs premiers est intentionné comme nous pouvons le voir ci-après.

Puisque S, la saison, est la durée qui capte toutes les variations d'arrivées en tenant compte de la supertrame, S peut s'écrire :

$$\begin{aligned} S &= PPCM(BI_{nat}, PPCM(P_i, 1 \leq i \leq N)) \\ &= PPCM(3 \times 2^{BO+4}, 2^n \times 3^k \times 5^m \times P^*) \end{aligned}$$

Ainsi :

$$S = 2^{n \vee BO+4} \times 3^{k \vee 1} \times 5^m \times P^* \tag{4.2}$$

Où $a \vee b = max(a, b)$.

On aura besoin fréquemment du notation maximum dans l'annexe, c'est pour cette raison qu'on va adopter la notation $\vee$ de la théorie de Lattice [59].

En supposant que $2^{10\alpha} = 10^{3\alpha}$ on peut reformuler le $PPCM$ des périodes P_i comme suivant :

$$PPCM(P_i, 1 \leq i \leq N) = 2^n \times 3^k \times 5^m \times P^* \times \frac{2^{10\alpha}}{10^{3\alpha}}$$

D'où :

$$PPCM(P_i, 1 \leq i \leq N) = 2^{n+10\alpha} \times 3^k \times 5^m \times P^* \times 10^{-3\alpha}$$

En d'autre part :

$$\begin{aligned} BI &= 0,01536 \times 2^{BO} = 3 \times 2^{BO+9} \times 10^{-5} \\ &= 3 \times 2^{BO+9} \times 10^{-5} \times 10^{3\alpha} \times 10^{-3\alpha} \\ &= 3 \times 2^{BO+9} \times 10^{3\alpha-5} \times 10^{-3\alpha} \\ &= 3 \times 2^{BO+9} \times 2^{3\alpha-5} \times 5^{3\alpha-5} \times 10^{-3\alpha} \\ &= 3 \times 2^{BO+4+3\alpha} \times 5^{3\alpha-5} \times 10^{-3\alpha} \end{aligned}$$

Pour que la partie $3 \times 2^{BO+4+3\alpha} \times 5^{3\alpha-5}$ soit naturelle, α devrait être supérieur strictement à 1 ($\alpha \geq 2$).

Par conséquent, la saison ajustée S_{ajt} s'écrit comme :

$$S_{ajt} = PPCM(3 \times 2^{BO+4+3\alpha} \times 5^{3\alpha-5}, 2^{n+10\alpha} \times 3^k \times 5^m \times P^*) \times 10^{-3\alpha}$$

Donc,

$$S_{ajt} = 2^{(n+10\alpha) \vee (BO+4+3\alpha)} \times 3^{k \vee 1} \times 5^{m \vee (3\alpha-5)} \times P^* \times 10^{-3\alpha} \tag{4.3}$$

En divisant (4.3) sur (4.2) nous obtenons l'efficacité d'ajustement saisonnier :

$$\frac{S_{ajt}}{S} = \frac{2^{(n+10\alpha) \vee (BO+4+3\alpha)} \times 5^{m \vee (3\alpha-5)}}{2^{n \vee (BO+4)} \times 5^m} \times 10^{-3\alpha} \tag{4.4}$$

L'ajustement multiplicatif ne peut être efficace que dans le cas ($n < BO+4$). Cela signifie que la formule (4.4) soit de valeur moins que l'unité (voir l'annexe B). Cette dernière sera donc de la forme :

$$\frac{S_{ajt}}{S} = \frac{2^{(n+10\alpha)\vee(BO+4+3\alpha)} \times 5^{m\vee(3\alpha-5)}}{2^{BO+4} \times 5^{m}} \times 10^{-3\alpha} \tag{4.5}$$

Soit α et $\acute{\alpha}$ deux ordres d'ajustement et S_{ajt} et $S^{'}_{ajt}$ les deux saisons ajustées par α et $\acute{\alpha}$, respectivement.

Voici quelques propriétés de l'efficacité de l'ajustement multiplicatif (annexe C) :

Propriété 4.1. *$\forall\alpha$, $\acute{\alpha}$ deux ordres d'ajustement :*

$$3 \leq \alpha < \acute{\alpha} \implies \frac{S_{ajt}}{S^{'}_{ajt}} \leq 1$$

Propriété 4.2. *Si $n \geq BO - 10$, alors, $\forall\alpha$, $\acute{\alpha}$:*

$$2 \leq \alpha < \acute{\alpha} \implies \frac{S_{ajt}}{S^{'}_{ajt}} \leq 1$$

Propriété 4.3. *Supposons que $n < BO - 10$ ($BO > 10$), $\alpha = 2$ et $\acute{\alpha} = 3$, alors :*

$$(m \leq 2)\ OU\ (m = 3\ ET\ n \geq BO - 12) \implies \frac{S_{ajt}}{S^{'}_{ajt}} \leq 1$$

$$(m \geq 4)\ OU\ (m = 3\ ET\ n < BO - 12) \implies \frac{S_{ajt}}{S^{'}_{ajt}} > 1$$

Les trois propriétés au dessus se résument dans les propositions suivantes :

- Le méga-ajustement et giga-ajustement sont les meilleurs ajustements dans tout l'espace des ajustements.
- Lorsque $BO \leq 10$ ou $n \geq 4$, le méga-ajustement surpasse tous les ajustements.
- Lorsque $BO > 10$, le choix entre le méga-ajustement et giga-ajustement dépend de la configuration (n, m, BO).

Ces trois propriétés concernent la comparaison entre les ajustements et ne considèrent pas l'efficacité de ceux-ci. De ce fait, un ajustement surpassé par un autre ne signifie pas que le premier ne soit pas efficace.

De manière générale, en cas de deux efficacités acceptés, celle de l'ordre le plus petit donne plus de flexibilité dans les choix de configurations et fournissent des efficacité acceptées avec des configurations raisonnables.

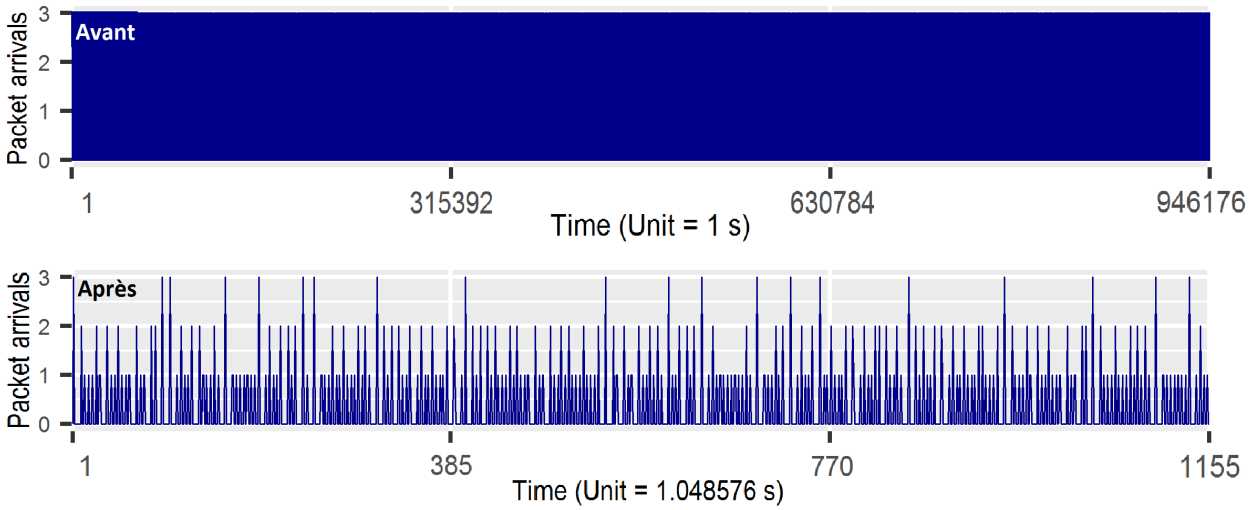


FIGURE 4.2: Un signal avant et après avoir appliqué l'ajustement multiplicatif.

Une solution pour améliorer la valeur de l'efficacité ou d'effectuer des ajustements d'ordres élevés tout en évitant les restrictions sur la configuration, c'est de modifier quelques facteurs 2 et 5 en d'autres facteurs comme 3 et 4 pour changer la valeur de n et m. Cependant, nous ne le recommandons pas, car cela va augmenter/réduire les valeurs des périodes concernées par 20% voire 33% ce qui déforme grandement le schéma de communication. De plus, l'ajustement multiplicatif est plus que suffisant sans avoir modifier les périodes, et nous ne voyons aucune intérêt de déformer le schéma juste pour de raisons qui sont probablement non fondées.

En augmentant les périodes seulement par $2,4\%$, l'ajustement multiplicatif donne des efficacités très impressionnantes allant jusqu'à $\frac{1}{15625}$ (pour le méga-ajustement sous le $62,5$ ksymbole/s).

La figure 4.2 montre un exemple de signal avant et après avoir appliqué l'ajustement multiplicatif. Dans la première sous-figure, on remarque que le signal prend une forme rectangulaire où presque toutes les observations enregistrent des arrivées 3. En fait, l'observation 3-arrivées a la fréquence la plus faible parmi toutes les fréquences des autres observations. La dominance de l'observation des arrivées à 3 est causée par le graphique empilé en raison de la taille énorme de la saison.

L'efficacité de l'ajustement multiplicatif pour l'exemple de la figure 4.1 est égale $\frac{4}{15625}$. Les trois saisons vont être réduites approximativement de $1,5$ mois à $990,90432\,s$ ($\approx$ 17 minutes). Les périodes seront donc $5,24288\,s$, $7,340032\,s$ et $9,437184\,s$.

FIGURE 4.3: Le signal après l'ajustement multiplicatif.

La figure 4.3 représente deux saisons du signal précédent après avoir appliqué l'ajustement multiplicatif (nous avons effectué la première différence saisonnière pour visualiser la saisonnalité dans la deuxième sous-figure).

Il faut, certainement, mentionner que l'ajustement multiplicatif affecte de la même manière l'espace mémoire nécessaire pour supporter le signal. De ce fait, en considérant que chaque observation prend 3 bits [3] de la mémoire, la configuration précédente coûterait approximativement $483.8\,Ko$ sans l'ajustement multiplicatif. Avec ce dernier les trois saisons peuvent être conservées par seulement $123,9$ octets.

Nous notons que, comme on peut le voir sur la figure 4.2, l'ajustement saisonnier change implicitement l'unité de temps naturelle (secondes). Pour l'ajustement de l'ordre α, l'unité est changée de $1\,(s)$ à $\frac{2^{10\alpha}}{10^{3\alpha}}\,(s)$.

4.4 Évaluation de performance

Pour étudier l'ajustement saisonnier, nous avons effectué l'évaluation en prenant des limites raisonnables car ni la période d'un appareil ni la taille du réseau n'ont de limite théorique.

3. Le maximum nombre de nœuds supporté par le mode GTS, à la fois et dans un réseau personnel élémentaire, est 7, donc pour une échantillonnage du signal par $3\,s$, il y a 8 observations possibles, qui peuvent être codées par 3 bits.

Nous avons pris un réseau IEEE 802.15.4 élémentaire avec une CFP entièrement réservée, et comme il est improbable que la période d'un appareil dépasse une journée, nous adoptons 24 heures comme limite supérieure pour toutes les périodes.

Pour chaque ordre de beacon BO, on considère toutes les combinaisons possibles des périodes P_i prenant les secondes comme unités de temps. Ainsi, nous couvrons tous les scénarios possibles et obtenons des ratios plus authentiques.

Nous avons analysé notre méthode quantitativement et qualitativement considérant les ajustements les plus efficaces, à savoir le Miga et Giga ajustements.

Dans l'évaluation quantitative, nous évaluons le rapport des ajustements effectifs dans toutes les configurations de réseau et périodiques possibles. Un ajustement pour une certaine configuration est dit efficace si la fraction $\frac{S_{adj}}{S}$ donne une valeur inférieure à 1, où S et S_{adj} sont la saison avant et après avoir effectué l'ajustement, respectivement. D'autre part, l'évaluation qualitative donne une description statistique de la portée des valeurs de l'efficacité.

Le tableau 4.1 résume les paramètres d'évaluation.

TABLEAU 4.1: Paramètres d'évaluation.

Paramètre	**Valeur**
Périodes des appareils	$\forall P_i,\ 1\,s \leq P_i \leq 86400\,s$
Ordre de beacon	$\forall BO,\ 1 \leq BO \leq 14$
Taille du réseau	7 (CFP entièrement réservée)

La figure 4.4 montre le taux des configuration réseaux efficaces et inefficaces de l'ajustement multiplicatif pour le débit de symboles $62,5$ ksymbole/s. Pour chaque configuration, nous avons choisi le meilleur rendement entre le Méga et Giga ajustement.

D'après la figure, nous notons que le Méga-ajustement a surpassé le Giga-ajustement pour presque toutes les configurations effectives. De plus, les configurations effectives font la majorité des cas. Cela garantit l'applicabilité de l'ajustement saisonnier.

La figure 4.5 représente une comparaison quantitative entre les ajustements Mega et Giga mais cette fois, et par souci de comparaison, nous avons pris chaque ajustement séparément et ne considérons pas le meilleur entre eux comme dans l'évaluation précédente.

Nous notons que plus l'ordre d'ajustement est faible, plus le taux de configurations efficaces est élevé. Cela pourrait probablement s'expliquer par la dominance des exposants contenant α dans la formule (4.5) lorsque ce dernier augmente.

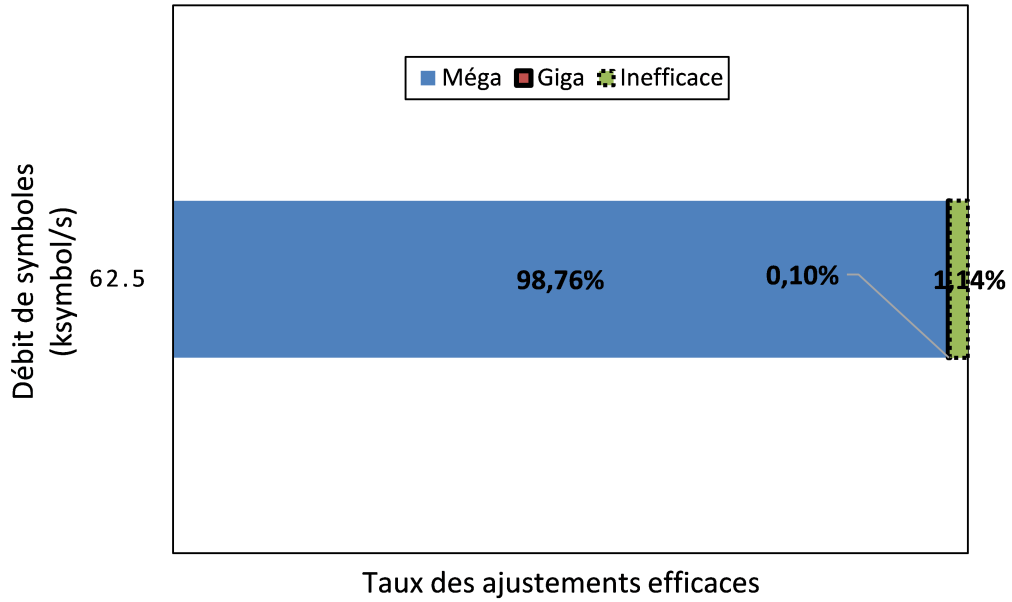


FIGURE 4.4: Taux des ajustements efficaces pour le Méga et Giga ajustements.

Dans la figure 4.6, nous montrons l'évaluation qualitative de l'ajustement saisonnier. Encore une fois, nous avons pris l'efficacité optimale à partir des ajustements possibles dans le débit de symboles $65,5$ ksymbole/s.

Généralement, l'ajustement saisonnier donne de bons résultats en termes d'efficacité. En fait, nous avons dû utiliser une échelle exponentielle pour étaler les barres. À l'échelle naturelle, les barres étaient empilées et condensées au bas de la figure.

Il convient de noter que le taux de l'altération de la périodicité de l'ajustement est indépendant de la configuration du réseau. Par conséquent, les taux d'altération sont constants quel que soit le débit de symboles ou la valeur de l'ordre de beacon. Le tableau 4.2 montre le taux de modification des périodes pour les ajustements Méga et Giga.

TABLEAU 4.2: Taux d'altération des périodes des appareils pour le Méga et Giga ajustements.

Configuration réseau	**Ordre d'ajustement**	**Taux d'altération des périodes**
$\forall\{P_i\}, \forall BO$	Méga-ajustement	4.86%
	Giga-ajustement	7.37%

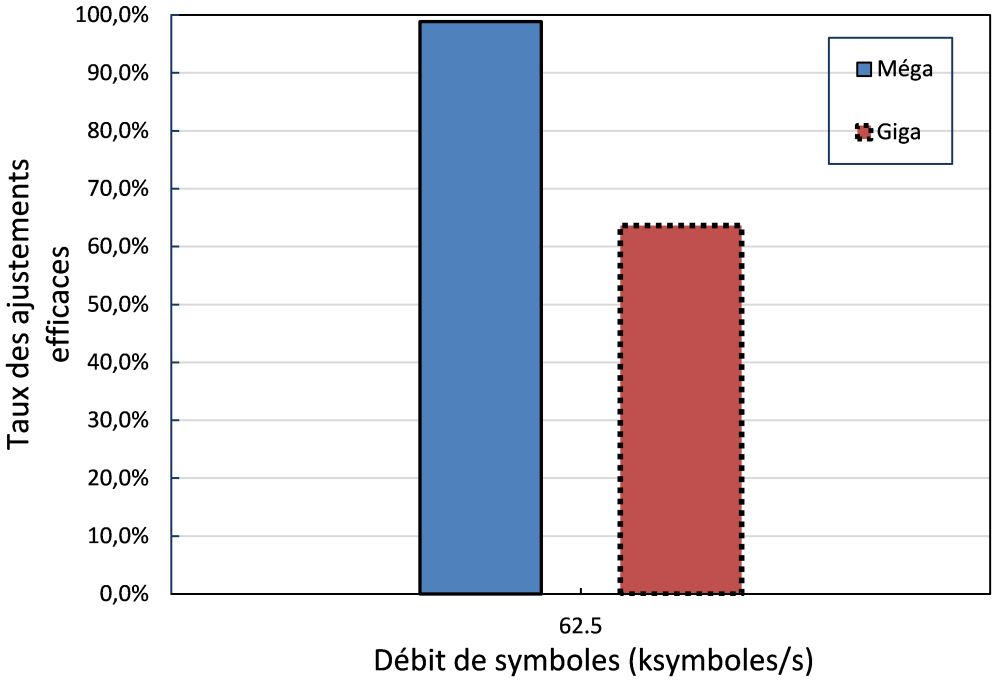


FIGURE 4.5: Taux des ajustements efficaces en considérant les meilleures efficacités

Par rapport aux avantages de l'application de l'ajustement, ces changements infimes sont très tolérables, d'autant plus que la majorité des ajustements les plus efficaces sont de l'ordre Méga.

4.5 Conclusion

La capture de la saisonnalité permet d'obtenir des analyses authentiques et constitue une étape primordiale dans la modélisation du réseau. Cependant, cette procédure peut être difficile dans le cas d'un trafic IEEE 802.15.4 périodique en raison des durées impaires de supertrame qui ne convient pas la périodicité naturelle. Par conséquent, la configuration du réseau doit subir une phase de prétraitement avant de commencer les procédures d'analyse ou de modélisation.

Pour résoudre ce problème, nous avons proposé l'ajustement multiplicatif saisonnier. L'objectif de ce dernier est de réduire la durée de saison tout en gardant la même configuration du réseau autant que possible. En fait, l'ajustement saisonnier a produit de bons rendements avec une modification minimale de la configuration du réseau selon nos évaluations quantitative et qualitative.

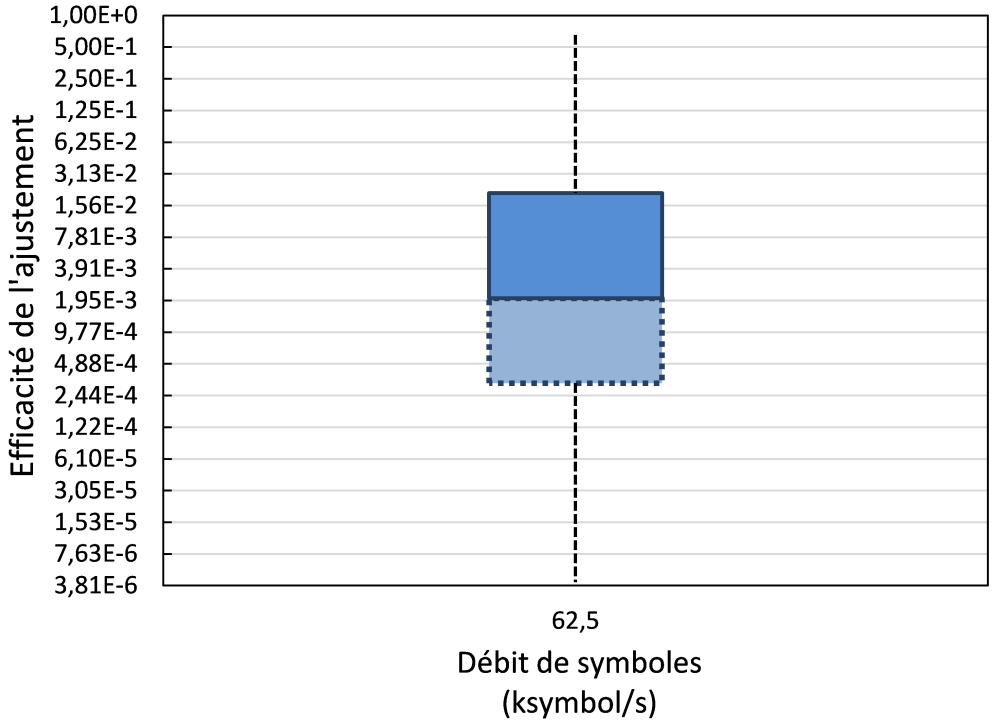


FIGURE 4.6: L'évaluation qualitative de l'ajustement saisonnier

Cette technique pourrait également être appliquée à d'autres débits de symboles qui ont la même forme exponentielle, mais avec des propriétés et des ordres d'ajustement différents.

Les travaux futurs consisteraient à la proposition d'autres approches d'ajustement qui exploitent la précision élevée de la supertrame pour fournir des ajustements plus efficaces. En fait, l'ajustement multiplicatif change l'unité de temps de manière implicite en faisant les périodes des appareils des valeurs semblables à la durée de la supertrame. On peut, par exemple, essayer de changer explicitement l'unité de temps pour inverser l'approche. En changeant l'unité de temps, on peut faire de la durée de la supertrame une valeur semblable au périodes des appareils. Donc, la supertrame va être implicitement de durée entière.

Ça serai intéressant de comparer l'approche d'ajustement saisonnier avec cette approche pour savoir quand l'une est meilleure que l'autre afin de définir un algorithme de prétraitement du signal capturé qui automatise la procédure de réduction de saison.

Il est intéressant aussi d'étudier l'effet du taux de symboles sur l'efficacité de l'ajustement et sur le taux de configurations efficaces. Cela peut déterminer la possibilité de considérer d'autres bandes de fréquence supportées par la norme. Cette étude peut faire partie de l'évaluation de l'applicabilité.

Chapitre 5

Détection des anomalies dans les réseaux corporels sans fil (WBANs)

La détection des anomalies est considérée parmi les méthodes les plus connues dans le domaine d'analyses des systèmes et détection d'intrusion, surtout avec l'exploitation répandue des technique d'apprentissage machine ces dernières années [60] [61]. Ces techniques servent à construire un modèle qui décrit le système, et toute déviation de cette modèle est classée comme une anomalie. Cette approche risque d'avoir un taux élevé de faux positifs en raison de la difficulté d'avoir un bon modèle qui s'ajuste bien au système.

La détection des anomalies dans les systèmes de communication se fait de plusieurs manières. La plus efficace de celles-ci est l'analyse du trafic qui circule dans le réseau, en particulier, en cas de trafic périodique [62]. Ceci est vrai car le trafic ne présente pas seulement un indicateur de fonctionnement du réseau, c'est plutôt le fonctionnement lui-même. C'est le but initial et final du déploiement du réseau à la base [63].

Pour cette raison, on trouve des travaux adoptant cette approche pour déterminer les différentes activités qui divergent du comportement légitime [64]. Cependant, beaucoup d'entre eux n'ont pas abordé les notions de périodicité à tel point qu'ils bénéficient de son plein potentiel dans la détection des anomalies. C'est, probablement, à cause qu'ils traitent le trafic indépendamment de la technologie utilisée. De plus, les trafics étudiés, souvent, ne suivent aucune supertrame et certainement ils n'adoptent pas la norme IEEE 802.15.4.

Dans [12], les auteurs ont focalisé sur les anomalies dans le volume du trafic lors de la surveillance réseau. Ils se sont servis de l'analyse en composantes principales [65] pour détecter l'attaque de déni de service et de la périodicité dans le volume du trafic pour améliorer le taux de faux positifs.

D. Miao et al. [13], ont bénéficié du modèles saisonniers SARIMA (Seasonal AutoRegressive Integrated Moving Average [52]) pour modéliser le trafic périodique dans les réseaux sans fil. La modélisation était basée sur des traces réelles de trafic de données mesurées à partir du réseau 2G/3G de China Mobile. Les expériences montrent que leur modèle est un bon choix pour capturer les propriétés du trafic réel et pour la prédiction à court terme (ce qui convient bien la détection des anomalies). Cependant, ce type de trafic (2G/3G) se caractérise par son volume, relativement, immense et ses variations conviennent la modélisation ARIMA compte tenu de sa ressemblance avec le signal continu. Ce n'est pas le cas pour le signal des petits réseaux comme celui de WBANs où beaucoup de périodes passent sans avoir aucune évènement.

En se basant sur les périodes inter-départs de chaque type de requête, les auteurs de [14] ont introduit un algorithme pour détecter les attaques dans les réseaux SCADA (Supervisory Control and Data Acquisition [66]). L'algorithme analyse l'écart type des périodes inter-départs d'un type de requête contre un seuil prédéfini pour signaler un comportement apériodique. L'algorithme montre sa efficacité en termes de taux de faux positifs et de détection.

Pour les mêmes réseaux, R. R. R. Barbosa et al. [15] ont proposé de détecter les anomalies dans la périodicité du trafic par un spectrogramme qui sert à visualiser les changements dans les intervalles et les tailles des pics périodiques. Le spectrogramme est réalisé après avoir extrait la taille et la périodicité des pics périodiques dans la phase d'apprentissage.

Bien que cette méthode s'est avérée efficace dans la détection des altérations dans la périodicité, elle reste impraticable en raison du manque d'automatisation lors de la procédure de détection qui demande une extra tâche d'interprétation.

En tout cas, les réseaux SCADA diffèrent beaucoup des réseaux personnels en termes de fonctionnement et de but de déploiement.

Après l'extraction de la saisonnalité, on peut construire un modèle pour le trafic afin de l'utiliser ensuite pour la détection des anomalies.

Dans les sections qui suivent, nous allons décrire, progressivement, notre approche de détection des anomalies dans les réseaux corporels sans fil basant sur la norme IEEE 802.15.4.

5.1 Détection d'anomalies

Après avoir ajusté la saison avec l'ajustement multiplicatif que nous avons introduit dans le chapitre précédent, la capture du celle-ci doit être réalisable. Donc, nous pouvons

FIGURE 5.1: Le signal ajusté avec un PER de 10^{-3}.

maintenant lancer la capture du signal en adoptant un pas approprié. Le signal résultant porte le schéma de communication légèrement déformé à cause des anomalies que nous allons les appeler anomalies naturelles. Ces anomalies sont l'incarnation du taux d'erreur dans le trafic. En fait, la figure 4.3 représente un signal capturé dans des conditions parfaites afin de visualiser la saisonnalité. Le même signal avec un taux d'erreur de paquet (PER : Packet Error Ratio) de 10^{-3} est présenté dans la figure 5.1.

Un signal normal porte à la fois le schéma de communication et les anomalies naturelles. Ces anomalies peuvent être visualisées en effectuant la différence saisonnière présentée dans la deuxième sous-figure de la figure 5.1.

Les perturbations dans la deuxième sous-figure correspondent, en fait, aux paquets erronés, ce qui se traduit en PER. Le taux d'erreur de bits (BER : Bit Error Ratio) et le PER représentent des indicateurs clés de performance réseau. Ce sont les probabilités qu'un bit ou un paquet soient erronés. Cette probabilité dépend de tous les composants du système de communication qui peuvent être affectés par divers facteurs comme le bruit du canal de transmission, atténuation, interférence, problèmes de synchronisation, etc [67].

Pour les réseaux corporels sans fil, l'effet de ces facteurs varie fréquemment à cause des changements environnementaux autour du corps humain. Ces changements varient d'une personne à l'autre. Par exemple, pour une personne située dans un hôpital ; le PER tend d'être stable durant tout le jour. Ce n'est, certainement, pas le cas pour une personne mobile qui entre et sort des portées d'autres systèmes de communications et qui s'expose aux diverses influences extérieures hors de chez lui.

Admettant que les facteurs quotidiens pour les différents scénarios d'exploit affectent le PER de manière qu'il suive une distribution presque normale de moyenne μ et variance σ^2.

Les valeurs de μ et σ^2, peu importe la distribution, peuvent être obtenues par une étude statistique sur terrain ou n'importe quel autre convenable méthode. Pour des résultats plus fiables, nous recommandons de diviser les personnes cibles par des classes qui partagent les mêmes caractéristiques environnementales, ex., mobiles, immobiles, âgées, jeunes, etc. Toutefois, la façon dont les deux paramètres sont obtenus excède le cadre du présent travail. Dans ce travail, nous allons considérer le PER (dans les conditions naturelles) comme l'ensemble des anomalies naturelles qui font partie du système de communication.

Définissons le seuil qui sert d'une borne supérieure pour le PER comme suivant :

$$SE_p = \mu + Z_p \times \sigma$$

Où p représente le pourcentage des PERs couverts en adoptant la borne SE_p. Z_p est le z-score correspondant au pourcentage p.

Notons que p doit être supérieur à 50% pour comprendre la moyenne et le queue gauche de la distribution afin de prendre en considération les petits PERs.

Nous avons choisi les z-scores au lieu de t-scores en supposant que la taille d'échantillon est suffisamment grande (une taille plus que 30 est une bonne règle de base [68]).

Basant sur la saisonnalité qui caractérise le trafic périodique dans le mode beacon de l'IEEE 802.15.4, et en adoptant nos suppositions sur la distribution du PER sous les différentes circonstances, nous proposons l'algorithme 6 pour détecter les anomalies "anormales".

Algorithme 6 Détection d'anomalies

1: **tant que** $Vrai$ **faire**
2: $T \leftarrow pas\_actuel$ ▷ premier pas : $\frac{S_{ajt}}{pas} + 1$
3: **si** $\frac{\sum_{t=T-w}^{T} |Y_t - Y_{t \bmod (\frac{S_{ajt}}{pas}+1)+1}|}{4 \times w \times pas \times \sum_{i=1}^{N} \frac{1}{P_i}} > SE_p$ **alors**
4: **Lancer_alerte()**
5: **fin si**
6: **fin tant que**

T représente l'ordre du pas actuel (ou tout simplement le temps en pas) et w représente la taille d'une fenêtre glissante.

Le principe général de l'algorithme est d'évaluer la différence entre les observations constituant la fenêtre glissante avec leurs observations correspondantes dans le modèle ;

la saison enregistrée dans le log (ou tout simplement, la première saison). Si cette différence dépasse la seuil SE_p, on considère qu'il existe une divergence anormale.

La partie gauche de l'inégalité à la ligne 3 de l'algorithme correspond, en fait, à une estimation locale du PER dans la fenêtre glissante qui va être comparée avec le PER réel (la partie droite). Le dénominateur estime le nombre totale des paquets reçus par le coordinateur. En fait, en faisant la première différence entre les fenêtres, on va capturer les erreurs faisant partie des deux fenêtres à la fois, de plus, les retransmissions vont être aussi incluses dans la différence (d'où la multiplication par 4).

Les seuls paramètres affectant l'algorithme 6 sont la taille w de la fenêtre et le seuil SE_p du PER (plutôt le pourcentage p). Plus p est proche de 100%, plus sera le nombre des PERs couverts, et donc plus de possibles anomalies anormales seront prises involontairement et vice versa ; plus p est proche de 50%, moins sera le nombres des PERs couverts, et donc moins de possibles anomalies anormales seront prises involontairement. D'une manière similaire, plus w est grande, plus sera la précision du PER estimé dans la fenêtre, cependant, plus sera l'espace mémoire nécessaire pour sauvegarder les observations faisant partie de la fenêtre et vice versa.

La figure 5.2 résume le principe de fonctionnement de l'algorithme 6.

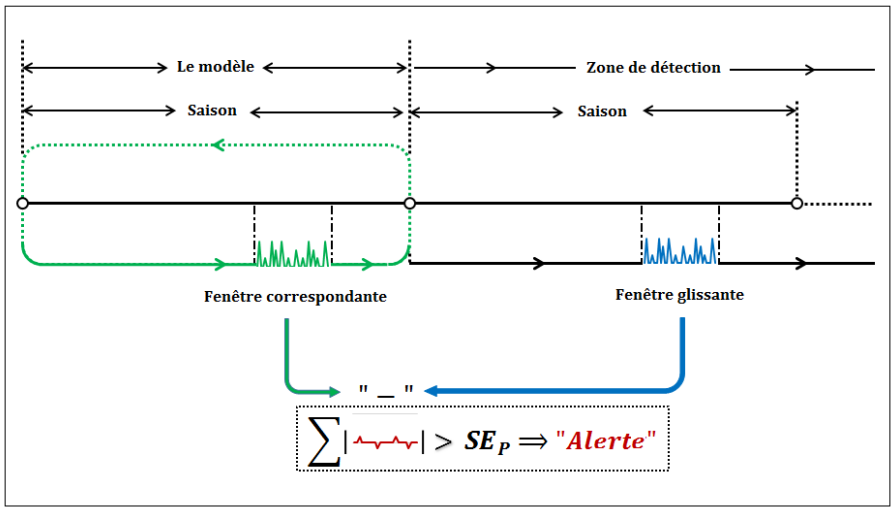


FIGURE 5.2: Mécanisme de détection des anomalies

5.2 Évaluation de performance

Dans cette section, nous allons évaluer l'algorithme 6 qui doit être applicable en effectuant l'ajustement multiplicatif de saison.

Nous avons capturé le trafic d'un réseaux corporel sans fil organisé en topologie étoile et constitué d'un coordinateur, six nœuds légitimes et un nœud attaquant. Ce dernier doit exercer un brouillage sélectif en tête de slot (SHJA) [16] de manière légère afin de ne pas être détecté pour le plus longtemps possible.

Nous avons simulé le réseau avec la norme IEEE 802.15.4 implimentée dans le framework INETMANET 2.0 [1] du simulateur OMNeT++.

Le tableau 5.1 décrit la configuration du réseau simulé.

TABLEAU 5.1: La configuration réseau.

La paire (SO, BO)	**Les périodes avant l'ajustement (s)**	**Les périodes après l'ajustement (s)**	**Bande radio de transmission**	**Nombre de simulations**
$(7, 8)$	$\{120, 280, 550, 700, 840, 900\}$	$\{125, 82912, 293, 60128, 576, 7168, 734, 0032, 880, 80384, 943, 7184\ \}$	2,4 GHz (250 kbps débit de données)	50 pour chaque type d'évaluation

Sans avoir appliqué l'ajustement multiplicatif sur les périodes entières du tableau 5.1, la saison qui englobe tous les scénarios d'arrivée des paquets de différents nœuds et qui prend en considération l'altération du trafic par la supertrame durerait plus que 2 ans et 3 mois et 11 jours. Le méga-ajustement réduira cette énorme durée à 40 heures et 22 minutes approximativement, donnant une efficacité de $\frac{32}{15625}$.

Nous avons adopté le taux de détection, le taux de faux positifs et la précision (accuracy) comme métriques de performance de l'algorithme. Pour chaque métrique, les résultats sont moyennés sur 50 simulations, chacune a un état d'initialisation différent.

À chaque supertrame, l'attaquant sélectionne, aléatoirement, un seul nœud du réseau en lui faisant subir l'attaque en tête de slot. En addition de limiter l'attaque sur un seul nœud victime à la fois pour assurer sa légèreté, cette dernière peut être renforcée en adoptant une probabilité représentant la certitude de l'attaque dans une supertrame. Par exemple, attaquer aléatoirement un nœud du réseau dans chaque supertrame est faite avec une probabilité d'attaque 100%. En revanche, pour réduire l'intensité de l'attaque à la moitié, il faut l'effectuer avec une probabilité de 50%.

1. http ://github.com/aarizaq/inetmanet-2.0

Que ce soit pour le taux de faux positifs ou le taux de détection, chaque simulation élémentaire dure trois saisons. Pour la première métrique, l'évaluation était en absence d'attaque où les anomalies naturelles, à savoir le PER, sont générées par un générateur aléatoire qui suit une distribution normale dont les paramètres sont présentés dans le tableau 5.2. La gamme BER qui correspond à la majorité des valeurs PER est présenté dans ce tableau [2] [3].

TABLEAU 5.2: Les paramètres de la distribution de PER.

μ	σ	**La gamme BER correspondante au 99% des valeurs PERs (≈)**
$\approx 4,838 \times 10^{-4}$	$\approx 1,875 \times 10^{-4}$	$10^{-14} - 10^{-6}$

Le taux de faux positifs et le taux de détection dans une durée de simulation (3 saisons) sont obtenus d'après la formule suivante :

$$\frac{Nbre(W^*)}{2 \times \frac{S_{ajt}}{pas} - w + 1}$$

Où $Nbre(W^*)$ est le nombre de fenêtres vérifiant la condition de la ligne 3 de l'algorithme 6 et w est la taille de la fenêtre en pas. La taille que nous avons choisie pour le pas est égale à $3.145728\,s$. Le dénominateur n'est que le nombre total de fenêtres dans les deux dernières saisons de test dans la période de simulation (la première saison est le modèle).

Bien qu'il existe une seule formule, l'évaluation des deux métriques se diffère selon le contexte. Le calcule de taux de faux positifs se fait en absence d'attaque tandis que celui de taux de détection est réalisé en présence d'attaque.

Nous introduisons la précision de l'algorithme comme suit :

$$Précision = \frac{VP + VN}{VP + VN + FP + FN}$$

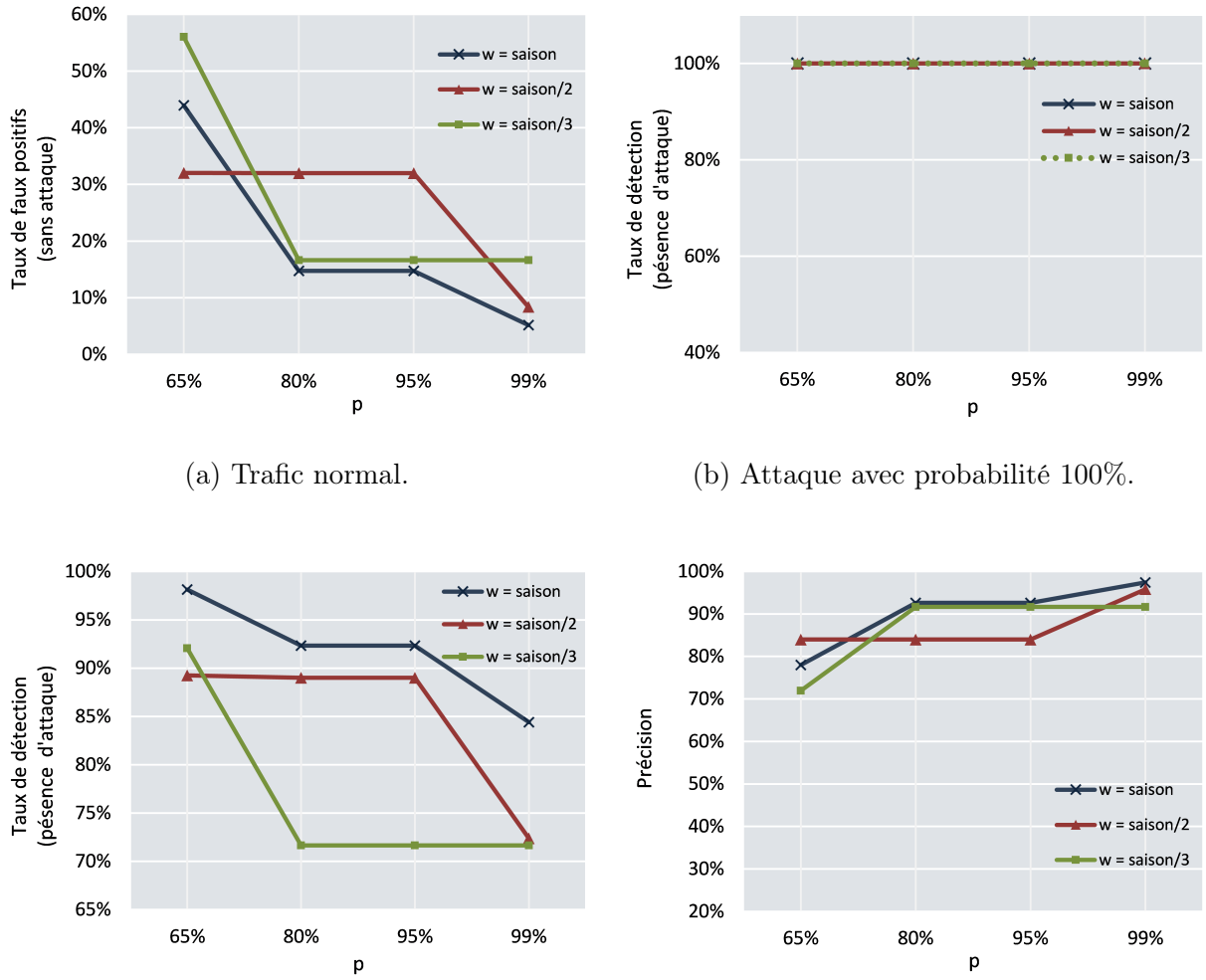
Où VP, VN, FP et FN sont respectivement le nombre de vrais positifs, de vrais négatifs, de faux positifs et de faux négatifs.

2. La correspondance se fait par la formule $PER = 1 - (1 - BER)^N$, où N est la taille de trame en bits. D'après cette formule, la distribution de BER ne doit nécessairement pas être normale comme celle du PER.

3. Dans ce travail, on considère la distribution en fonction des facteurs environnementaux et pas comme des facteurs physiques qui peuvent avoir une relation directe avec le BER comme le rapport signal sur bruit (SNR). Ainsi, l'environnement de déploiement affecte ces facteurs physiques de la même manière qu'il affecte le BER durant tout le jour.

Par souci d'authenticité, le générateur de PER, le générateur aléatoire d'attaque (la sélection du nœud victime) et le générateur de probabilité d'attaque sont réinitialisés par des graines aléatoires différentes dans chaque simulation.

La figure 5.3 présente les taux de faux positifs, taux de détection et précision en fonctions du facteur pourcentage p du seuil SE_p, et pour différentes tailles de fenêtres.



(a) Trafic normal.

(b) Attaque avec probabilité 100%.

(c) Attaque avec probabilité 1%.

(d) Attaque avec probabilité 100%.

FIGURE 5.3: Taux de faux positifs, taux de détection et précision pour l'algorithme 6 en fonction de la probabilité p.

Quant au taux de faux positifs (sous-figure 5.3a), nous constatons qu'il diminue avec la croissance du p, ce qui est naturel vue que ce dernier tend à couvrir le PER réel quand p augmente. En addition, nous observons, généralement, que plus est la taille de la fenêtre, meilleur serait le taux de faux positifs. Ceci s'explique, probablement, par l'amélioration de l'estimation du PER avec la croissance de la taille de la fenêtre.

Pour la deuxième sous-figure (5.3b), on remarque que, peu importe la taille de la fenêtre ou la valeur de p, le taux de détection était parfait. C'est une qualité persistante que nous avons observée dans cette algorithme. Pour cette raison, et malgré la légèreté de l'attaque, nous avons évalué le taux de détection de l'attaque avec probabilité 1% (presque en absence d'attaque) dans la sous-figure 5.3c. Ici, comme prévu, le taux de détection diminue avec la croissance de p ou la diminution de la taille de la fenêtre. Cependant, nous observons clairement que le taux de détection dépasse 70% dans tous les scénarios. C'est encore de très bons résultats pour une attaque assez légère comme celle en question.

L'algorithme, en fait, a bien fonctionné en termes de précision comme on peut le voir dans la sous-figure 5.3d. Même dans le cas d'un seuil PER de 65% et lorsque w est de taille $\frac{season}{3}$, la précision est toujours supérieure à 70%. Nous pensons que cette précision reflète les performances réelles de notre algorithme.

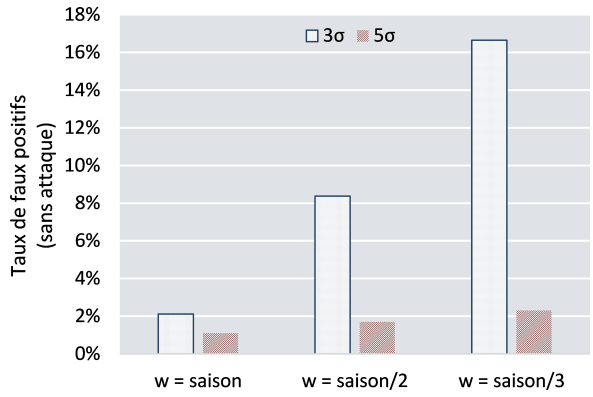
Bien que les résultats étaient, inclusivement satisfaisants, le taux de faux positifs de l'algorithme n'était pas à la hauteur du taux de détection. Pour cette raison, nous avons changer légèrement l'algorithme 6 pour améliorer le taux de faux positifs.

Nous pensons que les mesures élevées des taux de faux positifs étaient dû à la faible estimation du PER dans la partie gauche de l'inégalité de la ligne 3 de l'algorithme. La qualité de cette estimation dépend fortement à la taille w de la fenêtre et si cette taille n'est pas grande suffisamment, l'estimation locale du PER doit être trompeuse parfois. Donc, il faut mettre en place une technique pour corriger cette estimation.

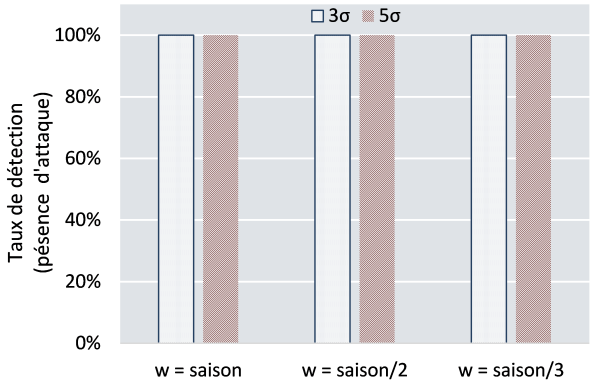
Puisque la taille de la fenêtre est limitée par les ressources disponibles dans le coordinateur, augmenter la taille de la fenêtre ne présente pas une solution pratique pour tous les scénarios, particulièrement, pour les plus petits PERs. Cependant, nous pouvons, plutôt, corriger le comportement de l'algorithme en modifiant la partie droite de l'inégalité en prenant des pourcentages plus grands que 100% (ou d'adopter la notation $SE_{n\sigma}$ au lieu de SE_p).

La figure 5.4 représente l'évaluation des métriques en question prenant $SE_{3\sigma}$ et $SE_{5\sigma}$ dans la partie droite de l'inégalité.

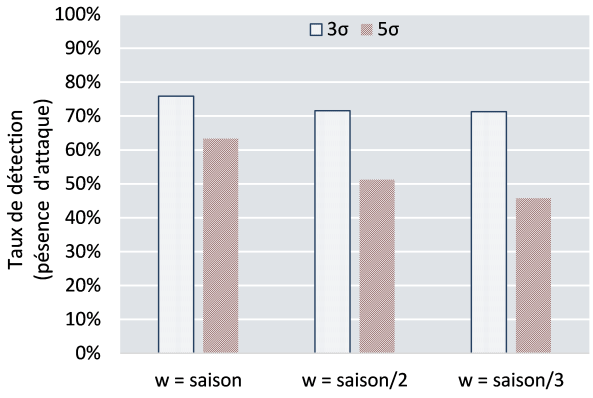
Dans la figure, nous observons que le taux de faux positif a été, en fait, amélioré tandis que le taux de détection est toujours parfait, même en cas de 5σ (sous-figure 5.4b). De plus, et prenant en considération le scénario d'attaque, le taux de détection pour celui avec probabilité de 1% était au moins acceptable.



(a) Trafic normal.



(b) Attaque avec probabilité 100%.



(c) Attaque avec probabilité 1%.

(d) Attaque avec probabilité 100%.

FIGURE 5.4: Taux de faux positifs, taux de détection et précision pour l'algorithme 6 après la correction de comportement.

5.3 Conclusion

L'analyse du trafic représente la meilleure approche de détection d'anomalies en cas de trafic périodique. Cette approche peut être inapplicable si le trafic subit des altérations à cause d'une supertrame comme celle de la norme IEEE 802.15.4. Cette dernière, en addition de la relation impair entre les périodes des nœuds, fait de la saison, qui englobe tous les scénarios d'arrivées des paquets, une durée insupportable, ni en temps ni en espace. Pour cette raison, nous avons proposé une ajustement de saison qui, en principe, cherche à créer plus de facteurs communs entre les périodes et la supertrame pour réduire sa durée.

En addition, nous avons proposé une technique qui bénéficie de l'ajustement multiplicatif pour la détection des anomalies dans le trafic périodique des réseaux basant sur l'IEEE

802.15.4 (à savoir les WBANs). Cette technique estime le PER localement dans une fenêtre glissante et vérifie s'il dépasse un seuil prédéfini qui représente le PER réel dans les condition naturelles.

Le taux de détection de la technique était parfait (100%) et le taux de faux positifs était raisonnable ($8,37\%$ pour $w = \frac{saison}{2}$) et ce dernier peut être amélioré en corrigeant le comportement de l'algorithme de détection.

Enfin, nous notons que l'ajustement multiplicatif et la technique de détection d'anomalies sont indépendant l'une de l'autre. De ce fait, on peut bénéficier de l'ajustement multiplicatif pour réduire la saison, et ensuite utiliser n'importe quelle autre méthode comme les modèles ARIMA (AutoRegressive Integrated Moving Average) [69] pour détecter les anomalies dans un signal continu que l'on choisit soigneusement.

Conclusion générale

Les réseaux de capteurs sans fil se composent d'un ensemble de capteurs physiologiques qui se trouvent autour et dans le corps humain dans le but de surveiller l'état physiologique du corps.

Ces réseaux ayant une large gamme d'applications allant de la surveillance continue de la santé et assistance des handicapés au sport et divertissement. Les différentes exigences de ces applications avec les caractéristiques restreintes de l'environnement de déploiement ont introduit beaucoup de défis à surmonter afin que ces réseaux soient prêts à être exploités.

Parmi les technologies qui convient les réseaux corporels sans fil, on trouve la norme IEEE 802.15.4 qui garantit un débit dédié aux appareils grâce au slots GTS dans la période CFP de la supertrame. Les slots GTS représentent une cible facile pour le brouillage sélectif vu la facilité de déterminer leurs débuts et longueurs. En outre, dans le cas du trafic périodique, un adversaire peut exploiter l'altération de la périodicité causée par la structure de la supertrame et le comportement de la norme pour optimiser les ressources de l'attaque.

Dans le brouillage en tête du slot, l'adversaire émet une petite trame au début du slot de la victime pour corrompre la majorité du trafic en évitant de brouiller le slot entier. Nos résultats confirment l'efficacité de cette attaque qui a atteint 97% en effectuant seulement $3,33\%$ du brouillage complet.

Une solution d'atténuation pour cette attaque est la randomisation du départ des paquets pour ajouter un facteur d'ambiguïté sur leur temps d'arrivée. Cette mesure peut, en fait, récupérer la majore partie du ressources et son efficacité a une relation inverse avec la durée de brouillage, ce qui présente un avantage majeur de cette technique.

La solution précédente tombe sous la section de la protection pro-active des réseaux. Pour compléter notre travail nous avons proposé un algorithme pour la protection active des réseaux corporels. Cet algorithme tend à surveiller la "normalité" des anomalies présentes dans le trafic en comparant le PER estimé dans une intervalle de temps prédéfinie avec le PER réel dans le but de détecter une divergence. Il s'avère que la surveillance du nombre de

paquets peut servir d'une approche très efficace pour la détection des anomalies en donnant des taux de faux positifs et détection très raisonnables.

Pour construire un modèle de communication pour la détection des anomalies, il faut d'abord capturer la saisonnalité dans le trafic. Ceci pourrait être impossible à cause de la durée immense de la saison, qui tend d'être insupportable vu la relation impaire entre les périodes des nœuds et la supertrame. Pour cette raison, nous avons proposé l'ajustement multiplicatif du saison. Avec ce dernier, les périodes seront changées légèrement afin de créer plus de facteurs communs entre la supertrame et les périodes. En fait, l'ajustement multiplicatif nous a servi énormément à capturer la saisonnalité en réduisant la saison à tel point que notre algorithme était facilement applicable.

Dans futur travail, et concernant la version optimisée du brouillage en tête de slot, on peut exploiter des propriétés mathématiques plus sophistiquées pour optimiser de plus les ressources de l'attaque.

Pour la détection des anomalies, nous tendons, à utiliser l'ajustement multiplicatif dans les modèles mathématiques existants pour la détection des anomalies dans les signaux continus, ce qui doivent être choisis soigneusement pour qu'ils modélisent réellement le fonctionnement du réseau.

Compte tenu de la tendance mondiale aux méthodes d'apprentissage approfondi, on peut les utiliser pour modéliser le trafic dans les cas où l'ajustement multiplicatif ne soit pas efficace.

Concernant l'évaluation des approches proposées, on peut considérer d'autres facteurs comme la taille du slot de l'appareil en termes de slots GTS lors de l'évaluation. De plus, on peut passer à l'échelle pour étudier les effets potentiels de la taille du réseau sur les différentes métriques d'évaluation réseau.

Annexes

Annexe A

Considérant les deux limites d'un tour arbitraire de la période P, nous définissons trois parties constituant ce tour ;

(1) La différence entre le début de slot de nœud qui suit la première limite et la limite elle-même. Nous appellerons cette période la *tête*.

(2) La période entre le début du premier et dernier slots situés dans le tour. Nous appellerons cette période le *corps*.

(3) La différence entre la deuxième limite et le début du dernier slot situé dans le tour. Nous appellerons cette période la *queue*.

Nous nous référons à la période entre la première limite du tour de P et le début du slot qui précède cette limite par le *décalage*.

La figure 5.5 illustre ces trois parties.

Soit N le nombre de supertrames qui séparent deux transmissions successives affectées par la couche MAC de l'IEEE 802.15.4 et soit $slot$ et BI la durée du slot et la durée de l'intervalle beacon, respectivement.

Le but de l'annexe est de prouver ce qui suit :

$$Pdiv_{réel}BI \leq N \leq Pdiv_{réel}BI + 1$$

Premièrement, nous avons :

$$N = pré\_délai + |corps| + post\_délai$$

Où :

- $pré\_délai$ c'est un nombre déterminant s'il y a un retardement au début du tour. Cette variable prend 0 en cas de retard et 1 dans le cas contraire.

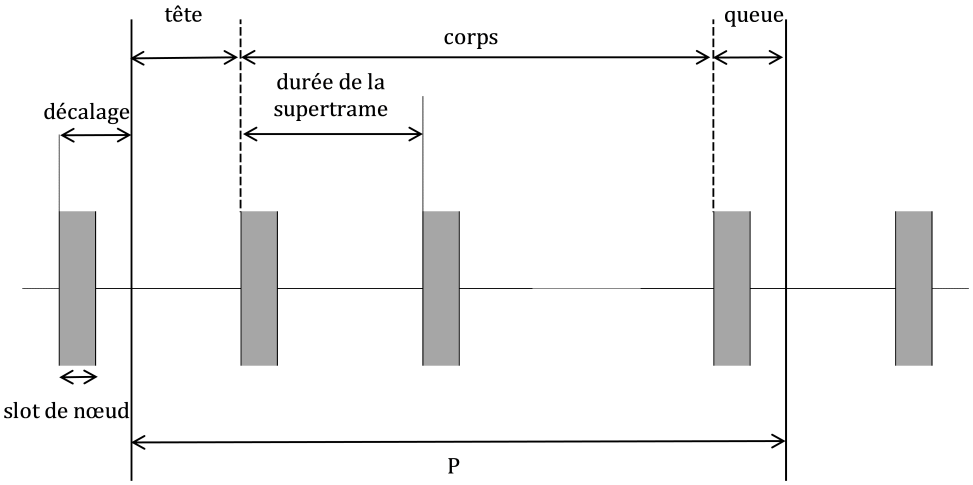


FIGURE 5.5: Un tour arbitraire de P avec les trois parties introduites : la tête, le corps et la queue

- $|corps|$ c'est le nombre de supertrames dans le *corps*.
- *post_délai* c'est le nombre de reports causés par la *queue*.

- En admettant que $décalage = 0$:

  Dans ce cas, il est évident que $tête = 0$, $corps = (Pdiv_{réel}BI) \times BI$ et $queue = Pmod_{réel}BI$.

  Donc, $pré\_délai = 0$ et $|corps| = Pdiv_{réel}BI$.

  Puisque $Pmod_{réel}BI < BI$, alors l'arrivée du deuxième paquet peut au plus être retardée une seule fois. Alors $post\_délai \leq 1$.

  Par conséquent : $Pdiv_{réel}BI \leq N \leq Pdiv_{réel}BI + 1$.

- Supposant que $décalage \neq 0$:

  Nous avons

$$\begin{aligned} corps &= P - (BI - décalage) - (Pmod_{réel}BI + décalage) \\ &= P - BI + décalage - Pmod_{réel}BI - décalage \\ &= P - BI - Pmod_{réel}BI \end{aligned}$$

  Puisque $P = (Pdiv_{réel}BI) \times BI + Pmod_{réel}BI$, alors,

$$\begin{aligned} corps &= (Pdiv_{réel}BI) \times BI + Pmod_{réel}BI - BI \\ &\quad - Pmod_{réel}BI \\ &= (Pdiv_{réel}BI) \times BI - BI \\ corps &= (Pdiv_{réel}BI - 1) \times BI \end{aligned}$$

Donc,

$|corps| = Pdiv_{réel}BI - 1$

Puisque $|corps|$ est constant, trouver une limite pour N implique de trouver une limite pour $pré\_délai$ et $post\_délai$.

Comme $décalage + tête = BI$ alors $0 \leq décalage \leq BI$.

En conséquence, nous avons deux possibilités :

$0 \leq décalage < slot$ et $slot \leq décalage \leq BI$, ce qui implique $pré\_délai = 1$ et $pré\_délai = 0$, respectivement.

D'où

$$0 \leq pré\_délai \leq 1$$

D'autre part, nous avons :

$$Pmod_{réel}BI < BI \text{ and } décalage < BI$$

Alors

$$Pmod_{réel}BI + décalage < 2 \times BI$$

Donc

$$queue < 2 \times BI$$

En conséquence, nous avons trois possibilités :

$0 \leq queue < slot$, $slot \leq queue < BI + slot$ et $BI + slot \leq queue < 2 \times BI$, ce qui implique $post\_délai = 0$, $post\_délai = 1$ et $post\_délai = 2$.

D'où

$$0 \leq post\_délai \leq 2$$

Donc

$$\begin{aligned} Pdiv_{réel}BI - 1 &\leq pré\_délai + |corps| \\ &\quad + post\_délai \\ &\leq Pdiv_{réel}BI + 2 \end{aligned}$$

Maintenant, nous devons prouver que cette somme ne peut pas prendre les frontières d'inégalité, c'est à dire, $Pdiv_{réel}BI - 1$ et $Pdiv_{réel}BI + 2$.

Puisque $pré\_délai$ a 0 et 1 comme valeurs possibles et $post\_délai$ peut prendre les valeurs 0, 1 et 2, il suffit de prouver que $pré\_délai$ inévitablement prend 0 quand $post\_délai$ prend 2 et prend 1 quand $post\_délai$ prend 0.

- Supposant que $post\_délai = 2$:

  Cela implique

$$queue \geq BI + slot$$

  Qui est l'équivalent de :

$$Pmod_{réel}BI + décalage \geq BI + slot$$

  Donc

$$décalage \geq BI + slot - Pmod_{réel}BI$$

  Puisque

$$Pmod_{réel}BI < BI$$

  Alors

$$décalage > slot$$

  Par conséquent, la première transmission est indéniablement différée, ce qui signifie $pré\_délai = 0$.

- $post\_délai = 0$

  Ça signifie

$$queue < slot$$

  c'est à dire

$$Pmod_{réel}BI + décalage < slot$$

Alors

$$décalage < slot$$

Par conséquent, la première transmission n'est pas différée, ce qui signifie $pré\_délai = 1$.

Cela se traduit par :

$$\begin{aligned} Pdiv_{réel}BI &\leq pré\_délai + |corps| \\ &\quad + post\_délai \\ &\leq Pdiv_{réel}BI + 1 \end{aligned}$$

C'est à dire $Pdiv_{réel}BI \leq N \leq Pdiv_{réel}BI + 1$

Annexe B

Supposons que $n \geq BO + 4$, donc,

$$n + 10\alpha \geq BO + 4 + 10\alpha > BO + 4 + 3\alpha$$

L'efficacité sera de la forme :

$$\begin{aligned} \frac{S_{ajt}}{S} &= \frac{2^{n+10\alpha} \times 5^{m \vee (3\alpha-5)}}{2^n \times 5^m} \times 10^{-3\alpha} \\ &= \left(\frac{5^{m \vee (3\alpha-5)}}{5^m}\right) \times \left(\frac{2^{10\alpha}}{10^{3\alpha}}\right) \\ &= \left(\frac{5^{m \vee (3\alpha-5)}}{5^m}\right) \times \left(\frac{2^{10}}{10^3}\right)^{\alpha} \end{aligned}$$

Il est clair que $\frac{5^{m \vee (3\alpha-5)}}{5^m} \geq 1$ et $(\frac{2^{10}}{10^3})^{\alpha} > 1$, d'où :

$$\frac{S_{ajt}}{S} > 1 \qquad , \forall n \geq BO + 4$$

Annexe C

Soit α et $\acute{\alpha}$ deux ordres d'ajustement et S_{ajt} et $S\acute{}_{ajt}$ les deux saisons ajustées par α et $\acute{\alpha}$, respectivement.

D'après la formule (4.3) :

$$S_{ajt} = 2^{(n+10\alpha) \vee (BO+4+3\alpha)} \times 3^{k \vee 1} \times 5^{m \vee (3\alpha-5)} \times P^* \times 10^{-3\alpha}$$

$$S\acute{}_{ajt} = 2^{(n+10\acute{\alpha}) \vee (BO+4+3\acute{\alpha})} \times 3^{k \vee 1} \times 5^{m \vee (3\acute{\alpha}-5)} \times P^* \times 10^{-3\acute{\alpha}}$$

Donc,

$$\begin{aligned}\frac{S_{ajt}}{S_{ajt}^{'}} &= \frac{2^{(n+10\alpha)\vee(BO+4+3\alpha)} \times 5^{m\vee(3\alpha-5)} \times 10^{-3\alpha}}{2^{(n+10\acute{\alpha})\vee(BO+4+3\acute{\alpha})} \times 5^{m\vee(3\acute{\alpha}-5)} \times 10^{-3\acute{\alpha}}} \\ &= \frac{2^{3\alpha} \times 2^{(n+7\alpha)\vee(BO+4)} \times 5^{m\vee(3\alpha-5)} \times 10^{-3\alpha}}{2^{3\acute{\alpha}} \times 2^{(n+7\acute{\alpha})\vee(BO+4)} \times 5^{m\vee(3\acute{\alpha}-5)} \times 10^{-3\acute{\alpha}}} \\ &= \frac{2^{(n+7\alpha)\vee(BO+4)} \times 5^{m\vee(3\alpha-5)} \times 5^{-3\alpha}}{2^{(n+7\acute{\alpha})\vee(BO+4)} \times 5^{m\vee(3\acute{\alpha}-5)} \times 5^{-3\acute{\alpha}}}\end{aligned}$$

Puisque $n + 7\acute{\alpha} \geq 7\acute{\alpha} \geq 21 > BO + 4$, d'où :

$$\frac{S_{ajt}}{S_{ajt}^{'}} = \frac{2^{(n+7\alpha)\vee(BO+4)} \times 5^{m\vee(3\alpha-5)}}{2^{n+7\acute{\alpha}} \times 5^{m\vee(3\acute{\alpha}-5)}} \times 5^{3(\acute{\alpha}-\alpha)} \tag{5.1}$$

- Supposons que $3 \leq \alpha < \acute{\alpha}$:

$$3 \leq \alpha < \acute{\alpha} \implies 21 \leq 7\alpha$$

Puisque $n \geq 0$ et $1 \leq BO \leq 14$, donc,

$$BO + 4 \leq 18 < n + 7\alpha$$

La formule (5.1) sera donc :

$$\begin{aligned}\frac{S_{ajt}}{S_{ajt}^{'}} &= \frac{2^{n+7\alpha} \times 5^{m\vee(3\alpha-5)}}{2^{n+7\acute{\alpha}} \times 5^{m\vee(3\acute{\alpha}-5)}} \times 5^{3(\acute{\alpha}-\alpha)} \\ &= (\frac{5^{3(\acute{\alpha}-\alpha)}}{2^{7(\acute{\alpha}-\alpha)}}) \times (\frac{5^{m\vee(3\alpha-5)}}{5^{m\vee(3\acute{\alpha}-5)}}) \\ &= (\frac{5^3}{2^7})^{(\acute{\alpha}-\alpha)} \times (\frac{5^{m\vee(3\alpha-5)}}{5^{m\vee(3\acute{\alpha}-5)}})\end{aligned}$$

Il est clair que $(\frac{5^3}{2^7})^{(\acute{\alpha}-\alpha)} < 1$ et $\frac{5^{m\vee(3\alpha-5)}}{5^{m\vee(3\acute{\alpha}-5)}} \leq 1$, d'où :

$$\forall \alpha, \acute{\alpha} : 3 \leq \alpha < \acute{\alpha} \implies \frac{S_{ajt}}{S_{ajt}^{'}} < 1$$

- Supposons que $n \geq BO - 10$ et $2 \leq \alpha < \acute{\alpha}$:

Nous avons $\alpha \geq 2$ et $n \geq BO - 10$, donc,

$$n + 7\alpha \geq 14 + BO - 10 = BO + 4$$

De la même manière que dans la supposition précédente nous trouvons :

$$\frac{S_{ajt}}{S_{ajt}^{'}} = (\frac{5^3}{2^7})^{(\acute{\alpha}-\alpha)} \times (\frac{5^{m\vee(3\alpha-5)}}{5^{m\vee(3\acute{\alpha}-5)}}) < 1, \forall n \geq BO - 10$$

- Supposons que $n < BO - 10$ ($BO > 10$), $\alpha = 2$ et $\acute{\alpha} = 3$:

La formule (5.1) s'écrit donc comme :

$$\frac{S_{ajt}}{S_{ajt}^{'}} = \frac{2^{(n+14)\vee(BO+4)} \times 5^{m\vee 1}}{2^{n+21} \times 5^{m\vee 4}} \times 5^3 = \frac{2^{(n+10)\vee BO} \times 5^{m\vee 1}}{2^{n+17} \times 5^{m\vee 4}} \times 5^3$$

$n < BO - 10 \implies 2^{(n+10)\vee BO} = 2^{BO}$, alors :

$$\frac{S_{ajt}}{S_{ajt}^{'}} = \frac{2^{(n+10)\vee BO} \times 5^{m\vee 1}}{2^{n+17} \times 5^{m\vee 4}} \times 5^3 = (\frac{2^{BO}}{2^{n+17}}) \times (\frac{5^{m\vee 1}}{5^{m\vee 4}} \times 5^3)$$

Il est clear que $n + 17 - BO \geq n + 17 - 14 \geq 3$, par conséquence :

$$\frac{2^{BO}}{2^{n+17}} \leq 2^{-3}, \forall m \leq 2$$

D'autre part, pour $m \leq 2$:

$$\frac{5^{m\vee 1}}{5^{m\vee 4}} \times 5^3 = \frac{5^{m\vee 1}}{5^4} \times 5^3 \leq \frac{5^2}{5^4} \times 5^3 = 5$$

Par conséquent,

$$(\frac{2^{BO}}{2^{n+17}}) \times (\frac{5^{m\vee 1}}{5^{m\vee 4}} \times 5^3) \leq (2^{-3}) \times (5) = \frac{5}{8} < 1$$

Donc,

$$\frac{S_{ajt}}{S_{ajt}^{'}} < 1, \forall m \leq 2$$

Si $m \geq 4$:

$$\frac{5^{m\vee 1}}{5^{m\vee 4}} \times 5^3 = \frac{5^m}{5^m} \times 5^3 = 5^3$$

D'autre part :

$$n < BO - 10 \implies n + 17 - BO < 7 \implies n + 17 - BO \leq 6$$

D'où

$$2^{n+17-BO} \leq 2^6 \implies \frac{2^{BO}}{2^{n+17}} = \frac{1}{2^{n+17-BO}} \geq \frac{1}{2^6}$$

Donc,

$$(\frac{2^{BO}}{2^{n+17}}) \times (\frac{5^{m\vee 1}}{5^{m\vee 4}} \times 5^3) \geq (\frac{1}{2^6}) \times (5^3) = \frac{125}{64}$$

Par conséquent,

$$\frac{S_{ajt}}{S_{ajt}^{'}} > 1, \forall m \geq 4$$

Maintenant, supposant que m=3, alors :

$$\frac{S_{ajt}}{S_{ajt}^{'}} = (\frac{2^{BO}}{2^{n+17}}) \times (\frac{5^3}{5^4} \times 5^3) = (\frac{2^{BO}}{2^{n+17}}) \times (5^2)$$

$$n \geq BO - 12 \implies n + 17 - BO \geq 5$$

Donc,

$$\frac{2^{BO}}{2^{n+17}} = \frac{1}{2^{n+17-BO}} \leq \frac{1}{2^5}$$

D'où,

$$\frac{S_{ajt}}{S_{ajt}^{'}} = (\frac{2^{BO}}{2^{n+17}}) \times (5^2) = (\frac{2^{BO}}{2^{n+17}}) \times (5^2) \leq \frac{5^2}{2^5} = \frac{25}{32}$$

Par conséquence,

$$\frac{S_{ajt}}{S_{ajt}^{'}} < 1, \forall n \geq BO - 12$$

En commençons par l'implication ($n < BO - 12 \implies n + 17 - BO \leq 4$), nous pouvons, avec des étapes similaires, arriver à :

$$\frac{S_{ajt}}{S_{ajt}^{'}} > 1, \forall n < BO - 12$$

Bibliographie

[1] B. Lo and G.-Z. Yang, "Key technical challenges and current implementations of body sensor networks," in *Proc. 2nd International Workshop on Body Sensor Networks (BSN 2005)*, Citeseer, 2005.

[2] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks : A survey," *Mob. Netw. Appl.*, vol. 16, pp. 171–193, Apr. 2011. doi : 10.1007/s11036-010-0260-8.

[3] I. . WG, "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4 : Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 1–320, Sept 2006. doi : 10.1109/IEEESTD.2006.232110.

[4] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Netw.*, vol. 17, pp. 1–18, Jan. 2011. doi : 10.1007/s11276-010-0252-4.

[5] S. Movassaghi, P. Arab, and M. Abolhasan, "Wireless technologies for body area networks : Characteristics and challenges," in *2012 International Symposium on Communications and Information Technologies (ISCIT)*, pp. 42–47, IEEE, 2012.

[6] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra, and T. H. Aldhyani, "Wearable wireless body area networks for medical applications," *Computational and Mathematical Methods in Medicine*, vol. 2021, 2021.

[7] R. Sokullu, O. Dagdeviren, and I. Korkmaz, "On the ieee 802.15.4 mac layer attacks : Gts attack," in *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*, pp. 673–678, Aug 2008. doi : 10.1109/SENSORCOMM.2008.75.

[8] R. Sokullu, I. Korkmaz, and O. Dagdeviren, "Gts attack : An ieee 802.15. 4 mac layer attack in wireless sensor networks," *International Journal On Advances in Internet Technologies*, vol. 2, no. 1, pp. 104–114, 2009.

[9] R. Daidone, G. Dini, and M. Tiloca, "A solution to the gts-based selective jamming attack on ieee 802.15.4 networks," *Wirel. Netw.*, vol. 20, pp. 1223–1235, July 2014. doi : 10.1007/s11276-013-0673-y.

[10] M. Tiloca, D. D. Guglielmo, G. Dini, G. Anastasi, and S. K. Das, "Jammy : A distributed and dynamic solution to selective jamming attack in tdma wsns," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 392–405, July 2017. doi : 10.1109/TDSC.2015.2467391.

[11] M. Tiloca, D. De Guglielmo, G. Dini, G. Anastasi, and S. K. Das, "Dish : Distributed shuffling against selective jamming attack in ieee 802.15. 4e tsch networks," *ACM transactions on sensor networks*, 2018.

[12] T. Kudo, T. Morita, T. Matsuda, and T. Takine, "Pca-based robust anomaly detection using periodic traffic behavior," in *2013 IEEE International Conference on Communications Workshops (ICC)*, pp. 1330–1334, IEEE, 2013.

[13] D. Miao, X. Qin, and W. Wang, "The periodic data traffic modeling based on multiplicative seasonal arima model," in *2014 Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, IEEE, 2014.

[14] J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion detection in scada systems by traffic periodicity and telemetry analysis," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 318–325, IEEE, 2016.

[15] R. R. R. Barbosa, R. Sadre, and A. Pras, "Towards periodicity based anomaly detection in scada networks," in *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)*, pp. 1–4, IEEE, 2012.

[16] M. Achour, M. Mana, and A. Rachedi, "New slot-head jamming attack and mitigation mechanism for wireless body area networks," in *2018 IEEE Global Communications Conference (GLOBECOM)*, (Abu Dhabi, United Arab Emirates), pp. 1–6, Dec 2018.

[17] M. Achour, M. Mana, and A. Rachedi, "On the issues of selective jamming in ieee 802.15. 4-based wireless body area networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 135–150, 2020.

[18] M. Achour and M. Mana, "Seasonal adjustment for traffic modeling and analysis in ieee 802.15.4 networks," in *2022 7th International Conference on Image and Signal Processing and their Applications (ISPA)*, (Mostaganem, Algeria), pp. 1–6, may 2022.

[19] M. Achour, M. Mana, and S. Achour, "Exploiting traffic seasonality for anomaly detection in IEEE 802.15.4 networks," in *2022 19th International Multi-Conference on Systems, Signals & Devices (SSD)*, (Sétif, Algeria), pp. 1–6, may 2022.

[20] G. Ragesh and K. Baskaran, "An overview of applications, standards and challenges in futuristic wireless body area networks," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 1, pp. 180–186, 2012.

[21] J. Ahmad and F. Zafar, "Review of body area network technology & wireless medical monitoring," *International Journal of Information and Communication Technology*, vol. 2, no. 2, pp. 186–188, 2012.

[22] E. Karulf, "Body area networks (ban)," *A survey paper written under guidance of Prof. Raj Jain*, 2008.

[23] H. Fouad, "Patient-oriented web telemedicine system for health monitoring," *J. Commun. Comput*, vol. 11, pp. 168–178, 2014.

[24] K. Lin, M. Chen, J. J. Rodrigues, and H. Ge, "System design and data fusion in body sensor networks," in *Telemedicine and E-Health Services, Policies, and Applications : Advancements and Developments*, pp. 1–25, IGI Global, 2012.

[25] S. M. R. Al Masud, "Study and analysis of scientific scopes, issues and challenges towards developing a righteous wireless body area network," *International Journal Of Soft Computing And Engineering (IJSCE)*, vol. 3, no. 2, pp. 243–251, 2013.

[26] S. Park and S. Jayaraman, "Enhancing the quality of life through wearable technology," *IEEE Engineering in medicine and biology magazine*, vol. 22, no. 3, pp. 41–48, 2003.

[27] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks : A survey," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 1658–1686, Third 2014. doi : 10.1109/SURV.2013.121313.00064.

[28] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless communications*, vol. 17, no. 1, pp. 80–88, 2010.

[29] C. Otto, A. Milenković, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *J. Mob. Multimed.*, vol. 1, pp. 307–326, Jan. 2005.

[30] M. Dash and R. Mishra, "The development & implementation of wireless body area networks," *International Journal of Engineering Research*, vol. 3, no. 3, pp. 138–140, 2014.

[31] X. Lai, Q. Liu, X. Wei, W. Wang, G. Zhou, and G. Han, "A survey of body sensor networks," *Sensors*, vol. 13, no. 5, pp. 5406–5447, 2013.

[32] O. Aziz, B. Lo, A. Darzi, and G.-Z. Yang, *Introduction*, pp. 1–39. London : Springer London, 2006. doi : 10.1007/1-84628-484-8_1.

[33] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks : architecture, security challenges and research opportunities," *Computers & Security*, vol. 104, p. 102211, 2021.

[34] M. A. Hanson, H. C. Powell Jr, A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor, and J. Lach, "Body area sensor networks : Challenges and opportunities," *Computer*, vol. 42, no. 1, pp. 58–65, 2009.

[35] A. Arya and N. Bilandi, "A review : Wireless body area networks for health care," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 4, pp. 3800–3806, 2014.

[36] A. Boulis, D. Smith, D. Miniutti, L. Libman, and Y. Tselishchev, "Challenges in body area networks for healthcare : The mac," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 100–106, 2012.

[37] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[38] S. F. Qadri, S. A. Awan, M. Amjad, M. Anwar, and S. Shehzad, "Applications, challenges, security of wireless body area networks (wbans) and functionality of ieee 802.15. 4/zigbee," *Sci. Int.(Lahore)*, vol. 25, no. 4, pp. 697–702, 2013.

[39] J. Dong and D. Smith, "Cooperative body-area-communications : Enhancing coexistence without coordination between networks," in *2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC)*, pp. 2269–2274, IEEE, 2012.

[40] S. Kanwal, J. Rashid, J. Kim, S. Juneja, G. Dhiman, and A. Hussain, "Mitigating the coexistence technique in wireless body area networks by using superframe interleaving," *IETE Journal of Research*, pp. 1–15, 2022.

[41] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101883, 2021.

[42] T. Jabeen, H. Ashraf, and A. Ullah, "A survey on healthcare data security in wireless body area networks," *Journal of ambient intelligence and humanized computing*, vol. 12, no. 10, pp. 9841–9854, 2021.

[43] IEEE 802.15 WG, "Ieee standard for local and metropolitan area networks–part 15.4 : Low-rate wireless personal area networks (lr-wpans) amendment 1 : Mac sublayer," *IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1–225, April 2012.

[44] N. Choudhury, R. Matam, M. Mukherjee, and J. Lloret, "A performance-to-cost analysis of ieee 802.15.4 mac with 802.15.4e mac modes," *IEEE Access*, vol. 8, pp. 41936–41950, 2020.

[45] C. Balarengadurai and S. Saraswathi, "Comparative analysis of detection of ddos attacks in ieee 802.15. 4 low rate wireless personal area network," *Procedia engineering*, vol. 38, pp. 3855–3863, 2012.

[46] V. B. Misic, J. Fang, and J. Misic, "Mac layer security of 802.15. 4-compliant networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, pp. 8–pp, IEEE, 2005.

[47] Y. M. Amin and A. T. Abdel-Hamid, "A comprehensive taxonomy and analysis of ieee 802.15. 4 attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[48] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N. R. Prasad, "An investigation on ieee 802.15. 4 mac layer attacks," in *Proc. of WPMC*, vol. 41, pp. 42–92, 2007.

[49] D. Martins and H. Guyennet, "Attacks with steganography in phy and mac layers of 802.15. 4 protocol," in *2010 Fifth International Conference on Systems and Networks Communications*, pp. 31–36, IEEE, 2010.

[50] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, pp. 101–114, Jan 2012. doi : 10.1109/TDSC.2011.41.

[51] F. Chen and F. Dressler, "A simulation model of ieee 802.15. 4 in omnet++," *Proc. of the 6th GI/ITG KuVS Fachgesprach Drahtlose Sensornetze (FGSN)*, pp. 35–38, 2007.

[52] R. J. Hyndman and G. Athanasopoulos, *Forecasting : principles and practice*. OTexts, 2018.

[53] M. Haffey, M. Arlitt, and C. Williamson, "Modeling, analysis, and characterization of periodic traffic on a campus edge network," in *2018 IEEE 26th Int. Symp. on Modeling, Anal., Simul. Comput. Telecommun. Syst. (MASCOTS)*, pp. 170–182, 2018.

[54] F. S. Passino and N. A. Heard, "Classification of periodic arrivals in event time data for filtering computer network traffic," *Statistics and Computing*, vol. 30, no. 5, pp. 1241–1254, 2020.

[55] S. P. Sone, J. Lehtomäki, Z. Khan, and K. Umebayashi, "Forecasting wireless network traffic and channel utilization using real network/physical layer data," in *2021 Joint Eur. Conf. on Netw. and Commun. & 6G Summit (EuCNC/6G Summit)*, pp. 31–36, 2021.

[56] A. Knapińska, P. Lechowicz, and K. Walkowiak, "Machine-learning based prediction of multiple types of network traffic," in *Int. Conf. on Comput. Sci.*, pp. 122–136, 2021.

[57] F. Metzger, T. Hoßfeld, A. Bauer, S. Kounev, and P. E. Heegaard, "Modeling of aggregated iot traffic and its application to an iot cloud," *Proc. IEEE*, vol. 107, no. 4, pp. 679–694, 2019.

[58] M. López-Benítez, C. Majumdar, and S. N. Merchant, "Aggregated traffic models for real-world data in the internet of things," *IEEE Wireless Commun. Letters*, vol. 9, no. 7, pp. 1046–1050, 2020.

[59] G. Grätzer, *Lattice Theory : Foundation*. 01 2011. doi : 10.1007/978-3-0348-0018-1.

[60] C. Do Xuan, H. Thanh, and N. T. Lam, "Optimization of network traffic anomaly detection using machine learning.," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 11, no. 3, 2021.

[61] O. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, "A machine learning based framework for iot device identification and abnormal traffic detection," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3743, 2022.

[62] A. Shahraki, M. Abbasi, A. Taherkordi, and A. D. Jurcut, "A comparative study on online machine learning techniques for network traffic streams analysis," *Computer Networks*, vol. 207, p. 108836, 2022.

[63] Q. Ma, C. Sun, B. Cui, and X. Jin, "A novel model for anomaly detection in network traffic based on kernel support vector machine," *Computers & Security*, vol. 104, p. 102215, 2021.

[64] F. Carrera, V. Dentamaro, S. Galantucci, A. Iannacone, D. Impedovo, and G. Pirlo, "Combining unsupervised approaches for near real-time network traffic anomaly detection," *Applied Sciences*, vol. 12, no. 3, p. 1759, 2022.

[65] H. Abdi and L. J. Williams, "Principal component analysis," *Wiley interdisciplinary reviews : computational statistics*, vol. 2, no. 4, pp. 433–459, 2010.

[66] S. A. Boyer, *SCADA : supervisory control and data acquisition*. International Society of Automation, 2009.

[67] J. Dong, *Estimation of Bit Error Rate of any digital Communication System*. PhD thesis, Université de Bretagne Occidentale, 2013.

[68] K. Meier, J. Brudney, and J. Bohte, *Applied statistics for public and nonprofit administration*. Nelson Education, 2011.

[69] G. E. Box, G. M. Jenkins, G. C. Reinsel, and G. M. Ljung, *Time series analysis : forecasting and control*. John Wiley & Sons, 2015.

Peer-to-Peer Networking and Applications (2021) 14:135–150
https://doi.org/10.1007/s12083-020-00988-1

On the issues of selective jamming in IEEE 802.15.4-based wireless body area networks

M'hammed Achour[1] · Mohammed MANA[1] · Abderrezak Rachedi[2]

Received: 3 November 2019 / Accepted: 11 August 2020 / Published online: 29 August 2020

Abstract

The beacon-enabled mode of IEEE 802.15.4 provides a Time Division Multiple Access (TDMA) method for low power devices by adopting Guaranteed Time Slots (GTS). GTS communication is a potential target for selective jammers where they perform GTS attacks. In GTS attacks, the adversary selectively picks one of the reserved device slots to corrupt its incoming communication. Considering countermeasures, most existing solutions rely on slot position randomization to distribute the harm of the attack over the other GTS slots. These solutions may be effective in the case of full-slot jamming. However, the introduced GTS attacks consider only TDMA property of GTS communication and ignore other important properties like the protocol behavior and the superframe structure effect on the traffic. Considering these properties while performing GTS attacks exempts the adversary from full-slot jamming and renders the existing solutions with no effect. In this paper, we introduce a new efficient version of GTS attacks that benefits from both the standard behavior and the superframe effect on the periodic traffic to conserve the adversary's resources for the longest period. Additionally, we provide a solution specially developed to mitigate the harm from this detrimental attack. From extensive simulations conducted in this work, it follows that the attack is economic in terms of jamming duration and jamming packets ratio and the solution is efficient in terms of packet delivery ratio, energy consumption and delay overhead.

Keywords IEEE 802.15.4 beacon-enabled mode · Time Division Multiple Access · Selective jamming · GTS attacks · Superframe

1 Introduction

The huge advancements in microelectromechanical systems (MEMS) and miniaturization in general along with the urgent need to reduce healthcare and elderly assistance costs are the main contributors to the emergence of a new network category; wireless body area networks (WBAN).

In a WBAN, small low power sensors collect physiological information and send it periodically or in an event fashion to a gateway. The gateway can be a PDA, smartphone or a dedicated device. This device represents the bridge between the WBAN and a widespread network such as the internet or cellular networks. The collected physiological data can be blood pressure, temperature, glucose level or any other parameter that helps in patient monitoring or disease diagnosis.

Military, health and disabled assistance to name a few are some of the critical applications of WBANs. Less critical applications such as sport and entertainment can also benefit from these networks. This wide range of applications that WBANs can cover share one important goal: enhancing the user's quality of life [12].

Considering their efficiency, WBANs are an effective way to monitor a patient's health status [3]. In fact, using WBANs in routine healthcare monitoring can significantly reduce costs in terms of money, time and medical

✉ M'hammed Achour
mhammed.achour2@gmail.com

Mohammed MANA
mana3.mohammed@gmail.com

Abderrezak Rachedi
rachedi@u-pem.fr

[1] STIC Lab, Department of computer science, University of Tlemcen, Tlemcen, Algeria

[2] LIGM Lab, Institute of Electronics and Computer science Gaspard-Monge, University of Paris-Est, Paris, France

staff efforts [16]. Furthermore, the user is no longer bound to a hospital to monitor his or her health status; this can be achieved anywhere while performing daily activities [8], [18], [12]. The emergence of WBANs is one of the best examples of the full exploitation of new wireless technologies in mHealth and telemedicine [10].

IEEE 802.15.4 is the standard that serves low-cost short-range communication networks known as low-rate wireless personal area networks (LR-WPAN).

Considering the low-power requirement of WBANs, IEEE 802.15.4 has proven its economic advantage among previously adopted medical technologies such as Bluetooth and Wi-Fi.

Most WBAN implementations use IEEE 802.15.4 as enabling technology, some of which adopting the full combination ZigBee/IEEE 802.15.4 and others taking only the lower part of this protocol stack. These applications are either interested in other technologies depending on their suitability or they simply do not need the ZigBee part [6], [12].

The existing implementations rely on the non-beacon enabled mode of the IEEE 802.15.4 to proceed with communications even though the beacon-enabled mode is more energy saving. The centralized fashion of beacon-enabled mode helps the nodes to sleep when there is no oncoming communication and matches the centric model of WBAN. In this model, the coordinator along with the associated nodes form a star topology.

Selective jamming is a reactive attack that exploits protocol awareness and the shared medium nature to thwart communication in wireless networks.

In selective jamming, the adversary performs intentional interference while saving power by performing the attack selectively for short periods of time. These periods are selected based on previous knowledge of the protocol functionality [19]. In IEEE 802.15.4 beacon-enabled mode, a selective jammer picks one slot from the Contention Free Period (CFP) to corrupt its communication and turns to inactive state over the rest of the time. This form of selective jamming is typically referred to as a GTS jamming attack [24]. This attack causes considerable harm and is easy to perform at the same time.

In this work, we introduce a new version of GTS attacks that exploits the standard behavior and the deterministic transmission pattern in GTS mode in the case of a periodic monitoring application. In addition, a mitigation mechanism that considerably reduces the harm of this attack is proposed herein. The attack is low cost to the extent that executing it in a certain way could take down the whole network and makes previously reported solutions [7], [27], [26] ineffective. The solution is convenient with the IEEE 802.15.4 GTS mode and it can be implemented in the application layer or directly integrated in MAC layer.

This work extends previous work [2] in two aspects: (1) improving the efficiency of the proposed attack by exploiting the superframe effect on the target transmission pattern; and (2) studying the effect of timing characteristics of the superframe on the devised attack and its countermeasure.

To achieve that, we have had to consider 45 possible network configurations rather than considering only one configuration as we did in our previous work. Along with that, we evaluated the efficiency of the new enhanced attack compared to the previous one.

The rest of this paper is organized as follows. Section 2 provides some highlights and clarifies our motivation in this work. In Section 3, we provide literature on the main works related to GTS attacks and prevention solutions. Section 4 offers a brief description of the IEEE 802.15.4 beacon-enabled mode. The network model and some analyses are provided in Section 5. Sections 6 and 7 introduce and discuss our contributions; SHJA and RPD. Details, algorithms and discussions are provided therein. Considering many performance metrics, Section 8 evaluates and discusses the results of our work. We conclude the paper in Section 9.

2 Highlights and motivation

Security is one of the most important aspects to consider in network deployment. It encompasses the adoption of protection techniques for known breaches and the discovery of possible unknown vulnerabilities. As an act of security, companies are even hiring security experts to assess the security robustness of their networks and information systems.

The low power requirement and the centric model of IEEE 802.15.4 beacon-enabled mode makes this technology a potential choice to deploy wireless body area networks. Therefore, securing the former results, directly or indirectly, in securing the latter.

Aiming to increase the security of IEEE 802.15.4 beacon-enabled mode, we analyzed the protocol functionalities and the superframe structure to extract possible weaknesses that an intruder can exploit to disturb the user's communication. As a result, we introduced an optimized version of a previously introduced attack that targets network availability. In addition, we proposed a mitigation countermeasure in order to accomplish our goal in this work.

We supported our work with extensive simulation taking almost all possible network configurations and we provided some necessary mathematical proofs.

3 Related work

In this section, the works that are more relevant to our subject will be discussed in more detail.

A secure key exchange and management scheme for wireless body area networks using physiological signals is proposed in [13] and [14]. The proposed approach exploits the unique characteristics of ECG signals to manage and distribute the symmetric cryptographic keys in order to protect the user privacy.

In [9], the authors deal with collisions in vehicular networks by adopting a distributed MAC scheduler (DMS). The authors attempt to balance the channel load by introducing intentional deferrals while delivering messages. DMS actually increased reception rate and improved the channel load balancing.

V. K. Sharma et al. [21] proposed a cross-layer adaptive transmission method to deal with congestion in mobile ad-hoc networks (MANETs). The method estimates the experienced congestion level in a per-node fashion and classifies packet losses according to their original causes. The upper layer adapts packet generation rate according to the congestion-related information provided by the lower layers. Furthermore, congestion notifications are exclusively sent to the main congestion contributors to adapt their transmission rate. The proposed method outperformed other existing ones in terms of network performance.

In [23], the authors proposed a fuzzy based classification as energy aware routing policy in MANETs. Based on the classified energy level, the policy includes energy-rich nodes in the selected routes and maintains the local congestion intensity level. In reality, based on the results, the policy showed a lower number of dead nodes and longer network lifetime.

The same authors proposed a load distribution approach [22] to balance congestion in wireless ad-hoc routing protocols. They considered congestion estimation to assess the traffic status for the whole routing path and used the traffic load information to identify new available paths with the preferred load condition. In the case of no better new route, the nodes simply adapt congestion locally. Simulation results showed better network performance compared to other routing protocols.

A survey on the mobility management protocols in wireless sensor networks is produced in [4]. This work treated mobility aspects in the IEEE 802.15.4 with 6LoWPAN and provided a comparative study with classification.

In [20], the authors introduce an optimization model to ensure security and QoS while guaranteeing optimal usage of the available resources in transmitting data. The authors adopted multi-objective optimization and genetic algorithm to achieve their goal and the results prove the model efficiency in terms of security settings accuracy and computing delay.

The impact of MAC parameters such as packet size and packet arival rate on the slotted CSMA/CA of the beacon-enabled mode of IEEE 802.15.4 standard is studied in [15]. The slotted CSMA/CA regime is analytically modelled using discrete time Markov chains and M/G/1/K queueing system. The results demonstrated the effect of the packet arrival rate, network size and packet size on the access probability.

Attacks on integrity and availability were considered in [11]. The authors treated the case of insider attacks in IEEE 802.15.4 beacon-enabled mode by providing security protocol based on authentication methods.

H. Nguyen-Minh et al. [17] propose a jamming detection approach to detect reactive jamming targeting beacon frames in 802.11p vehicular networks. The detecting approach attempt to distinguish between packets lost due to a normal collision in multichannel operation and that caused by the jamming attack. Results revealed a high detection rate.

The most studied selective jamming attacks exclusively targeting IEEE 802.15.4 beacon-enabled mode are the so-called GTS attacks. GTS attacks can be classified based on the target selection criteria and the solutions are either centralized or distributed:

In [24], the authors identified a new attack that aims to corrupt GTS communication between devices and the network coordinator.

After achieving synchronization with the coordinator, by means of beacon frames reception, the attacker can intercept the GTS descriptor within the beacon frames to know exactly the start and length of a node GTS slot. The attacker will then direct a selective jamming attack to the picked slot in order to degrade the link quality. In this work, no selection criterion was defined for picking the target slot.

An extended work considering the number of attackers and node slot length as a selection criterion [25] was introduced by the same authors. They defined four possible scenarios: one intelligent attacker (OIA), one random attacker (ORA), two intelligent attackers (TIA) and two random attackers (TRA). In the intelligent cases, the attacker selects the longest node slot in CFP to jam. In the case of TIA, the two attackers collaborate to select the longest and second longest slots with the aim of decreasing network bandwidth utilization as much as possible. In the random cases, the attacker picks the slot randomly. There is no collaboration between attackers in TRA, and this leads to possible jamming overlap. The attacks were evaluated in terms of corrupted slots ratio and attacker energy consumption. As expected, intelligent attacks outperformed random ones in both metrics.

Even though the authors have defined a new attack with four different scenarios, the evaluation was poor and limited. For instance, the corrupted slot ratio for OIA was 50.48% which is far from a realistic scenario. In a real network with many nodes, the probability of a node being alone in CFP is very low. The reason behind the high

value above is progressive network joining, performed by nodes, and very short simulation time compared to the superframe duration. Another example, that depicts the results subjectivity, is that OIA outperformed TRA in both evaluation metrics. Theoretically, two random attackers will jam nearly double the average length of all slots. If the length of the longest slot in CFP is larger than double the average, which was the case in the evaluation inputs, TRA will barely keep up with OIA.

R. Daidone et al. [7] introduced a new GTS attack along with a selective jamming resistant GTS scheme (SJRG). By adopting node ID as a selection criterion, Sniper Attack, selectively, targets certain slots in CFP.

Aiming to decrease the harm of this attack and other GTS attacks, the authors suggested a new GTS allocation scheme, which was supposed to be resistant to such attacks. The main goal of SJRG is to distribute the damage experienced by a victim over all active nodes in CFP. To this end, SJRG forces the attacker to switch onto a random attack.

SJRG consists of two steps: (1) securing GTS allocation information in beacon frames; and (2) randomizing slot allocation by changing the order of slots in each superframe. The former step was realized by moving GTS-related information to the beacon payload to be encrypted and authenticated by IEEE 802.15.4 security services. The latter step is the core of SJRG that makes the attacker blind in their activity.

The work was evaluated in a real scenario using Tmote Sky motes. Considerations included packet delivery ratio, memory footprint, delay and per packet extra energy consumption. The packet delivery ratio in the presence of SJRG was close to the analytical one, and all other metric measurements were reasonable. The main drawback of this work was altering the GTS allocation and the security service functionalities. Furthermore, SJRG improves delivery ratio of the victim, but the number of attacked nodes per superframe will increase considerably. Actually, jamming duration can cover many parts of different slots due to the attacker's blindness.

JAMMY [27] is a distributed and dynamic solution for selective jamming attacks in TDMA-based WSNs.

In order to avoid continuous exposure to jamming signals, JAMMY uses the same principle as SJRG to alter the slots order, but this time, in a distributed fashion. Unlike SJRG, in which nodes rely on beacon information to know their slot order, nodes in JAMMY independently generate the same slot sequence in a consistent manner. The authors claimed that using a pseudo random sequence generator locally in each node, to know the next slot position, is more energy efficient than receiving it in each superframe.

Even though both centralized and distributed approaches provided equal corrupted packet ratios, the analytical evaluation of the centralized approach, in terms of energy consumption, revealed extra overhead.

JAMMY can be more energy efficient in TDMA case. However, in IEEE 802.15.4 GTS transmission scenario, beacon frames are transmitted in any case. Therefore, the communication overhead in the distributed approach will be the same as the centralized one. In fact, there will be an extra treatment overhead for each node in the distributed case. In addition, to generate the same sequence in all nodes, an initialization phase is required in order to exchange initial parameters. This can be vulnerable from a security point of view. Therefore, using JAMMY in a GTS allocation scheme is not only useless and energy inefficient, it is also more security threatening.

M. Tiloka et al. [26] introduced a distributed shuffling (DISH) against selective jamming attacks in IEEE 802.15.4e TSCH networks. The time slot channel hopping (TSCH) networks combine time slotted access of IEEE 802.15.4 with channel hopping capability. This combination provides large network capacity and ensures predictable latency. DISH changes the order of the slots and channel utilization in a random, distributed and per superframe manner. Quantitative analysis of DISH showed its effectiveness against selective jamming for different network configurations.

From the reviewed literature, we conclude that the main idea of the proposed solutions for TDMA-oriented jamming attacks is slot position randomization.

4 An overview of IEEE 802.15.4 beacon-enabled mode

IEEE 802.15.4 [1] serves low data rate, low cost and low power consumption wireless networks, known as wireless personal area networks. This standard defines PHY and MAC layers and relies on other technologies for upper layers.

IEEE 802.15.4 encompasses two modes: slotted and unslotted modes. The unslotted one is the so-called non beacon-enabled mode in which nodes perform an unslotted CSMA/CA to communicate in a distributed fashion. The beacon-enabled one is the slotted mode in which the time is divided to equally sized time slots. In this mode, all devices should follow one time superframe. The length of the superframe is called beacon interval (BI) and presents the time passed between two beacon frame transmissions. The personal area network (PAN) coordinator periodically sends beacon frames to synchronize with the associated devices and make new devices join the network.

The beacon interval includes an active and an optional inactive period. In the inactive period, all the devices including the coordinator enter into a low-power state to

save energy. In the active period, the device can enter an active state according to requirements and configuration. The length of the active period is called superframe duration (SD) and divided into 16 equally sized time slots.

There are two parts in the superframe duration: contention access period (CAP) and contention free period (CFP). The devices follow slotted CSMA/CA to gain access to the medium in CAP and pursue TDMA method with a maximum size of 7 slots in CFP. The CFP slots, also referred to as guaranteed time slots (GTS), could be reserved in a FCFS fashion by the devices which need a dedicated bandwidth.

Figure 1 shows an example of the superframe structure.

The superframe duration and the beacon interval in PAN are characterized by the superframe order (SO) and beacon order (BO) parameters, respectively. In essence, the pair (SO, BO) summarizes the timing characteristics of the superframe. Equations (1) and (2) depict the superframe duration and the beacon interval as a function of these parameters.

$$BI = aBaseSuperframeDuration \times 2^{BO} \quad (1)$$

$$SD = aBaseSuperframeDuration \times 2^{SO} \quad (2)$$

Where $0 \leq SO \leq BO \leq 14$.

aBaseSuperframeDuration corresponds to 960 symbols duration, which is 15.45 ms for the 2.4 GHz frequency band, which will be considered throughout this work.

5 Network model and analysis

To understand the logic behind the proposed attack and its associated countermeasure, a clear view of the network model and communication pattern is required.

In this work, we consider a wireless body area network, consisting of a set of sensor devices that periodically transmit their physiological measurements to a central entity called a coordinator. This network forms a star topology and uses IEEE 802.15.4 GTS scheme for packet delivery (Figure 2).

Let N be the number of nodes (devices) in the network. For a node i ($1 \leq i \leq N$), we note by D_i, P_i and S_i, the first packet arrival time, packet inter-departure period (the time between two successive packet arrivals) and node slot duration, respectively. Therefore, the first packet will be generated in the application layer at D_i, the second one at $D_i + P_i$ and the third one at $D_i + 2 \times P_i$, and so on. We refer to the beacon interval duration by SF notation.

Theoretically speaking, a node i will transmit its j^{th} frame at $D_i + (j - 1) \times P_i$. However, the real packet transmission time can be different due to the limiting IEEE 802.15.4 superframe structure. In fact, if a packet arrives at MAC layer when the device is out of its slot; the transmission will be deferred to the next arrival of the node's slot.

This introduced delay depends on three factors:

(1) The pair $(D_i \ mod_{float} \ SF, P_i \ mod_{float} \ SF)$
(2) Superframe timing characteristics (SO, BO)
(3) Length of the device slot in GTS slots

When mod_{float} is the last positive remainder after performing successive subtraction.

These delays are accompanied by a certain behavior that reveals a serious vulnerability in GTS transmission mode.

In next sections, we present our main contributions, namely, Slot-Head Jamming Attack (SHJA) and Random Packet Departure (RPD) and we will study the effect of the above factors throughout the paper.

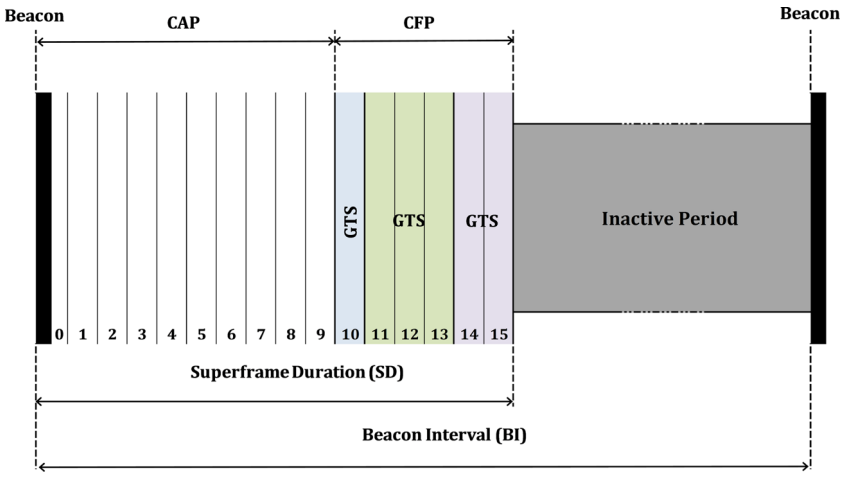


Fig. 1 An example of the superframe structure

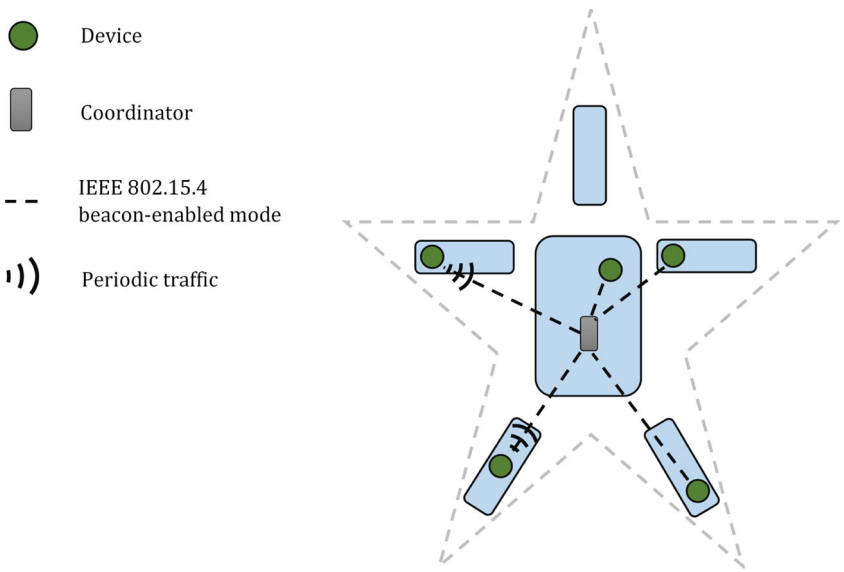


Fig. 2 Star-topology Wireless Body Area Network

6 Slot-Head Jamming attack (SHJA)

SHJA is an efficient version of a GTS attack that, given the classic version, achieves nearly the same harm with minimum attacking activity.

This attack relies on two basic aspects: an easily exploitable vulnerability in the core functionality of IEEE 802.15.4 GTS transmission mode, and the overlap of the superframe with the inter-departure time of a certain node.

Basically, IEEE 802.15.4 GTS mode has two effects on the carried periodic traffic:

(1) Superframe effect: the effect of the superframe structure on the packet inter-arrival pattern.
(2) Standard behavior effect: resulting from the behavior of the standard while transmitting the traffic affected by the superframe effect.

6.1 Guaranteed time slot (GTS) transmission vulnerability

The IEEE 802.15.4 MAC protocol sends a frame in the slot start, intentionally, in two cases: (we mean by intentionally, that the frame was not supposed to be sent in the slot start)

(1) Frame retransmission
(2) When a packet arrives before the device's slot starts

This behavior introduces a significant vulnerability for a selective jammer to exploit since the attacker will not be forced to jam the full slot to guarantee his attack success. It will be sufficient for the attacker to jam only the start of the slot.

Nevertheless, if the ratio of MAC deferred packets is low, this vulnerability will not present a considerable security threat. In the opposite case, this will give adversaries the chance to cause nearly as much harm as full-slot jamming with much less resource exhaustion.

Assuming that $P_i \ mod_{float} \ SF \neq 0$ (the other case will be discussed in the next subsection).

There are two cases:

– When $P_i mod_{float} SF > slot\_duration$:

Let t_j be the j^{th} packet arrival that has happened inside the slot, so:

$$\begin{aligned} t_{j+1} &= t_j + P_i \\ &= t_j + N \times SF + P_i mod_{float} SF \end{aligned}$$

Where $N = P_i div_{float} SF$.

It is clear that $t_j + N \times SF$ will arrive in the same position within the slot as t_j.

Since $slot\_duration < P_i mod_{float} SF < SF$, t_{j+1} will, certainly, arrive beyond the slot.

We conclude that whatever the packet arrival time is, if it happens inside the slot, the next arrival will take place outside the slot. This results in at least 50% of beyond-slot arrivals.

– When $P_i mod_{float} SF \leq slot\_duration$:

In this case, the number of beyond-slot arrivals is proportional to $\frac{SF - slot\_duration}{SF}$.

By taking the worst scenario (when SF takes its smallest value and $slot\_duration$ takes its largest value in terms of GTS slots number) this should be $\frac{16-7}{16} = 56.25\%$.

Even though we have considered the worst scenario for both cases, the number of beyond-slot arrivals is still high and takes at least half the traffic volume. Damaging this quantity of traffic is very harmful and it is not tolerated.

6.2 Slot-Head Jamming attack (SHJA) algorithm

By exploiting the vulnerability mentioned above, the adversary can corrupt the majority of specific node traffic.

In SHJA, the adversary repeatedly jams the victim's slot start and stop jamming in its remainder. This would buy the attacker extra resources to perform the attack for the longest period. Algorithm 1 shows how the jammer performs the attack.

Algorithm 1 Slot Head Jaming Attack

```
▷ Initialization phase
selectSlot()                          ▷ based on node ID or Slot size
waitUntil(slot_start)                 ▷ in current or next superframe
schedule (Timer, beacon_interval_duration) ▷ when the waiting ends
▷ Periodic jamming procedure
procedure FIRED (Timer)               ▷ executed when Timer expires
    schedule (Timer, beacon_interval_duration)
    wakeUp()
    jam_Slot_Head()
    sleep()
end procedure
```

The only way to avoid the jamming is by avoiding the transmission deferring itself. This can be achieved by making D_i happen within the slot, and choosing an inter-departure period that is a multiple of the beacon interval i.e. $(S_i\_start + N \times SF \leq D_i < S_i\_start + S_i + N \times SF)$ and $(P_i mod_{float} SF = 0)$, Where S_i_start is the difference between the start time of the slot and that of its enclosed superframe. However, by choosing D_i and P_i satisfying the aforementioned conditions, the attack will be even more successful and easier than the first time.

Since $P_i mod_{float} SF = 0$, the packet arrival will take the same position within the slot all the time. Hence, the adversary can achieve 100% corruption ratio by jamming the same slot portion repeatedly.

We note that SHJA do not take any selection criteria to pick its target. SHJA, in fact, is a general improved version of GTS attacks. In this regard, we introduce three new versions of GTS jamming attack, namely, Slot-Head Jamming Intelligent Attack (SHJIA), Slot-Head Jamming Random Attack (SHJRA) and Slot-Head Jamming Sniper Attack (SHJSA). Figure 3 illustrates these new attacks in the whole context.

6.3 Exploiting the deterministic transmission pattern to increase SHJA efficiency

SHJA exploits the standard behavior in the case of beyond-slot arrival to decrease the jamming duration. However, the deterministic transmission pattern imposed by the superframe structure is not yet exploited since the attack has to be performed in each superframe.

An attacker can benefit from some mathematical properties to avoid continuous jamming and perform the attack in a limited number of superframes.

Since the transmissions are performed exclusively in the node slot, the attacker can exploit the characteristics of the number of superframes separating two successive transmissions in order to perform more sophisticated attacks.

For instance, one can prove that this number takes only two values: $P_i div_{float} SF$ and $P_i div_{float} SF + 1$ (see the Appendix). Therefore, by tracking any two successive transmissions we can get a bounding of $P_i div_{float} SF$ value.

Let N be the number of superframes separating two successive transmissions and N_i the number of superframes corresponding to the i_{th} packet arrival ($N_0 = N$).

Based on the two values that N can take, N_1 value is either $N_0 + N - 1$, $N_0 + N$ or $N_0 + N + 1$ and N_2 can take the values $N_1 + N - 1$, $N_1 + N$ or $N_1 + N + 1$ and so on. Therefore, N_1 will take $2 \times N - 1$, $2 \times N$ or $2 \times N + 1$ and N_2 takes $3 \times N - 2$, $3 \times N - 1$, $3 \times N$, $3 \times N + 1$ or $3 \times N + 2$.

The generalized formula of the possible values that N_i can take is of the form:

$$N_i = (i + 1) \times N - i + k \tag{3}$$

Where $0 \leq k \leq 2i$.

After finding N by eavesdropping on the medium, an attacker can jam all the superframes of order $(i + 1) \times N - i + k$ to guarantee 100% corruption until the attack transforms to a continuous one (the number of jammed superframes covers N). Then the attacker should track only one transmission to repeat the procedure since we already have N. Algorithm 2 depicts the attack procedure.

Algorithm 2 Optimized Slot-Head Jamming attack

```
find (N)                              ▷ two successive packet arrivals
i ← 0
while 2 * i ≤ N do                    ▷ we have not achieved full-slot jamming yet
    jamPacketsOfOrder( (i + 1) × N − i + k )   ∀k ≤ 2 * i
    i++
end while
listenOnePacket()
goto(2:)
```

Algorithm 2 exploits a simple mathematical property to optimize the resources expenditure while performing the attack efficiently. An attacker can exploit other

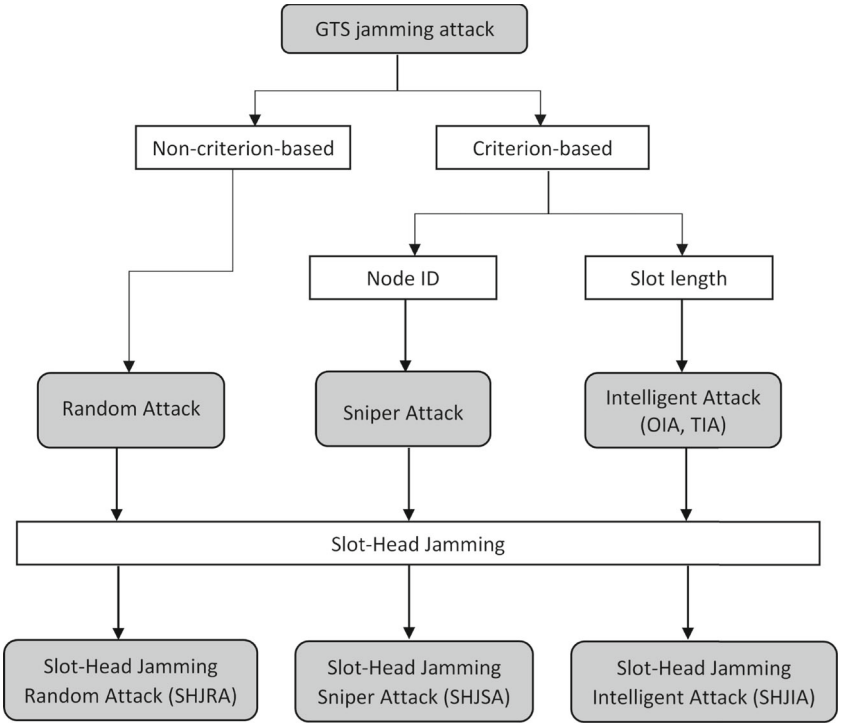


Fig. 3 New versions of GTS jamming attacks

complex properties to produce even more economic attacks. For instance, the number of superframes between two successive transmissions follows a well-defined sequence in which one of the possible values, $P_i div_{float} SF$ or $P_i div_{float} SF + 1$, cannot arrive two successive times. Therefore, N_i has fewer possibilities to take, which is going to affect the number of jamming packets.

An entirely different approach is tracking N_i values until we are sure that we have a repeated pattern. The attacker, then, can corrupt the entire traffic without any further eavesdropping. However, it is difficult to determine whether we have achieved a closed pattern. Furthermore, the tracking procedure can take a long time due to the odd relation between SF and P_i.

The main drawback of communication tracking algorithms is the need to be inside the communication range of both the network coordinator and the victim. In contrast, in continuous jamming, the attacker has only to be in the coordinator range, which is relatively large compared to the intersection of the two ranges. Figure 4 shows the attacker's possible locations in continuous and optimized jamming.

Figure 4 shows that improving the attack efficiency costs the attacker some of his/her location flexibility.

We note that previous works have simulated full-slot jamming by (1) sending a packet in the victim's slot head; (2) making the first packet time coincident with beacon arrival time; and (3) choosing an interdeparture period equal to the beacon interval.

By doing so, they guaranteed full-slot jamming without using an extra-large packet. Therefore, their action is done as part of facilitating performance evaluation and not as the attacking technique as we did. This explains why they take the configuration $D_i mod_{float} SF = 0$ and $P_i mod_{float} SF = 0$ in the evaluation procedure. It is important to distinguish between the first case, which is a facilitative act, and the second case, which is an intentionally proposed technique in which we have also considered the odd relation between P_i and SF.

In the next section, we present our countermeasure that mitigates SHJA harm to $\frac{jamming\_duration}{slot\_duration}$, theoretically.

7 Random Packet Departure (RPD)

The intentional slot-start transmission takes place in two cases: retransmission and beyond-slot arrival. Hence, to avoid SHJA shots, a device can track the occurrence of these two events with the aim of sending the packet at a different moment within the slot.

A node i can continuously perform a simple comparison between the next P_i arrival (of the form $D_i + N \times P_i$) and the slot start/end in the current superframe to assess whether or not it takes place inside the slot.

Let M and N be the counters of the superframe and P_i arrivals, respectively, and Delay be a random amount of time:

– If $D_i + N \times P_i \leq S_i\_start + M \times SF$ then the packet will be transmitted at $S_i\_start + M \times SF + Delay$

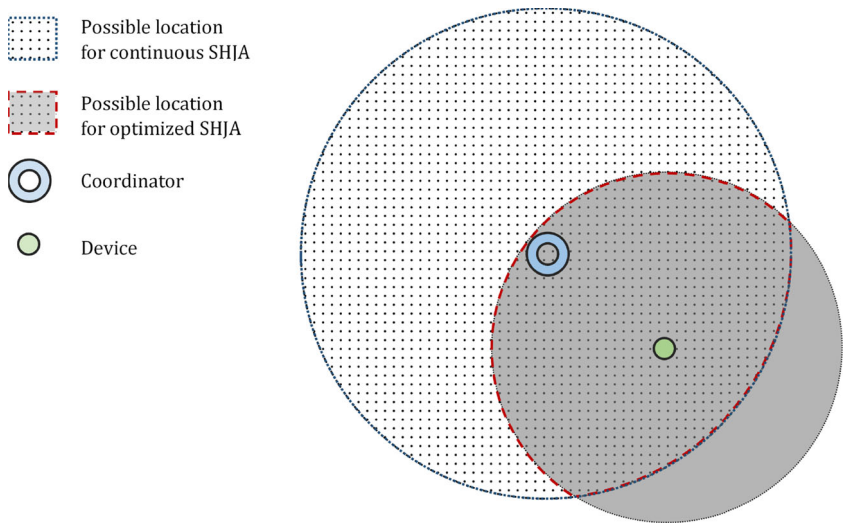


Fig. 4 Possible attacker locations for continuous and optimized SHJA

– If $D_i + N \times P_i > S_i\_start + S_i + M \times SF$ then the packet will be transmitted at $S_i\_start + (M + 1) \times SF + Delay$

We can make the procedure simpler by randomizing all packet departures whether they were deferred, retransmitted or otherwise.

RPD can be implemented in application layer or directly integrated in MAC layer functionalities. This flexibility makes RPD a very practical solution.

Algorithm 3 summarizes the RPD packet transmission procedure in the case of application implementation.

In this algorithm, $packet\_transm\_dur$ is the sufficient time to send all bits in a packet along with its associated ACK including all the IFS material.

Algorithm 3 Random Packet Departure (Application layer)

```
1: if fired (interDepartureTimer) then ▷ transmission time arrival
2:     T ← current_time()
3:     generate (random_time)
4:     ▷ random_time < slot_dur − pack_transm_dur
5:     if T < slot_start_current_SF then
6:         waitUntil(slot_start_current_SF + random_time)
7:     end if
8:     if T > slot_end_current_SF−packet_transm_dur then
9:         waitUntil(slot_start_next_SF + random_time)
10:    end if
11:    sendPacketToLowerLayer() ▷ when the waiting is finished
12: end if
```

In this case, the application layer should emulate the MAC layer superframe in order to know whether it should immediately send down the packet (we are in the middle of our slot) or keep it until the next slot (deferred packet). In the latter case, it waits for an additional random time before it sends the packet down. Along with that, the application layer should know what it takes, for a packet, to reach the physical layer. This small amount of time is of the utmost importance. It encompasses inter-layer propagation time and the headers construction time in all intermediate layers. Ignoring this amount of time while calculating the departure time in the application layer, may cause beyond-slot arrival in MAC layer. This leads the latter to defer the transmission again to the next superframe. However, this time the transmission will take place in the slot start since MAC layer is not aware of the RPD protocol.

The second problem with application-layer RPD is retransmitted packets. To allow RPD to randomize packet retransmissions, a cross-layer approach has to be enabled. In this regard, MAC layer retransmission has to be deactivated and a retransmission triggering process should be emulated by the application layer. These details are not considered in Algorithm 3.

We can avoid all these issues by integrating RPD directly in the MAC layer (Algorithm 4). The RPD procedure is much simpler in this case since RPD has a fine grained synchronization with the MAC layer. Furthermore, the information that determines whether a packet should be submitted to RPD or not is already available.

The only issue with that is altering the standard functionality. We believe that RPD does not bring a huge alteration to the standard and that it is affordable.

Algorithm 4 Random Packet Departure (MAC layer)

```
1: if fired (slotStartTimer) then ▷ my slot has just started
2:     T ← current_time()
3:     finished ← false
4:     while NOT finished do ▷ RPD task has not finished yet
5:         packet ← head(MAC_QUEUE)
6:         if packet ≠ NULL then
7:             if retransmitted(packet) OR ArrivalTime(packet) < T then
8:                 generate (random_time)
9:                 waitUntil(T + random_time)
10:            end if
11:            wakeUp()
12:            sendPacketToLowerLayer()
13:            sleep() ▷ when the transmission finishes
14:            finished ← true
15:        end if
16:        if fired (slotEndTimer) then ▷ the slot end
17:            finished ← true
18:        end if
19:    end while
20: end if
```

8 Performance evaluation

In this section, we evaluate our work by taking different metrics into consideration. To this end, we have considered different simulation scenarios, and results were consistent with our analytical predictions.

8.1 Simulation setup

We have simulated SHJA and RPD in IEEE 802.15.4 implementation [5], which is included in INETMANET 2.0 [1] framework. This implementation supports beacon-enabled mode with full GTS functionality. We have imported the above framework into OMNet++ [2] to proceed with our simulations.

We consider seven nodes that, along with a coordinator, form a star topology. Each node in the network occupies one slot of the seven GTS slots. Table 1 depicts the parameters chosen for all simulations.

We have considered four evaluation metrics:

- **Packet Corruption Ratio:** is the number of corrupted packets relative to the total number of transmitted packets.

[1] http://github.com/aarizaq/inetmanet-2.0

[2] https://www.omnetpp.org

Table 1 Simulation parameters

Parameter	Value
Node packet size	121 B (maximum allowed size)
Residual capacity for energy evaluation (ordinary nodes)	capacity= 25 mAh
Simulation time limit	100 h (for each simulation)
Radio transmission band	2.4 GHz (250 kbps data rate)

- **Packet Delivery Ratio (PDR):** is the number of successful transmissions relative to the total number of packets.
- **Delay:** is the difference between the time when a packet actually leaves the MAC layer and its supposed leaving time.
- **Per packet energy consumption:** the average consumption of energy for all successful packet transmissions obtained by dividing the full battery capacity by the number of successfully transmitted packets during the whole node life.

Since the superframe is characterized by its size on the one hand and by the active-inactive ratio on the other hand, we considered BO and $BO - SO$ as variable parameters during the evaluation. We used these two parameters to assess the effect of the superframe structure on the results.

We assume that the nodes schedule periodic transmission timer immediately after being assigned a slot from the coordinator. The slot assignment happens upon receiving the second beacon after an association request is sent from a node to the coordinator.

Since only $P_i mod_{float} SF$ affects the packet arrival position within the superframe, we chose P_i where $P_i div_{float} SF = 1$. This ensures that P_i turns enough times during the simulation, making the results more consistent.

For each pair (SO, BO), we took all possible values that $P_i mod_{float} SF$ can take while considering seconds as a time unit and $P_i div_{float} SF = 1$. For instance, for the pair (7, 8), the beacon interval duration (SF) is 3.93216 s. Therefore, all possible values that P_i can take are 4, 5, 6 and 7 s.

8.2 Results analysis

In the simulations, the attacker is one of the associated nodes and performs the attack by sending a packet into the victim's slot head in each superframe.

8.2.1 Slot-Head Jamming Attack

To evaluate the damage that SHJA may inflict on the network, we performed an extensive sequence of simulations of 100 hours long, in which we considered all

possible values of (SO, BO). For each instance pair, we covered the whole set of values that $P_i mod_{float} SF$ can take considering seconds as a time unit. The results were then averaged over each set.

Figure 5 shows the effect of the superframe structure on the averaged packet delivery ratio in the presence of SHJA.

Since we have considered seconds as a time unit, we had to eliminate all the pairs (SO, BO) that resulted in a period P shorter than 1 s. Therefore, the value of BO had to be at least 6.

To show the efficiency of SHJA, we had to take the smallest fraction $\frac{jamming\_duration}{slot\_duration}$ while taking as many SO values as possible. However, since MAC and PHY header size is fixed, we had to skip the short slot durations that do not conserve this fraction. The smallest conservable fraction that gives the largest number of SO values is $\frac{1}{30}$. Therefore, SO cannot be lower than 5.

It is important to mention that the IEEE 802.15.4 implementation is not tested in the case $SO = BO$, so we have not considered this case in the simulations.

From Figure 5, we can see that SHJA achieved at least 97% corruption by performing only 3.33% of full-slot jamming. Therefore, there was a significant difference in terms of efficiency compared to the classic jamming. This efficiency is given by the fact that most of the traffic was delivered in the target slot head.

In general, we notice that the packet delivery ratio average decreases as BO and $BO - SO$ increase in both curves. This is obvious in the case of $BO - SO$ since there is a reverse relationship between $BO - SO$ and $\frac{slot\_duration}{SF}$. In fact, when $BO - SO$ increases ($\frac{slot\_duration}{SF}$ decreases), the probability of beyond-slot arrival would increase.

In the case of BO variation, the decrease of PDR is due to the effect of averaging over all SO values corresponding to each BO. For instance, when $BO = 14$, there are nine SO values to average with. In contrast, there are only two values in the case $BO = 7$.

Figure 6 depicts the performance of the optimized SHJA summarized in Algorithm 2 compared to a continuous SHJA. The results were averaged over the set of $(7, 8)$ instance pair.

From the figure, we notice that as $P_i div_{float} SF$ increases, packet corruption ratio of the optimized SHJA approaches that of the continuous attack whereas the ratio of jamming packets decreases. It follows that exploiting a simple mathematical property has saved half the attacker's resources.

As $P_i div_{float} SF$ increases, the ratio $\frac{listened\_packets\_number}{jamming\_packets\_number}$ and the interference between the listening/jamming phases decrease. This would increase packet corruption ratio on the one hand and decrease the number of jamming packets on the other hand.

8.2.2 Random packet departure

To assess the performance of our solution in different network configurations, we evaluated packet delivery ratio in the presence and absence of RPD. We used a uniform distribution to generate the random delays added by RPD and we changed the seed of the generator in a per pair manner to make RPD behave differently each time.

According to Figure 7, we see that RPD has significantly improved the network throughput. In fact, on average, RPD augmented the PDR from 1% to 96%, changing the state of the link from paralyzed to active.

The figure reveals that the packet delivery ratio was almost constant and close to $\frac{slot\_duration - jamming\_duration}{slot\_duration}$. This is due to the large number of beyond-slot packet arrivals.

We chose a uniform distribution rather than an average-based one in order to avoid the situation when the attacker focuses the attacks on the average proximity.

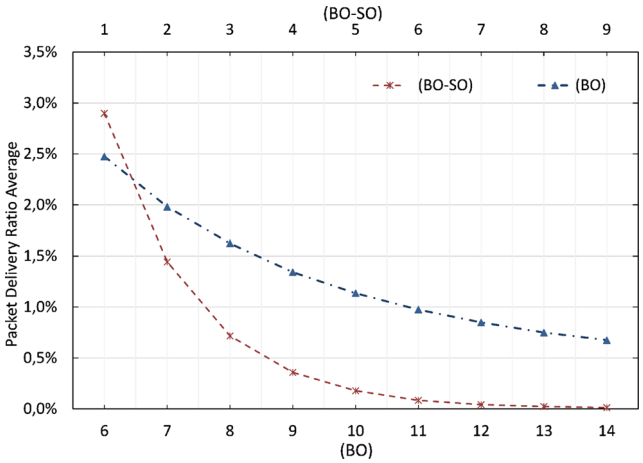


Fig. 5 Slot-Head Jamming vs. Full-Slot Jamming

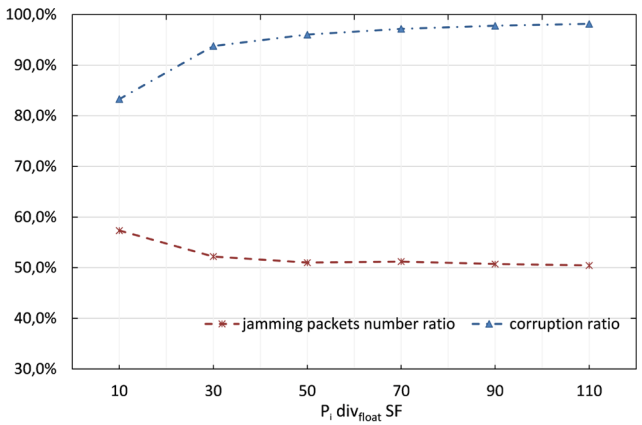


Fig. 6 Optimized jamming vs continuous jamming

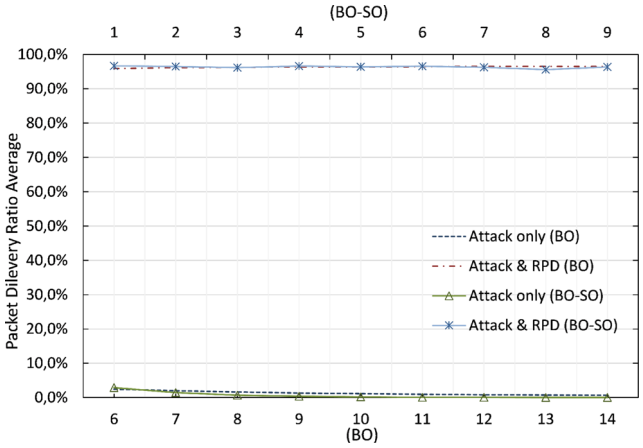


Fig. 7 Random Packet Departure evaluation

Since our protocol introduces an extra delay overhead, we investigated delivery times in both cases: when RPD is enabled and when only the IEEE 802.15.4 superframe structure is followed.

IEEE 802.15.4 GTS mode sends the packets deferred by the superframe in the slot start. Therefore, any packet deferred by the superframe structure will also imply a RPD deferral. Therefore, RPD delay is going to include the delay resulting from the effect of the superframe structure. Figure 8 shows changes in the average of the ratio $\frac{RPD\_delay}{superframe\_delay}$ in different superframe configurations.

As we can see, RPD has added a negligible delay to the previous relatively large one. In fact, we had to consider the ratio to avoid overlap in the curves caused by convergence of the results.

The same factors influencing packet delivery ratio in SHJA evaluation affect the delay ratio as BO and $BO - SO$ increase. In General, we think that this delay overhead is affordable, especially when P takes large values compared to the beacon interval duration.

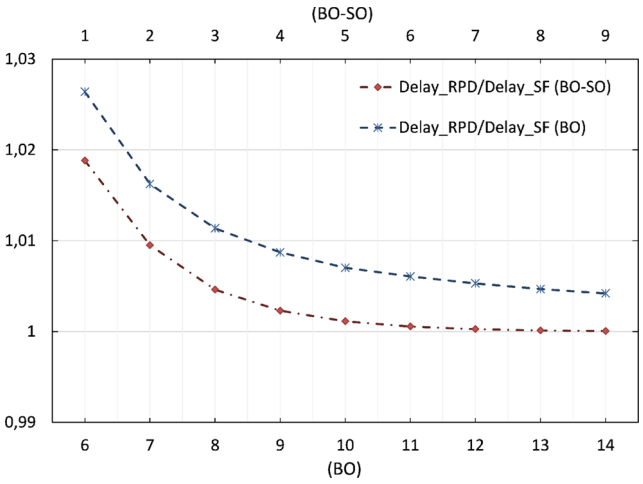


Fig. 8 RPD delay evaluation

Variation of per packet energy consumption as a function of jamming duration for the pair instance $(7, 8)$ is shown in Figure 9. We have considered three cases: no attack, presence of an attack and RPD scenario (the 'attack only' curve is presented on the left axis and the two others on the right one). This time we pursued the simulation until the victim battery ran out.

Considering the energy consumption in the case of 'no attack' as an evaluation metric, on average, a packet in RPD scenario corresponds to 4.3 'no attack' packets. In contrast, the packet in the 'attack only' case corresponds to 137.7 packets. Therefore, the difference between the case of 'no attack' and the RPD scenario was negligible compared to the high values recorded in the 'attack only' case.

In order to clearly show the damage resulting from SHJA and the network throughput that RPD can recover, we compared our work with random slot allocation, proposed in [7] and adopted by [27] and [26]. The authors claimed that the attacker likely relies on simple sensor nodes and aims to conserve energy by attacking only one node slot.

By assuming the same limitations on the attacker, we performed slot-head jamming and jammed all GTS slots, each by a seventh of the total jamming duration ($\frac{1}{7}$ slot duration). Figure 10 shows the packet delivery ratio average in random GTS allocation (RGTS) and RPD for one node from the network. The PDR is averaged over the period set of the pair instance $(7, 8)$.

From Figure 10, we note that the attack caused an extensive damage to the whole traffic even though it spent the same resources as classic sniper attack. However, in this case, random GTS allocation was useless. Since all the slots will be jammed by $\frac{1}{7}$ slot duration, changing the slots order cannot help with avoiding the attack.

The point behind performing this simulation, even though random GTS allocation is not designed to address such attacks, is to show that there is a way for the attacker to proceed with the attack and avoid RGTS, again without consuming extra resources.

It should be noted that SHJA did not only make the random GTS exert no effect, it also paralyzed the entire network traffic, contrary to sniper attack that targets only one node.

From the simulations performed in this work, we can see that the main factors affecting the communication pattern of IEEE 802.15.4 in the case of periodic traffic is the superframe structure and the standard transmission policy.

After considering almost all network configurations along with all possible discrete values of the inter-departure period, we can see that a huge part from the traffic is delivered in the node's slot head. This is what made SHJA very destructive to the communicated information.

By performing only 3.33% of full-slot jamming, SHJA achieved from 99% to 97% corruption according to

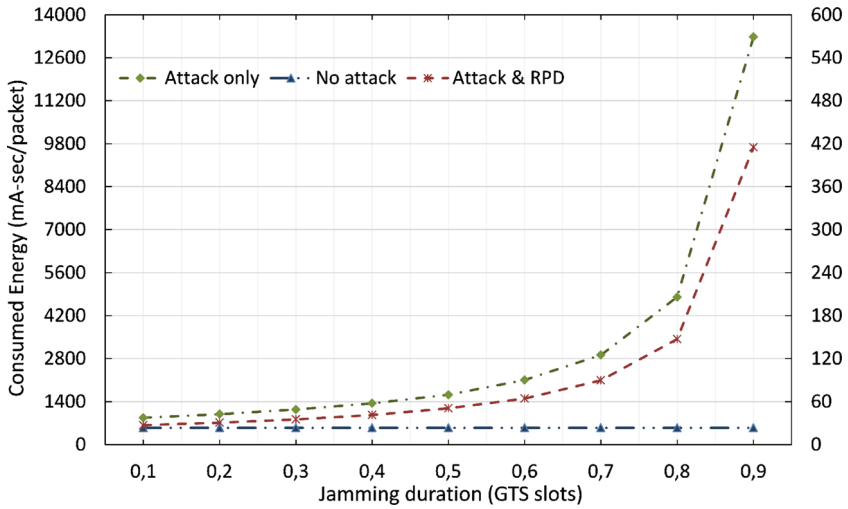


Fig. 9 Energy consumption evaluation

the network configuration. Therefore, the effect of the superframe on SHJA is negligible, which necessitates, in our opinion, reconsideration of some of the standard functionalities. The situation can be worse if the attacker tends to limit his or her attack to the superframe which will most likely have incoming communication.

One possible solution for SHJA is randomizing packet departure within the slot. By doing so, RPD could decrease the corruption of SHJA down to 4.3% according to our simulation inputs.

Additionally, the results show that the superframe alters the timing pattern of the communication to the extent that the delay introduced by RPD was negligible. Notably, the latter presents at most 3% of the superframe delay.

The energy evaluation shows that packet departure randomization improves the energy efficiency of the victim, which results in longer network lifetime. In fact, RPD saves the nodes from battery drain caused by frame retransmissions on the one hand and ensures maximum network availability by saving most of the targeted traffic on the other hand.

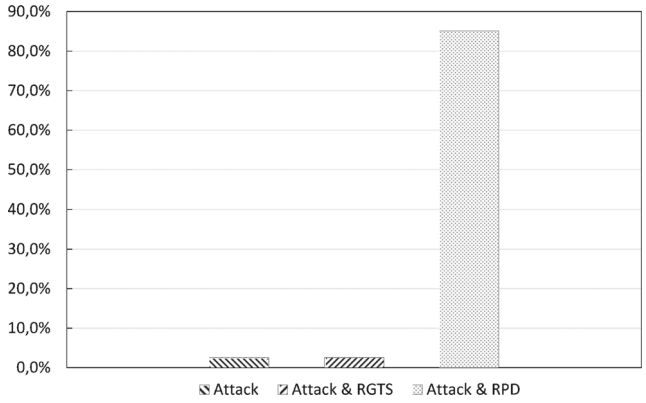


Fig. 10 Packet Delivery Ratio of RPD and RGTS

9 Conclusion

In this paper, we introduced a new GTS attack version along with a mitigating countermeasure. The target application is the periodic traffic in IEEE 802.15.4-based wireless body area networks.

From the simulations that were carried out, we conclude that selective jamming attacks can be easily performed without spending much resources. This ease is given by the fact that the superframe structure alters, in a deterministic way, the transmission pattern of the enabling node.

SHJA can take down the whole network expending only what a classic GTS attack needs to target a single node from the network.

RPD can reduce the damage caused by SHJA to $\frac{jamming\_duration}{slot\_duration}$ without introducing a big delay overhead.

In further work, we intend to improve SHJA to be more economic by adopting more sophisticated algorithms to track the target communication scheme. The next stage of our work can possibly be an intrusion detection system that exploits the deterministic alteration in GTS mode to detect anomalies in the device's behavior.

Appendix

Considering the two boundaries of an arbitrary turn of the period P, we define three parts constituting this turn;

(1) The difference between the start of the node slot that follows the first boundary and the boundary itself. We refer to this period as the $head$.
(2) The period between the first and last slot start located in the turn. We refer to this period as the $body$.
(3) The difference between the second boundary and the last slot start located in the turn. We refer to this period as the $tail$.

We refer to the period between the first boundary and the start of the node slot that precedes this boundary as the $shift$.

Figure 11 illustrates these three parts.

Let N be the number of superframes between two successive transmissions affected by the IEEE 802.15.4 MAC layer and let $slot$ and SF be the slot duration and full superframe duration, respectively.

The goal of the Appendix is proving the following:

$$Pdiv_{float}SF \leq N \leq Pdiv_{float}SF + 1$$

Firstly, we have:

$$N = pre\_delaying + |body| + post\_delaying$$

Where:

- $pre\_delaying$ is a number determining whether there is a delay in the beginning of the turn. This variable takes 0 in the case of delay and 1 otherwise.
- $|body|$ is the number of superframes in $body$.
- $post\_delaying$ is the number of deferrals caused by the $tail$.

- Assuming that $shift = 0$:
  In this case, it is obvious that $head = 0$, $body = (Pdiv_{float}SF) \times SF$ and $tail = Pmod_{float}SF$.
  Thus, $pre\_delaying = 0$ and $|body| = Pdiv_{float}SF$.
  Since $Pmod_{float}SF < SF$, then the second packet arrival can at most be delayed once. Then $post\_delaying \leq 1$.
  As a result: $Pdiv_{float}SF \leq N \leq Pdiv_{float}SF + 1$.
- Assuming that $shift \neq 0$:
  We have

$$\begin{aligned} body &= P - (SF - shift) - (Pmod_{float}SF + shift) \\ &= P - SF + shift - Pmod_{float}SF - shift \\ &= P - SF - Pmod_{float}SF \end{aligned}$$

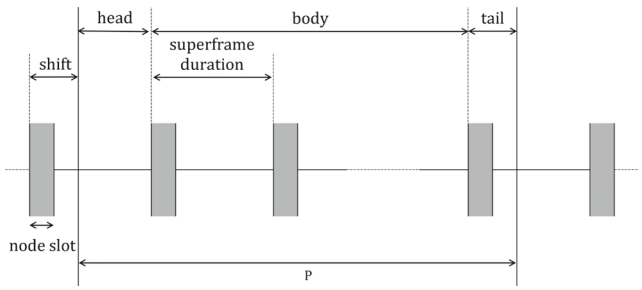


Fig. 11 An arbitrary turn of P with the introduced three parts: head, body and tail

Since $P = (Pdiv_{float}SF) \times SF + Pmod_{float}SF$,then,

$$\begin{aligned} body &= (Pdiv_{float}SF) \times SF + Pmod_{float}SF - SF \\ &\quad - Pmod_{float}SF \\ &= (Pdiv_{float}SF) \times SF - SF \\ body &= (Pdiv_{float}SF - 1) \times SF \end{aligned}$$

Therefore,

$|body| = Pdiv_{float}SF - 1$

Since $|body|$ is constant, finding a boundary for N implies finding a boundary for $pre\_delaying$ and $post\_delaying$.

Since $shift + head = SF$ then $0 \leq shift \leq SF$.

Consequently, we have two possibilities:

$0 \leq shift < slot$ and $slot \leq shift \leq SF$, which implies $pre\_delaying = 1$ and $pre\_delaying = 0$, respectively.

Thus

$$0 \leq pre\_delaying \leq 1$$

On the other hand, we have:

$$Pmod_{float}SF < SF \text{ and } shift < SF$$

Then

$$Pmod_{float}SF + shift < 2 \times SF$$

Therefore

$$tail < 2 \times SF$$

As a consequence, we have three possibilities:

$0 \leq tail < slot$, $slot \leq tail < SF + slot$ and $SF + slot \leq tail < 2 \times SF$, which implies $post\_delaying = 0$, $post\_delaying = 1$ and $post\_delaying = 2$.

Thus

$$0 \leq post\_delaying \leq 2$$

Therefore

$$\begin{aligned} Pdiv_{float}SF - 1 &\leq pre\_delaying + |body| \\ &\quad + post\_delaying \\ &\leq Pdiv_{float}SF + 2 \end{aligned}$$

Now, we have to prove that this sum cannot take the inequality boundaries i.e., $Pdiv_{float}SF - 1$ and $Pdiv_{float}SF + 2$.

Since $pre\_delaying$ has 0 and 1 as possible values and $post\_delaying$ can take the values 0, 1 and 2, it is sufficient to prove that $pre\_delaying$ inevitably takes 0 when $post\_delaying$ takes 2 and takes 1 when $post\_delaying$ takes 0.

- Suppose that $post\_delaying = 2$:
  This implies

$$tail \geq SF + slot$$

Which is equivalent to:

$$Pmod_{float}SF + shift \geq SF + slot$$

Thus

$$shift \geq SF + slot - Pmod_{float}SF$$

Since

$$Pmod_{float}SF < SF$$

Then

$$shift > slot$$

Therefore, the first transmission is undeniably deferred, which means $pre\_delaying = 0$.

- $post\_delaying = 0$

This means

$$tail < slot$$

i.e.

$$Pmod_{float}SF + shift < slot$$

Then

$$shift < slot$$

Therefore, the first transmission is not deferred, which means $pre\_delaying = 1$.

This results on:

$$\begin{aligned} Pdiv_{float}SF &\leq pre\_delaying + |body| \\ &\quad + post\_delaying \\ &\leq Pdiv_{float}SF + 1 \end{aligned}$$

i.e. $Pdiv_{float}SF \leq N \leq Pdiv_{float}SF + 1$

References

1. IEEE 802.15 WG (2006) IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs). IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp 1–320. https://doi.org/10.1109/IEEESTD.2006.232110
2. Achour M, Mana M, Rachedi A (2018) New Slot-Head jamming attack and mitigation mechanism for wireless body area networks. In: 2018 IEEE Global communications conference: ad hoc and sensor networks (globecom2018 AHSN). Abu Dhabi, United Arab Emirates
3. Al Masud SMR (2013) Study and analysis of scientific scopes, issues and challenges towards developing a righteous wireless body area network. Int J Soft Comput Eng (IJSCE) 3(2):243–251
4. Bouaziz M, Rachedi A (2016) A survey on mobility management protocols in wireless sensor networks based on 6lowpan technology. Comput. Commun 74(C):3–15. https://doi.org/10.1016/j.comcom.2014.10.004
5. Chen F, Dressler F (2007) A simulation model of ieee 802.15. 4 in omnet++. Proc. of the 6th GI/ITG KuVS Fachgesprach Drahtlose Sensornetze (FGSN), pp 35–38
6. Chen M, Gonzalez S, Vasilakos A, Cao H, Leung VC (2011) Body area networks: A survey. Mob. Netw. Appl 16(2):171–193. https://doi.org/10.1007/s11036-010-0260-8
7. Daidone R, Dini G, Tiloca M (2014) A solution to the gts-based selective jamming attack on ieee 802.15.4 networks. Wirel. Netw 20(5):1223–1235. https://doi.org/10.1007/s11276-013-0673-y
8. Dishman E (2004) Inventing wellness systems for aging in place. Computer 37(5):34–41. https://doi.org/10.1109/MC.2004.1297237,
9. Haddadou N, Rachedi A, Ghamri-Doudane Y (2016) To send or to defer? improving the ieee 802.11p/1609.4 transmission scheme. Ad Hoc Netw 48:53–65
10. Istepanian R, Laxminarayan S, Pattichis CS (2007) M-health: emerging mobile health systems springer science & business media
11. Jung SS, Valero M, Bourgeois A, Beyah R (2015) Attacking and securing beacon-enabled 802.15.4 networks. Wireless Networks 21(5):1517–1535. https://doi.org/10.1007/s11276-014-0855-2
12. Latré B, Braem B, Moerman I, Blondia C, Demeester P (2011) A survey on wireless body area networks. Wirel. Netw 17(1):1–18. https://doi.org/10.1007/s11276-010-0252-4
13. Mana M, Feham M, Bensaber BA (2009) Sekeban (secure and efficient key exchange for wireless body area network)
14. Mana M, Feham M, Bensaber BA (2011) Trust key management scheme for wireless body area networks. I. J. Network Security 12:75–83
15. Mišić J, Shafi S, Mišić VB (2005) The impact of mac parameters on the performance of 802.15. 4 pan. Ad Hoc Networks 3(5):509–528
16. Movassaghi S, Abolhasan M, Lipman J, Smith D, Jamalipour A (2014) Wireless body area networks: a survey. IEEE Communications Surveys Tutorials 16(3):1658–1686. 10.1109/SURV.2013.121313.00064
17. Nguyen-Minh H, Benslimane A, Rachedi A (2015) Jamming detection on 802.11p under multi-channel operation in vehicular networks. In: 2015 IEEE 11Th international conference on wireless and mobile computing, networking and communications (wimob), pp. 764–770, https://doi.org/10.1109/WiMOB.2015.7348039
18. Otto C, Milenković A, Sanders C, Jovanov E (2005) System architecture of a wireless body area sensor network for ubiquitous health monitoring. J. Mob. Multimed 1(4):307–326. http://dl.acm.org/citation.cfm?id=2010498.2010502
19. Proano A, Lazos L (2012) Packet-hiding methods for preventing selective jamming attacks. IEEE Transactions on Dependable and Secure Computing 9(1):101–114. https://doi.org/10.1109/TDSC.2011.41
20. Rachedi A, Benslimane A (2016) Multi-objective optimization for security and qos adaptation in wireless sensor networks. In: 2016 IEEE International conference on communications (ICC), pp. 1–7, https://doi.org/10.1109/ICC.2016.7510879
21. Sharma VK, Kumar M (2017) Adaptive congestion control scheme in mobile ad-hoc networks. Peer-to-Peer Networking and Applications 10(3):633–657
22. Sharma VK, Kumar M (2019) Adaptive load distribution approach based on congestion control scheme in ad-hoc networks. Int J Electron 106(1):48–68
23. Sharma VK, Verma LP, Kumar M (2018) A fuzzy-based adaptive energy efficient load distribution scheme in ad-hoc networks. International Journal of Intelligent Systems and Applications 11(2):72
24. Sokullu R, Dagdeviren O, Korkmaz I (2008) On the ieee 802.15.4 mac layer attacks: Gts attack. In: 2008

Second international conference on sensor technologies and applications (sensorcomm 2008), pp. 673–678, https://doi.org/10.1109/SENSORCOMM.2008.75
25. Sokullu R, Korkmaz I, Dagdeviren O (2009) Gts attack:, An ieee 802.15. 4 mac layer attack in wireless sensor networks. International Journal On Advances in Internet Technologies 2(1):104–114
26. Tiloca M, De Guglielmo D, Dini G, Anastasi G, Das SK (2018) Dish: Distributed shuffling against selective jamming attack in ieee 802.15. 4e tsch networks ACM transactions on sensor networks
27. Tiloca M, Guglielmo DD, Dini G, Anastasi G, Das SK (2017) Jammy: a distributed and dynamic solution to selective jamming attack in tdma wsns. IEEE Transactions on Dependable and Secure Computing 14(4):392–405. https://doi.org/10.1109/TDSC.2015.2467391

M'hammed Achour is currently a Ph.D. student at the Department of Computer Science, University of Abou Bekr Belkaid, Tlemcen, Algeria. He received his B.Sc in computer science and his M.Sc. in networks and distributed systems from the University of Amar Telidji, Laghouat (Algeria) in 2013 and 2015, respectively. His research interest lie in wireless technologies, distributed systems and intrusion prevention/detection.

Mohammed MANA is an associate professor at the University of Abou Bekr Belkaid and a member of STIC Laboratory in Tlemcen, Algeria. He received his PhD degree in telecommunications at the University of Tlemcen in 2012. He obtained his engineer degrees in computer science and his M.S. degree in networks and telecommunication systems from the same University in 2003 and 2007, respectively. His research interests cover wireless networking, ad hoc networks management, distributed systems, bioinformatics, security and privacy.

Abderrezak Rachedi is currently working as full professor at the University Paris-Est Marne-la-Vall?e (UPEM) and a member of the Gaspard Monge Computer Science laboratory (LIGM CNRS UMR 8049) since september 2008. He received his Habilitation to Direct Researsh (HDR: habilitation ? Diriger des Recherches) from Paris-Est University in Dec. 2015, and his PhD degree in computer science from the university of Avignon (France) in 2008. He received his research M.S. degree (DEA) in computer science from the University of Savoie in France in 2003, and his engineer degree in computer science from the University of Technology and Science H. B. (USTHB) in 2002. He is a senior member of the IEEE and has served asTechnical Program Committee member and reviewer of many international conferences and journals. His research interests lie in Internet of Things (IoT), wireless networking, Vehicular ad hoc networks (VANETs), Trust models design, quality of services (QoS) and security.