


République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université AMO de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Mémoire de Master

en Informatique

Spécialité : *Génie des Systèmes Informatiques*

Sujet

Modélisation et Évaluation des Performances des Appareils Autonomes à RF-EH et Sécurité de Niveau Physique dans l'IOT avec les Réseaux de Petri

---

Encadré par :

— Dr. OUKAS Nourredine

Réalisé par :

— BAHMED Kahina

— MOSTEGHANEMI Yasmine

2022/2023

Remerciements

Nous remercions Dieu, pour nous avoir guidé et donné la force de terminer ce mémoire de fin d'étude.

Nous souhaitons également remercier notre encadrant, Dr.Oukas Noureddine, pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant la préparation de ce mémoire. Ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans son aide.

Nous remercions les membres du jury d'avoir accepté d'examiner ce travail et pour leurs commentaires constructifs.

D'un cœur sincère, Nous remercions nos enseignants pour leurs précieux enseignements et leur encouragement constant. Leur passion et leur expertise nous ont inspiré tout au long de notre études.

Enfin, Nous adressons nos remerciements sincères à toutes les personnes, qu'elles aient été directement ou indirectement impliquées dans la réalisation de ce mémoire, ainsi qu'à tous ceux qui ont contribué à notre développement personnel et académique.

Ce mémoire a été rendu possible grâce à la contribution précieuse de chacun d'entre vous, et nous ressentons une profonde reconnaissance pour l'expérience inestimable acquise tout au long de ce processus.

Dédicaces

Je dédie ce modeste travail :

À mon père et ma mère, Je tiens à exprimer ma profonde gratitude pour votre précieux soutien tout au long de mon parcours académique et particulièrement lors de la réalisation de ce mémoire de fin d'étude.

À mon époux, et mes enfants : Aksil et Ghiles Votre soutien indéfectible, votre encouragement et votre compréhension inestimable ont été la lumière qui a éclairé chaque étape de ce voyage. Votre amour et votre soutien ont été le moteur qui m'a poussé à donner le meilleur de moi-même. Ce mémoire est aussi le vôtre, car sans vous, il n'aurait pas été possible.

À ma sœur Iman, son mari, et ses enfants Célia, Louise et Aksel Votre amour inconditionnel et votre soutien ont été un pilier fondamental tout au long de ma vie. Votre présence m'ont apporté la force nécessaire pour mener à bien ce mémoire.

À toute ma famille et mes amis sans exception, mes grands parents, mes tantes, mes cousins, mon binome Yasmine...

Ce mémoire est le fruit de l'effort collectif de nombreuses personnes exceptionnelles, et je tiens à vous rendre hommage. Votre présence dans ma vie a été une source de motivation et de joie.

Avec tout mon amour et ma gratitude,

Bahmed Kahina.

Dédicaces

Avec toute sincérité et avec tout respect, je dédie ce modeste travail à :

Ma chère mère«Souhila» qui s'est toujours sacrifiée pour mon éducation, qui ma entourée de son amour et son affection, je la remercie et je n'oublierai jamais son soutien moral dans les moments les plus difficiles, et surtout lors de la réalisation de ce mémoire de fin d'étude que dieu la protège.

Mon cher père «Toufik», témoignage de l'amour, affection et le soutien. Pour toutes les peines et tous les sacrifices que tu as consentis pour mon éducation, tu m'as appris à me battre jusqu'au bout pour réussir. Puisse Dieu, tout puissant, te prêter longue vie, santé et bonheur.

Mon marie«Abdelhak» qui m'a aidé, supporté, et encouragée dans les moments difficiles.Puisse Dieu le tout puissant t'accorder une longue vie couronnée de santé.

Ma sœur « Aicha Nermine » vous apporte joie et bonheur au quotidien. Votre présence est une bénédiction. Que notre lien grandisse plein d'amour et je vous souhaite du succès dans votre parcours académique.

Et à tous les membres de la famille «Mosteghanemi» paternelle et maternelle.

A mon binome «Kahina Bahmed», mes amies et surtout mes collègues de promotion.

Ce mémoire est la lumière de l'effort collectif de nombreuses personnes extraordinaires, et je souhaite vous rendre hommage. Votre présence dans ma vie a été une source d'encouragement et de joie. Merci à tous, je vous aime.

MOSTEGHANEMI Yasmine.

Résumé

Ce document présente une méthode de modélisation basée sur les réseaux de Petri stochastiques généralisés (RPSG) appliquée aux dispositifs autonomes sans fil, en particulier dans le contexte de l'Internet des objets. Chaque appareil est pourvu d'un système de récupération d'énergie par radiofréquence (EH-RF) qui exploite les signaux électromagnétiques afin de recharger les batteries à distance. Toutefois, ces sources d'énergie sont exposées à des risques d'attaque tels que le brouillage (Jamming), qui perturbe les signaux et impacte le fonctionnement des dispositifs. Pour résoudre ce problème, cette étude représente une approche de modélisation qui met en œuvre des changements de canal pour équilibrer la consommation d'énergie et la réactivité du service. Une analyse est entreprise pour identifier les configurations optimales des paramètres en vue d'applications concrètes.

Mots clés : Internet des Objets, Appareils autonomes sans fils, Modélisation avec Réseaux de Petri, Récupération d'énergie RF, Attaque de brouillage, Sécurité de niveau physique.

ملخص

يقدم هذا المستند أسلوب نمذجة يعتمد على شبكات بيتري الاحتمالية المعممة والمُطبق على أجهزة مستقلة لاسلكية ، وبخاصة في سياق ءنترنت الأشياء. كل جهاز مجهز بنظام استخلاص الطاقة باستخدام إشارات تردد الراديو لإعادة شحن البطاريات عن بعد. ومع ذلك، تكون مصادر الطاقة هذه عُرضة لمخاطر مثل هجمات التشويش ، التي تعطل الإشارات الحاملة للمعلومات وتؤثر على عمل الجهاز. لمعالجة هذه المشكلة، تقدم هذه الدراسة نهج نمذجة يدمج الانتقال بين القنوات لتحقيق توازن بين استهلاك الطاقة واستجابة الخدمة. يُجرى تحليل لتحديد تكوينات المعلمات الأمثل لتنفيذات عملية.

الكلمات المفتاحية : أنترنت الأشياء ، الأجهزة المستقلة اللاسلكية ، النمذجة بشبكات بيتري، استخلاص الطاقة الترددية، هجوم التشويش، الأمان على مستوى الطبقة الفيزيائية.

Abstract

This document presents a modeling method based on generalized stochastic Petri networks (GSPN) applied to autonomous wireless devices, particularly in the context of the Internet of Things (IoT). Each device is equipped with an energy harvesting system using radio frequency (RF) signals to remotely recharge batteries. However, these energy sources are susceptible to risks such as jamming attacks, which disrupt signals and impact device operation. To address this issue, this study introduces a modeling approach a modeling approach that incorporates channel hopping to balance energy consumption and service responsiveness. An analysis is conducted to identify optimal configuration's parameters for practical implementations.

Key words : Internet of Things, Wireless autonomous devices, Petri Nets Modeling, RF-Energy harvesting, Jamming Attack, Physical Layer Security.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AWD : Autonomous Wireless Devices

IoT : Internet of things

QoL : quality of life IdO : Internet des objets

IAB : Internet Architecture Board

NFC : Near Field Communication

RF : Radio frequency

EH : Energie harvesting

RdPSG : Réseau de petri stochastique généralisé

GPS : Global positioning system

RFID : Radio frequency identification

WS : Wiress sensor

WSN : Wirless sensor networks

RCSF : Réseau de capteurs sans fil

RRFE : Réseaux à récupération d'énergie RF

ABCN : Ambient Backscatter Communication Networks

WPCN : Wirless Powered Communication Networks

SWIPT : Simultaneous Wirless Information and Power Transfers

WAD : Wirless autonomes devices

GSPN : Generalized Stochastic Petri Nets

Introduction générale

L'avènement de l'Internet des Objets (ou Internet of Things : IoT) a ouvert la voie à de nouvelles perspectives ainsi qu'à des défis majeurs dans les domaines des communications et de la sécurité. Parmi les innovations les plus prometteuses figurent les Appareils Autonomes à Récupération d'Énergie Radiofréquence (RF-EH), qui offrent la capacité de fonctionner de manière autonome en exploitant l'énergie captée à partir des signaux radio. Cependant, la montée en puissance de ces dispositifs autonomes s'accompagne d'un nouvel éventail de risques liés à la sécurité physique, exposant ainsi les systèmes de l'IoT à des menaces potentielles.

La radiofréquence (RF) émerge comme une source d'énergie novatrice et prometteuse. Elle tire parti des ondes électromagnétiques pour générer une énergie exploitable. Cette approche trouve des applications diversifiées, particulièrement au sein des réseaux des objets autonomes, où elle est mise en œuvre pour recharger les batteries et prolonger la durée de vie des dispositifs. La technologie RF ouvre des perspectives fascinantes en matière de transmission d'énergie sans fil, contribuant ainsi à l'autonomie et à l'efficacité des systèmes énergétiques modernes.

L'évaluation des performances des réseaux des objets autonomes est entreprise selon deux approches distinctes : la simulation et la modélisation. Dans le cadre de la première méthodologie, les chercheurs recourent à des simulateurs spécialement conçus pour analyser virtuellement le comportement d'un réseau avant sa mise en œuvre pratique. Parmi les plate formes couramment utilisées, on peut citer NS, NS2, NS3, OMNET++, OPNET, et autres. Ces outils permettent une évaluation préliminaire des performances du réseau, offrant ainsi la possibilité d'anticiper et d'optimiser son fonctionnement avant le

déploiement réel.

Le présent projet vise à plonger au cœur de l'étude des réseaux des objets autonomes reposant sur la récupération d'énergie. Parallèlement, notre démarche se propose de développer une modélisation en utilisant les Réseaux de Petri Stochastiques Généralisés pour appréhender plus efficacement ces réseaux. Cette approche tiendra compte simultanément de la récupération d'énergie et de la mise en place de mécanismes de sécurité en vue de protéger le réseau contre d'éventuelles attaques.

Ce mémoire adoptera la structure suivante pour approfondir ces thématiques :

- Chapitre 1 : Vue générale sur l'Internet des Objets, incluant ses caractéristiques, architectures, domaines d'application, technologies, avantages et inconvénients, architecture des objets connectés, problématiques et solutions envisageables.
- Chapitre 2 : Exploration détaillée des attaques et des solutions de sécurité au niveau physique pour les Réseaux à Récupération d'Énergie RF (RF-EH).
- Chapitre 3 : Présentation approfondie des Réseaux de Petri stochastiques généralisés.
- Chapitre 4 : Présentation des travaux connexes et Proposition d'une nouvelle approche de modélisation pour les objets autonomes connectés en utilisant les Réseaux de Petri stochastique généralisé, en intégrant la sécurité de niveau physique.
- - Chapitre 5 : Description des paramètres de simulation, conduite d'une étude expérimentale.

On termine notre travail par une conclusion générale et quelques perspectives.

Chapitre 1

Internet des Objets

1.1 Introduction

L'Internet des objets (IoT) se profile comme l'une des technologies les plus prometteuses pour améliorer la qualité de vie humaine (QoL). Il joue un rôle crucial dans divers domaines tels que les services de santé, l'industrie automobile, l'agriculture, l'éducation et de nombreuses applications métiers intersectorielles. Dans les paragraphes suivants, nous explorerons différentes définitions de l'IoT, ses diverses architectures ainsi que les défis majeurs auxquels son adoption est confrontée, en particulier en ce qui concerne la sécurité.

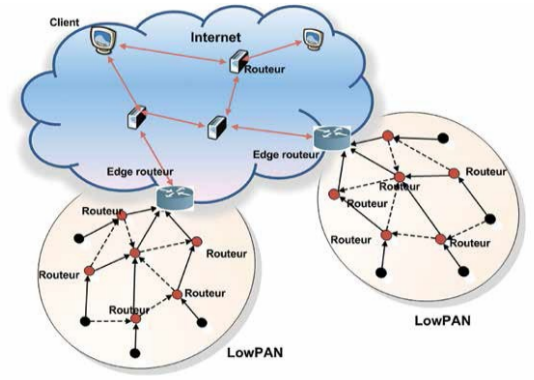

FIGURE 1.1 – L'internet des objets

1.2 Définition

Ce terme a été introduit pour la première fois en 1999 par Kevin Ashton. Il désigne l'association entre Internet et des objets, des lieux et des environnements physiques via des connexions. L'Internet des objets relie les éléments du monde réel au monde virtuel, offrant une connectivité permanente et universelle, non seulement pour les individus, mais aussi pour les objets. Il décrit un univers où objets physiques, entités humaines, données et environnements virtuels interagissent de manière synchronisée dans un même espace-temps [8]. L'Internet des objets (IoT) englobe un ensemble d'infrastructures et de technologies. Il garantit la connexion, au travers d'un réseau, des objets physiques afin qu'ils puissent échanger des informations concernant à la fois leur nature intrinsèque et leur environnement. La figure 1.1 illustre l'interconnexion entre différentes sphères d'application de l'Internet des objets [9].

1.3 Caractéristiques de l'internet des objets

Les caractéristiques fondamentales de l'IoT sont les suivantes [10] :

1.3.1 Interconnectivité

L'ensemble de l'infrastructure mondiale de l'information et de la communication peut être interconnecté, permettant une interaction fluide entre différents éléments.

1.3.2 Capteurs et actuateurs

Les objets de l'IoT sont pourvus de capteurs pour recueillir des données de leur environnement, ainsi que d'actuateurs pour réaliser des actions en réponse à ces données.

1.3.3 Services liés aux objets

L'IoT est en mesure de fournir des services liés aux objets, respectant les limites définies pour ces objets. Cela inclut des aspects tels que la protection de la vie privée et la cohérence sémantique entre les objets physiques et leurs homologues virtuels. Pour offrir ces services, une évolution des technologies à la fois dans le monde physique et celui de l'information sera nécessaire.

1.3.4 Hétérogénéité

Les dispositifs connectés à l'IoT peuvent provenir de divers fournisseurs, utiliser différentes technologies de communication et fonctionner dans des contextes variés.

1.3.5 Changements dynamiques

L'état des appareils peut changer de manière dynamique, par exemple, passer de l'état de sommeil à celui de réveil, se connecter et/ou se déconnecter, tout comme leur contexte, comprenant des éléments tels que la localisation et la vitesse. De plus, le nombre d'appareils peut varier dynamiquement.

1.3.6 Échelle énorme

Le nombre d'appareils gérés et interagissant entre eux dépassera au moins d'un ordre de grandeur le nombre d'appareils connectés à l'Internet actuel. La gestion de ces appareils et l'interprétation de la masse de données générées seront cruciales, tout comme la manipulation sémantique de ces données.

1.3.7 Sécurité et confidentialité

Étant donné la nature sensible des données collectées, la sécurité et la confidentialité des informations au sein de l'IoT sont d'une importance vitale et doivent être gérées avec précaution.

1.3.8 Impact sociétal

L'IoT détient le potentiel de transformer de nombreux aspects de la société, de l'industrie et de l'économie en améliorant les processus, en offrant de nouveaux services et en introduisant des innovations majeures.

1.3.9 Extensibilité

L'IoT peut être mis à l'échelle pour englober un grand nombre d'objets et de dispositifs, répondant ainsi aux besoins changeants des utilisateurs et des entreprises.

1.3.10 Connectivité étendue

L'IoT facilite la connexion d'une vaste gamme d'objets et de dispositifs grâce à diverses technologies de communication telles que le Wi-Fi, le Bluetooth, la 4G/5G, ainsi que des protocoles spécifiquement conçus pour les objets à faible consommation énergétique.

En somme, l'Internet des objets tisse une toile complexe d'objets connectés qui interagissent et collaborent pour améliorer la qualité de vie, optimiser les opérations et créer de nouvelles opportunités.

1.4 Architecture d'Internet des objets

L'architecture de l'Internet des objets (IoT) est conçue pour permettre la connectivité, la communication et la gestion efficaces des objets connectés. Elle est composée de plusieurs couches qui coopèrent pour faciliter la collecte, le traitement et la transmission des données. Voici les principales couches de l'architecture IoT [1] :

1.4.1 La couche perception

Au niveau bas dans la hiérarchie,se trouve la couche perception,cette couche englobe les objets physiques dotés de capteurs et d'actuateurs. Les capteurs collectent des données à partir de l'environnement, comme la température, l'humidité, la luminosité, etc. Les actuateurs permettent d'effectuer des actions sur l'environnement, comme allumer une lumière ou actionner un moteur. Cette couche comprend aussi l'équipement nécessaire pour mettre en œuvre la collecte de données de contexte d'objets connectés, à savoir les capteurs, les étiquettes RFID, caméras, GPS (Global Positioning System), etc.

1.4.2 La couche réseau

la couche réseau est un élément essentiel de l'architecture IoT. Elle permet la connectivité entre les différents objets connectés, les dispositifs de traitement, les serveurs cloud et les applications. Cette couche est responsable de l'acheminement des données entre les différents éléments de l'architecture IoT. Elle gère la connectivité, la communication et l'interopérabilité entre les objets connectés, les points d'accès réseau, les routeurs et les passerelles. Au sein de la couche réseau, il peut y avoir plusieurs éléments :

— Objets Connectés :Les objets équipés de capteurs et d'actuateurs sont les points de départ de la communication dans l'IoT. Ils envoient des données collectées via des protocoles de communication appropriés.

— Passerelles : Les passerelles agissent comme des intermédiaires entre les objets connectés et le réseau principal. Elles peuvent convertir les différents protocoles de communication utilisés par les objets en un protocole standard pour la transmission vers le réseau.

— Points d'Accès et Routeurs : Ces dispositifs assurent la connectivité sans fil des objets et des passerelles au réseau. Ils gèrent les connexions Wi-Fi, Bluetooth, 4G/5G, etc., et acheminent les données vers les destinations appropriées.

— Réseau Principal : C'est la partie centrale de la couche réseau. Elle permet la transmission des données entre les différents dispositifs connectés, les systèmes de traitement et les serveurs cloud. Le réseau principal peut utiliser divers protocoles de communication en fonction des besoins, tels que TCP/IP.

— Sécurité et Authentification : La couche réseau intègre également des mécanismes de sécurité pour garantir que seuls les dispositifs autorisés peuvent se connecter au réseau. Cela implique des protocoles d'authentification, de chiffrement et de gestion des clés.

En résumé, la couche réseau joue un rôle crucial dans l'acheminement efficace des données entre les objets connectés, les passerelles, les systèmes de traitement et les applications dans l'architecture IoT. Elle assure une communication fluide, sécurisée et interopérable au sein du réseau étendu de l'Internet des objets.

1.4.3 La couche application

C'est ici que les utilisateurs interagissent avec l'IoT. Les applications permettent aux utilisateurs de surveiller, de contrôler et d'interagir avec les objets connectés. Cela peut aller des applications domestiques intelligentes aux outils industriels avancés.

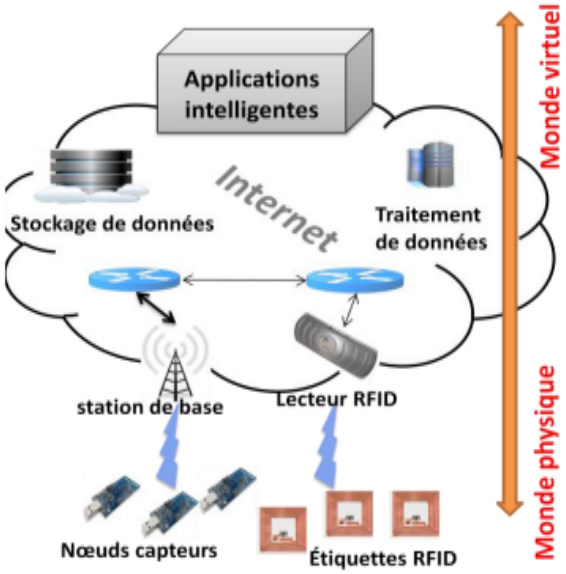

FIGURE 1.2 – Architecture de l'internet des objets [1].

En mars 2015, le comité de l'Internet Architecture Board (IAB) a publié la RFC 7452. Il propose quatre modèles d'interaction communs pour les acteurs IOT [11] :

- La communication entre objets, qui est basée sur une communication sans fil entre deux objets. Les informations sont transférées grâce à l'intégration de technologies de communication sans fil telles que zigbee ou bluetooth.
- Communication objet vers le cloud, dans ce modèle les données collectées par les capteurs sont envoyées à la plateforme de service via le réseau.
- Communication Object vers une passerelle, le modèle est basé sur un intermédiaire qui établit le lien entre le capteur et l'application dans le cloud.
- De l'objet au partage de données back-end, l'objectif de ce modèle est de permettre le partage de données entre les fournisseurs de services. Il est basé sur le concept de « réseau programmable ». Les fabricants ont mis en place une API qui permet d'utiliser les données collectées par d'autres fabricants.

1.5 Application de l'internet des objets

Les applications de l'Internet des objets (IoT) sont vastes et couvrent de nombreux domaines, offrant des solutions innovantes et améliorant divers aspects de la vie quotidienne, de l'industrie et de la société. Voici quelques exemples d'applications concrètes de

l'IoT :

- Santé Connectée :Les dispositifs portables tels que les montres intelligentes et les capteurs médicaux permettent de surveiller en temps réel la santé des individus, de suivre les signes vitaux, de gérer les médicaments et de fournir des alertes en cas de situations critiques.
- Villes Intelligentes :L'IoT est utilisé pour créer des infrastructures urbaines plus efficaces et durables. Cela inclut la gestion du trafic, l'éclairage public intelligent, la collecte des déchets basée sur la demande et la surveillance environnementale.
- Agriculture Intelligente : Les capteurs IoT dans les exploitations agricoles collectent des données sur le sol, les cultures et le bétail, permettant une gestion précise des ressources, une irrigation optimisée et une surveillance des conditions météorologiques.
- Industrie : L'IoT révolutionne l'industrie en permettant la surveillance en temps réel des machines, la maintenance prédictive, l'automatisation avancée et l'optimisation des chaînes de production.
- Maisons Intelligentes : Les appareils domestiques connectés, tels que les thermostats, les serrures, les appareils électroménagers et les systèmes de sécurité, peuvent être contrôlés et surveillés à distance, améliorant le confort et la sécurité.
- Logistique et Suivi des Biens :L'IoT permet de suivre en temps réel la localisation et l'état des marchandises en transit, réduisant les pertes, améliorant l'efficacité logistique et garantissant la fraîcheur des produits sensibles.
- Énergie Intelligente :Les compteurs intelligents et les réseaux électriques connectés permettent la gestion efficace de la consommation d'énergie, l'intégration des énergies renouvelables et la réduction des coûts.
- Environnement et Surveillance :Les capteurs IoT sont utilisés pour surveiller et collecter des données sur l'environnement, tels que la qualité de l'air, la pollution de l'eau, les niveaux sonores et les vibrations.
- Soins aux Animaux : L'IoT est également appliqué dans l'industrie agroalimentaire pour surveiller la santé et le bien-être des animaux d'élevage, en veillant à leurs besoins et à leur confort.
- Vêtements Connectés : Les textiles intelligents intégrant des capteurs peuvent être utilisés pour surveiller l'activité physique, la posture, la température corporelle,

etc.

Ces exemples ne représentent qu'une infime partie des nombreuses applications potentielles de l'IoT. En vérité, l'IoT demeure en constante évolution et s'étend vers des secteurs inexplorés, ouvrant ainsi un large éventail d'opportunités pour améliorer notre vie quotidienne et influencer la trajectoire de notre avenir technologique.

1.5.1 Les réseaux de capteur sans fils WSN

Un réseau WSN est un réseau composé d'un ensemble d'unités de traitements embarquées, appelées capteurs (nœuds).Ces noeuds communiquent entre eux afin de surveiller un phénomène précis(mouvement,vibration,température,humidité....). Dans une zone de captage "sensing field".Les données récoltées par les nœuds sont ensuite transmit vers un nœud médiateur dit puits (sink) pour pouvoir faire des traitements spécifiques avant de les transmettre à l'utilisateur final via internet ou liaison satellitaire (figure 1.3). de plus les capteurs sans fil sont dotés de moyens de traitement et de communication de l'information [2].

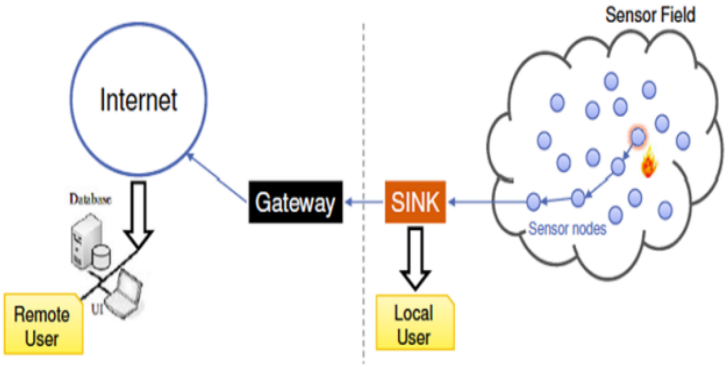

FIGURE 1.3 – Réseau de capteur sans fil [2].

Les capteurs Ce sont les principaux éléments des réseaux de capteurs sans fil. ils peuvent etre mobile ou statique. Leur rôle est d'obtenir des informations de leur environnement (par exemple, constantes corporelles, température, vitesse du courant océanique, etc.) et les trasmettres au noeud puits [12].

Architecture d'un noeud capteur sans fil

Un nœud capteur comprend quatre unités fondamentales. De plus, un réseau WSN peut également incorporer d'autres modules, tels qu'un système de localisation (récepteur GPS) pour déterminer sa position géographique, une source d'énergie génératrice (cellules solaires), voire un mécanisme de mobilité pour se déplacer [2](voir Figure 1.4).

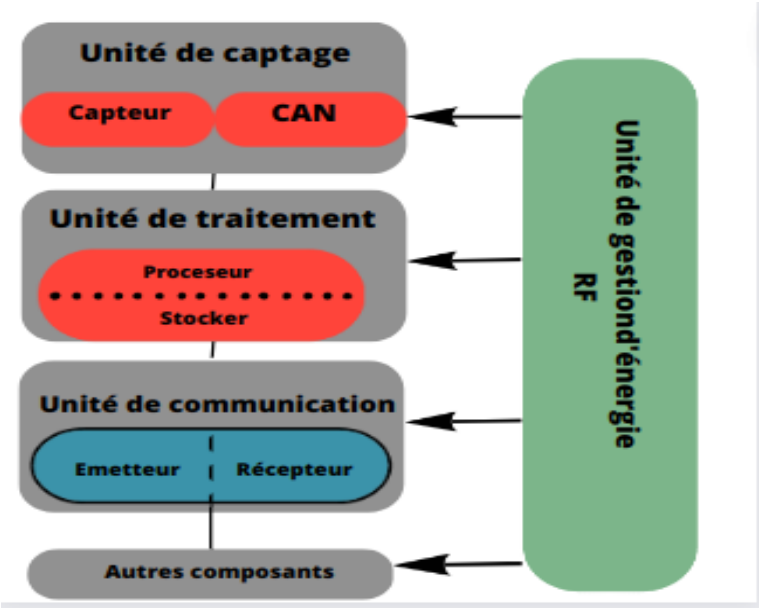

FIGURE 1.4 – Architecture d'un noeud de capteur sans fil.

Unité de captage

L'unité se compose de 2 sous unités : d'un capteur électronique et d'un convertisseur analogique numérique. Cette unité transforme ces signaux en un signal numérique compréhenible, qui sera ensuite soumis à l'unité de traitement.

Unité de traitement

Elle comprend un processeur associé a une unité de stockage. Elle implémente des protocoles de communication qui permettent aux nœuds de coopérer avec d'autres nœuds du réseau. Ainsi cette unité peut également analyser les données capturées pour faciliter la tâche du nœud puit (sink).

Unité de transmission (communication)

Elle réalise toutes les émissions et réception des données.

Unité de gestion d'énergie

Elle est responsable de la distribution de l'énergie disponible à tous les modules. Elle peut initier un mode "sommeil" des composants inactifs tout en minimisant la consommation et en réduisant les pertes d'énergie. Elle prend en charge également la gestion de mécanisme de charge énergétique utilisé pour augmenter la durée de vie des nœuds, prolongeant ainsi la durée de vie du réseau de nœuds.

1.6 Les technologies de l'IOT

Dans les applications IoT, les données générées par les appareils ou les sources doivent être transmises à Internet. Prouver la connectivité et la couverture est une tâche ardue pour les applications IoT. Les utilisateurs ou les fournisseurs veulent toujours collecter des données et les analyser pour un traitement ultérieur afin de mieux améliorer leurs appareils. L'émergence des nouvelles technologies dans la communication et l'informatique est cruciale. Au lieu d'aller sur un autre réseau, choisissez un meilleur réseau préféré, en particulier pour votre propre application. Aujourd'hui, les industriels participent activement au développement de canaux ou de protocoles de communication filaires ou sans fil. Mais le développement des coûts et des infrastructures joue un rôle crucial dans le développement de la technologie IoT. Une brève description de chacun de ces éléments est donnée ci-dessous [13].

1.6.1 RFID (Radio Frequency Identification)

L'acronyme RFID signifie « Radio Frequency Identification », qui se traduit en français par « Identification par Radiofréquence ». Grâce à des étiquettes émettant des ondes radio attachées ou intégrées aux objets (étiquettes RFID), cette technologie permet l'identification, le suivi en temps réel et la localisation d'objets dans des environnements intérieurs. La technologie RFID autorise la lecture des étiquettes sans nécessiter de ligne de vue directe et peut traverser des couches minces de matériaux (peinture, emballage, neige légère, etc.). Une étiquette radiofréquence (transpondeur ou étiquette RFID) est connectée

à une antenne via une puce et enveloppée dans un support (étiquette RFID). Un lecteur est utilisé pour capter les informations de cette étiquette et les transmettre au serveur [14].

1.6.2 Protocoles de Communication

Divers protocoles sont utilisés pour permettre la communication entre les objets connectés et les systèmes de traitement. Cela inclut des protocoles comme MQTT, CoAP, AMQP et HTTP, qui permettent des échanges de données efficaces et sécurisés.

1.6.3 Réseaux sans fil

Les technologies de communication sans fil, telles que le Wi-Fi, le Bluetooth, Zigbee, Z-Wave et LoRaWAN, jouent un rôle crucial dans la connectivité des objets au sein du réseau IoT.

1.6.4 NFC (Near Field Communication)

Cette technologie permet des échanges de données entre dispositifs à courte distance, généralement en touchant ou en plaçant les appareils à proximité les uns des autres.

1.6.5 Cloud Computing

Les services cloud sont utilisés pour stocker, traiter et analyser les données collectées par les objets connectés. Ils offrent également une infrastructure évolutive pour gérer un grand nombre d'objets.

1.7 L'architecteur des objets connectes

1.7.1 Definition d'un objet connecté

Un objet connecté est un dispositif de traitement ayant la capacité de se connecter à Internet et d'échanger des informations avec le cloud. Des exemples d'objets connectés comprennent les montres intelligentes, l'éclairage connecté, les caméras, et bien d'autres [15].

1.7.2 Definition d'un Objet autonome

Un objet autonome est un dispositif ou une entité capable de fonctionner, prendre des décisions et exécuter des actions de manière indépendante, sans nécessiter une intervention humaine constante. Il est doté de la capacité de traiter les informations de son environnement, d'analyser les données et de prendre des mesures appropriées en fonction de sa programmation, de ses capteurs et de son propre jugement. Les objets autonomes sont conçus pour accomplir des tâches spécifiques de manière autonome, ce qui peut inclure des actions réactives en réponse à des conditions préalablement définies ou à des événements.

1.7.3 Definition d'un objet autonome connecté

Un objet autonome connecté est un dispositif capable de fonctionner de manière autonome tout en étant connecté à Internet ou à un réseau de communication. Il peut collecter des données de son environnement à l'aide de capteurs intégrés, prendre des décisions basées sur ces données grâce à son propre traitement interne ou à des algorithmes d'intelligence artificielle, et exécuter des actions en réponse aux informations recueillies. De plus, il peut échanger ces données avec d'autres systèmes ou utilisateurs via la connectivité réseau. Cette combinaison d'autonomie et de connectivité permet à l'objet de fonctionner de manière intelligente et réactive, tout en étant capable de partager des informations et de contribuer à des systèmes plus larges.

Le concept de l'IoT prend forme grâce aux développements dans plusieurs domaines de recherche, notamment les réseaux de capteurs, le Web et le cloud computing. Étant donné que les capteurs fonctionnent sur batterie, la recharge des batteries des capteurs sans fil (WS) peut s'avérer coûteuse voire impossible dans certaines situations. Pour prolonger la durée de vie des WS, un domaine de recherche émergent au cours des dernières années est la récupération d'énergie (EH). Ces capteurs sans fil sont maintenant familiers dans la littérature sous le terme de EH-WS [9].

1.8 Problématiques des réseaux sans fil à des objets autonomes

— Le fonctionnement continu ou sur une longue période de ces applications est limité par la capacité restreinte des batteries des nœuds. Par conséquent, la réduction de la consommation énergétique s'avère être un enjeu critique [16].

— L'utilisation de la récupération d'énergie pourrait ainsi se présenter comme une réponse pour conférer une autonomie [17].

— Quant à la sécurité, les données collectées par les objets sont sensibles et doivent être protégées contre les accès non autorisés et les attaques. Les défis de sécurité incluent le maintien de la confidentialité des données, l'assurance de l'authenticité et de l'intégrité des informations, la détection des tentatives d'intrusion et la gestion sécurisée des clés.

— Les mécanismes de sécurité doivent être conçus de manière à minimiser leur impact sur la consommation d'énergie, tout en assurant la protection des données critiques collectées et transmises.

1.9 Les solutions de l'économisation d'énergie

1.9.1 Les mécanismes de veille

Pour résoudre le problème énergétique, certains auteurs ont proposé des méthodes basées sur des mécanismes de veille [18] [19].L'idée est de désactiver l'unité de communication de temps en temps. Le but est de conserver l'énergie d'une écoute constante. D'autres composants du capteur peuvent être désactivés à volonté.

1.9.2 La Récolte d'énergie

La récolte d'énergie est la conversion d'une forme d'énergie (comme l'énergie solaire, l'énergie éolienne, etc.) en énergie électrique. L'énergie issue des sources renouvelables appliquée aux nœuds capteurs, fournit une alimentation à long terme au capteur. Par la suite, c'est une solution ultime pour augmenter la durée de vie d'un RCSF. En prenant en considération la consommation énergétique d'un nœud, les technologies de récupération

d'énergie peuvent répondre totalement ou partiellement à ses besoins énergétiques [20].

1.10 Les avantages et les inconvénients de l'IoT

L'Internet des Objets (IoT) apporte un large éventail d'avantages et d'inconvénients. Voici un aperçu des principaux points positifs et négatifs de l'IoT :

1.10.1 Les avantages

— Gagne du temps en automatisant les activités ,les informations sont facilement disponibles, même lorsque nous sommes loin de notre emplacement réel, et elles sont souvent mises à jour en temps réel.

— Il est utile pour la sécurité car il détecte tout danger potentiel et avertit l'utilisateur. Par exemple, GM OnStar est un appareil intégré au système qui peut identifier les accidents de voiture ou les accidents de la route. Il passe des appels immédiatement en cas d'accident ou de collision.

— Il minimise les connexions des appareils IoT car ils Communiquent entre eux et effectuent diverses tâches sans intervention humaine.

— Le suivi du trafic ou des expéditions, le contrôle des stocks, la livraison, la surveillance, le suivi des commandes individuelles et la gestion des clients peuvent tous être plus rentables avec le bon système de suivi.

1.10.2 Les inconvénients

— L'IoT soulève des préoccupations majeures en matière de sécurité, car les dispositifs connectés peuvent être vulnérables aux cyberattaques. De plus, la collecte de données personnelles peut compromettre la confidentialité des utilisateurs.

— La mise en œuvre de l'IoT peut être complexe et coûteuse, notamment en ce qui concerne le développement de dispositifs, la mise en place d'infrastructures et la maintenance.

— L'IoT nécessite une connectivité Internet constante. Les interruptions de réseau peuvent entraîner des dysfonctionnements et des interruptions de service.

— L'IoT génère d'énormes quantités de données, nécessitant des systèmes de gestion et d'analyse sophistiqués pour en tirer des informations utiles.

— Il existe un risque élevé de chômage parmi les travailleurs non qualifiés, ce qui peut conduire au chômage. Des caméras de surveillance intelligentes, des robots, des systèmes de repassage intelligents, des machines à laver intelligentes et d'autres installations remplacent les agents de sécurité.

1.11 Conclusion

Ce chapitre nous a permis de plonger dans un univers en constante expansion, où la connectivité entre les objets physiques et virtuels révolutionne la manière dont nous interagissons avec le monde qui nous entoure. L'IoT a émergé comme l'une des technologies les plus prometteuses, avec des applications variées et des implications profondes dans de nombreux domaines de notre vie quotidienne.

Nous avons exploré les caractéristiques fondamentales de l'IoT, notamment son interconnectivité, la présence de capteurs et d'actuateurs, la fourniture de services liés aux objets, ainsi que les défis tels que l'hétérogénéité, les changements dynamiques, la sécurité et l'impact sociétal. Nous avons également examiné l'architecture de l'IoT, mettant en lumière les couches réseau, la couche application et les composants clés de chaque couche.

Dans le domaine des applications, nous avons découvert une multitude de cas concrets où l'IoT transforme les opérations, améliore la qualité de vie et offre de nouvelles opportunités dans des secteurs tels que la santé, l'agriculture, la domotique, la gestion environnementale et bien d'autres encore.

Cependant, il est essentiel de garder à l'esprit les défis qui accompagnent cette révolution technologique. La gestion de la consommation d'énergie, la garantie de la sécurité des données, l'interopérabilité et la complexité sont autant de considérations critiques qui nécessitent une attention constante pour garantir le succès et la durabilité de l'IoT.

En fin, l'IoT continue d'évoluer, d'explorer de nouveaux horizons et de façonner notre avenir technologique. En exploitant ses avantages tout en gérant ses inconvénients, nous pouvons construire un monde où la connectivité intelligente enrichit notre quotidien, améliore nos processus et ouvre la voie à des innovations encore inimaginables.

Chapitre 2

Attaques et Solutions de Sécurité au Niveau Physique dans les Réseaux à Récupération d'Énergie RF

2.1 Introduction

Les avancées rapides dans les technologies de l'interner des Objets (IoT) ont créé de nouvelles façons de communiquer, dont les Réseaux à Récupération RF d'Énergie (RRFE) jouent un rôle important. Ces réseaux utilisent l'énergie des signaux radio pour fonctionner et pourraient changer la manière dont les objets IoT sont alimentés. Cependant, cela soulève des questions, surtout en matière de sécurité. Les attaques physiques sont un grand problème pour la sécurité des RRFE, car elles pourraient perturber leur fonctionnement et leur fiabilité. Dans ce chapitre, nous examinons attentivement les différentes attaques possibles sur les RRFE au niveau physique, ainsi que les solutions pour les protéger et les rendre solides dans le monde complexe de l'IoT.

2.2 Récupération d'énergie par RF

Pour alimenter un système embarqué, il est également possible d'utiliser le transfert d'énergie électromagnétique. Cette technologie se présente comme particulièrement prometteuse et séduisante pour les dispositifs embarqués. Ainsi, la production d'énergie se fait par le biais d'une liaison sans fil, sans qu'il soit nécessaire d'établir un lien physique entre

les sources d'énergie et les équipements alimentés.Pour plus de détails nous renvoyons les lecteurs intéressés à la contribution de l'auteur dans [21] Pour mieux comprendre les principes des matériaux qui facilitent la récupération d'énergie électromagnétique, nous nous penchons sur les informations scientifiques les plus récentes disponibles dans la littérature. Ces sources indiquent que les signaux RF employés pour alimenter les équipements embarqués peuvent présenter des densités de puissance allant de 0,000012 à 15 mW/cm^2 par unité de temps. Ces valeurs varient en fonction de différents facteurs, tels que la distance par rapport à la source RF et la puissance maximale du signal [22] ; [23]. Globalement, trois principales architectures de réseaux électromagnétiques sans fil peuvent être identifiées :

— ABCN (Ambient Backscatter Communication Networks) Réseaux de communication par rétrodiffusion ambiante.

— WPCN (Wireless Powered Communication Networks) Réseaux de communication alimentés sans fil.

— SWIPT (Simultaneous Wireless Information and Power Transfers) Réseaux de transferts simultané d'informations et d'énergie sans fil.

2.3 Réseaux de communication par rétrodiffusion ambiante (ABCN)

Les réseaux de communication par rétrodiffusion ambiante, également connus sous le nom de "Backscatter Communication Networks" en anglais, sont des systèmes de communication sans fil qui exploitent les signaux radiofréquences existants dans l'environnement pour transmettre des données. Cette technologie repose sur le principe de la modulation par rétrodiffusion, où les dispositifs de communication modulent des signaux ambiants pour transmettre des informations.

Dans ces réseaux, les appareils utilisent des antennes passives pour réfléchir les signaux RF émis par des sources telles que les stations de base Wi-Fi, les tours cellulaires ou même les signaux de diffusion audio et vidéo. En modulant la rétrodiffusion de ces signaux, les dispositifs peuvent transmettre des données à d'autres appareils à proximité ou à des récepteurs équipés pour détecter les variations de la rétrodiffusion.

Cette approche présente des avantages potentiels en termes de faible consommation

d'énergie, de coût réduit et de facilité de déploiement. Les réseaux de communication par rétrodiffusion ambiante trouvent des applications dans divers domaines tels que l'Internet des Objets (IoT), les objets connectés et les systèmes de suivi à faible consommation. Cependant, ils peuvent également présenter des défis en termes de débit de données, de portée et d'interférences avec les signaux ambiants. À leur tour, d'autres appareils ABCN du réseau utilisent le même principe de réponse et d'activation de la communication D2D. Supposons un réseau ABCN générique, comme illustré à la Figure , où une source RF générique est utilisée comme une alimentation du signal RF ambiant K ABCN fournit des informations pour un seul récepteur ABCN.

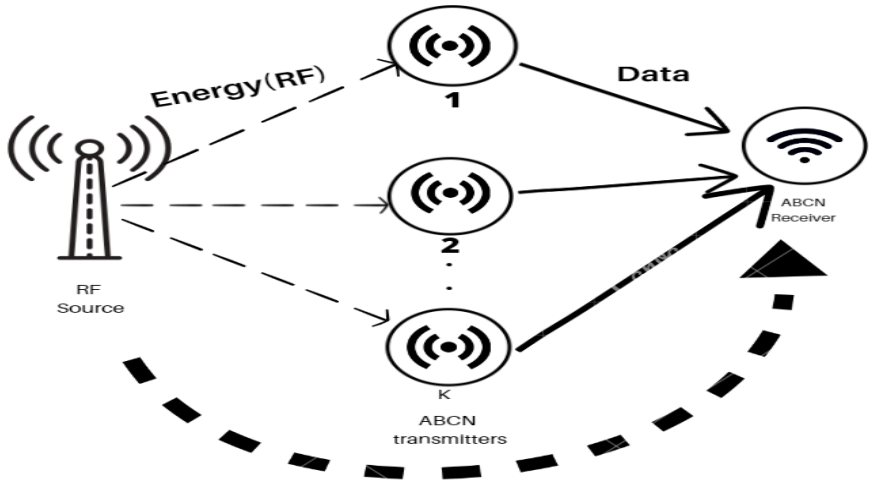

FIGURE 2.1 – Modèle de réseaux de communication par rétrodiffusion ambiante (ABCN).

2.4 Réseaux de communication alimentés sans fil (WPCN)

Les réseaux de communication alimentés sans fil (WPCN), souvent désignés comme des réseaux de transfert d'énergie sans fil en champ lointain (WPT), sont des systèmes de communication qui tirent leur énergie de sources d'alimentation spécifiques. Ces sources fournissent l'énergie nécessaire pour alimenter les appareils au moyen de la technologie WPT. Un modèle de ce système est illustré dans la figure, où la balise de puissance émet un signal RF dédié. Ce signal est utilisé par la source pour accumuler l'énergie requise en vue de la communication avec plusieurs appareils destinataires.

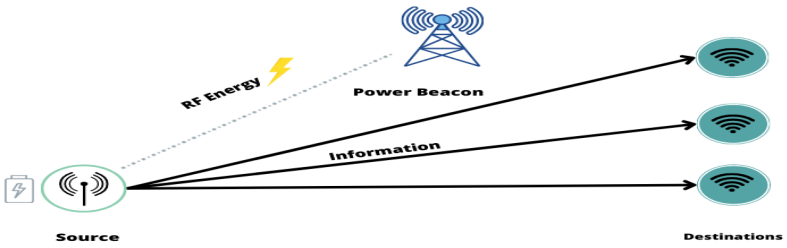

FIGURE 2.2 – Modèle d'un réseau de communication alimentée sans fil générique. La balise de puissance émet une source RF qui alimente l'émetteur et lui permet de communiquer avec un récepteur [3].

Comparativement aux réseaux de communication à rétrodiffusion, les réseaux de communication alimentés sans fil (WPCN) se distinguent par l'utilisation de signaux spécifiques dédiés à cette fonction (non utilisés pour d'autres tâches de communication). De plus, ils sont caractérisés par des portées de communication plus étendues. Cela est possible grâce à l'utilisation d'antennes d'émission plus grandes en comparaison avec la longueur d'onde du rayonnement [24].

Comparé au concept de SWIPT (Simultaneous Wireless Information and Power Transfer), la différence essentielle réside dans l'utilisation de l'énergie récupérée pour soutenir la transmission d'informations plutôt que pour recharger les dispositifs. Cela prévoit ainsi une anticipation de la phase de communication, une approche souvent appelée "récolter-puis-transmettre". De plus, il est important de noter que le signal qui alimente les dispositifs est dissocié du signal d'information, car il n'est pas spécifiquement conçu pour transférer des données.

Supposons que t0 représente le temps alloué à la récupération d'énergie dans un intervalle de temps T. Il est crucial d'optimiser ce temps de récolte d'énergie pour trouver un équilibre entre la puissance disponible sur les appareils et le débit de données.

Cependant, il convient de noter que des problèmes de sécurité significatifs émergent au niveau de la couche physique, en particulier pour les dispositifs situés à une certaine distance de la source d'alimentation. Ces dispositifs récoltent moins d'énergie que d'autres, mais ont besoin d'une puissance supérieure pour permettre une transmission sur une plus

grande distance [25].

2.5 Réseaux de transferts simultané d'informations et d'énergie sans fil (SWIPT)

Comme présenté dans la Figure, les réseaux de transfert simultané d'énergie et d'informations sans fil (SWIPT) se distinguent par la coexistence de processus de récupération d'énergie contextuels et de transfert d'informations. Cette coexistence est rendue possible grâce à l'utilisation d'architectures matérielles spécifiquement conçues à cet effet. D'une manière générale, les systèmes SWIPT se caractérisent par une centrale émettrice

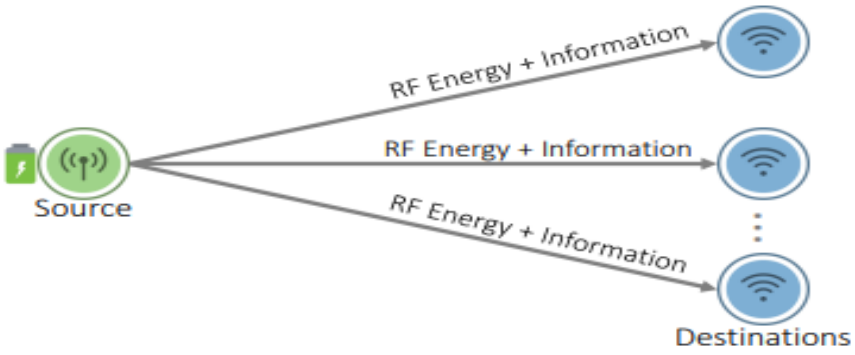

FIGURE 2.3 – Modèle d'un système générique à entrée unique et à sorties multiples d'un Réseau de transfert d'énergie et d'information sans fil. Une source alimentée par batterie émet un signal transférant des informations et de l'énergie RF, en même temps [3].

et plusieurs N (N $>$ 1) nœuds destinataires.

2.6 La sûreté et la sécurité dans les WAD basés sur RF

Le transfert de puissance à longue portée par ondes radio présente des défis en matière de sûreté et de sécurité, ce qui requiert des solutions appropriées. Dans les systèmes de transfert d'énergie sans fil (WPT) basés sur les ondes radiofréquences (RF), l'objectif principal de la sécurité est d'assurer les caractéristiques classiques de sécurité telles que la confidentialité, l'intégrité et la disponibilité des canaux de transfert de puissance. Il

existe plusieurs aspects liés à la sûreté et à la sécurité dans les dispositifs autonomes sans fil (WAD) qui doivent être pris en considération [4] :

- Lorsqu'il s'agit de transmettre de l'énergie sans fil, un défi majeur réside dans l'incapacité à crypter et à authentifier cette transmission, ce qui compromet la confidentialité de la charge destinée à un récepteur spécifique [26]. Cette situation expose les canaux de transfert d'énergie à des vulnérabilités face à diverses attaques, dont les conséquences sont doubles
  - Elles pourraient mettre en péril la sécurité et la sûreté des utilisateurs concernés.
  - Elles pourraient également perturber le processus même du transfert d'énergie, entravant ainsi son efficacité.
- Les approches classiques de sécurité exigent une grande quantité de ressources informatiques [27]. Cependant, dans le contexte des réseaux de capteurs sans fil alimentés par radiofréquence (RF WAD), il n'est pas toujours possible de générer une puissance adéquate pour exécuter des opérations de sécurité au niveau des nœuds de collecte. Par conséquent, l'enjeu consiste à assurer une protection suffisante malgré des ressources limitées, principalement sous forme d'énergie récupérée.

2.7 Sécurité des données de la couche physique

2.7.1 Adversaires externes

Nous désignons comme adversaire externe un dispositif qui n'est pas impliqué dans les schémas de communication conventionnels du réseau, ce qui le maintient anonyme vis-à-vis des périphériques du réseau. Ce scénario est courant dans divers contextes de réseaux sans fil, notamment les réseaux de capteurs sans fil (WSN) et l'Internet des objets (IoT), où un observateur externe peut simplement utiliser une antenne de réception accordée sur la même fréquence de canal que la communication légitime pour intercepter les informations avec succès, en supposant que des techniques de cryptographie ne sont pas en place. La caractéristique distinctive de ces travaux réside dans le fait qu'aucune information sur l'adversaire n'est disponible [28].

2.7.2 Adversaires internes

Nous donnons la définition d'un adversaire interne comme étant un dispositif qui fait partie légitime du réseau, participant activement aux opérations du réseau en émettant et en recevant des informations. Dans la littérature relative à la sécurité de la couche physique pour les réseaux RF EH, ce type de scénario contradictoire est souvent qualifié de "modèle actif indiscret", caractérisé par la coexistence d'activités fonctionnelles légitimes (transmissions/réceptions autorisées) et d'activités passives non autorisées (telles que l'écoute des communications) [28].

2.7.3 Relais non fiables (Untrusted relays)

"Relais non fiables" ou "relais non dignes de confiance" désigne des nœuds ou dispositifs dans un réseau de communication qui ne peuvent pas être considérés comme étant sûrs ou dignes de confiance pour transmettre ou manipuler les données de manière sécurisée. Ces relais peuvent présenter des risques de sécurité en raison de leur nature non fiable, ce qui peut entraîner des problèmes tels que l'interception malveillante, la modification ou la divulgation de données sensibles. Dans de nombreux contextes, des mécanismes de sécurité, tels que le cryptage des données, l'authentification des nœuds ou des protocoles de routage sécurisés, sont nécessaires pour atténuer les risques associés aux relais non fiables dans un réseau [28].

2.8 Attaques et menaces

Les mécanismes et les stratégies sous-jacents qui soutiennent les dispositifs d'harvesting d'énergie exposent les appareils et les réseaux sans fil à une pluralité d'attaques à travers différentes couches de la pile de protocoles. Ces menaces ne se limitent pas à des attaques d'écoute anodines, mais visent également la disponibilité et la fiabilité des systèmes. La littérature [3] a identifié et examiné divers types d'attaques, chacun exigeant des outils et des compétences spécifiques, tout en ciblant des technologies habilitantes spécifiques [3].

2.8.1 L'écoute clandestine (Eavesdropping)

En premier lieu, plusieurs recherches, notamment les travaux de [24], [4] et [29],mettent en avant le fait que les réseaux RF EH sont généralement déployés sans aucune intégration de mécanismes de cryptage. Cette situation expose donc l'énergie et les informations fournies aux risques d'écoute clandestine. En réalité, du fait que les réseaux RF EH sont souvent limités en puissance par rapport à d'autres sources d'énergie, l'incorporation de techniques de cryptage prêtes à l'emploi n'est souvent pas appropriée. Ces considérations ont suscité une quantité importante de travaux académiques, se concentrant sur la sécurisation de la couche physique dans le but d'améliorer la confidentialité des données et de développer des techniques de cryptographie adéquates, spécialement conçues pour les dispositifs à faible disponibilité énergétique.

2.8.2 DoS

Les attaques de type Déni de Service (DoS) ont pour but de compromettre la disponibilité des réseaux fonctionnant grâce à l'harvesting d'énergie (EH). Parmi ces réseaux, ceux alimentés par des signaux RF sont particulièrement susceptibles aux attaques. Dans ce contexte, l'une des méthodes les plus simples pour rapidement épuiser l'énergie d'un dispositif EH consiste à mener une attaque par épuisement énergétique. Comme mentionné par les auteurs dans l'article [30], ce type d'attaque par épuisement de puissance se caractérise par l'envoi de faux paquets à un nœud alimenté par des signaux sans fil. Les opérations de radio et de traitement nécessaires pour analyser et rejeter ces paquets fictifs peuvent accélérer le déchargement de la batterie de l'appareil, perturbant ainsi le bon fonctionnement des nœuds du réseau. Un exemple concret d'une telle attaque est une attaque d'inondation. Les auteurs explorent plusieurs scénarios d'attaque, parmi lesquels un attaquant pourrait :

— Introduire un logiciel malveillant au sein d'un réseau de capteurs sans fil (WSN) pour augmenter la puissance d'émission (et donc la consommation d'énergie) des dispositifs légitimes.

— - Adopter des techniques de brouillage pour injecter du bruit dans le canal de communication, forçant ainsi les nœuds à augmenter leur puissance de transmission et à consommer plus d'énergie.

— Exploiter les vulnérabilités de certains schémas d'agrégation de trafic afin d'aug-

menter la taille des paquets à retransmettre.

2.8.3 Infection par des logiciels malveillants (malware infection)

Un autre moyen employé par les attaquants pour drainer rapidement la batterie d'un dispositif consiste généralement à introduire intentionnellement des applications malveillantes sur un appareil ciblé, afin d'envoyer de multiples demandes d'alimentation, ce qui a pour effet de diminuer l'efficacité globale du système. À titre d'exemple, les auteurs [31], ont illustré une situation où des logiciels malveillants sont utilisés pour induire un comportement spécifique au sein de la cible victime. Parmi les autres types d'attaques spécifiques aux réseaux RF EH, on compte celles qui ciblent la validité des messages utilisés pour acheminer l'énergie RF nécessaire à la charge des dispositifs.

Les réseaux de communication d'énergie sans fil (WPCN) requièrent l'émission de signaux pilotes spécifiques par des balises d'alimentation, permettant ainsi d'activer physiquement les dispositifs à collecte d'énergie. Néanmoins, ces signaux pilotes sont généralement dépourvus de mesures de sécurité telles que l'authentification, l'intégrité et la confidentialité. En conséquence, comme le mettent en avant les auteurs dans l'article de référence [26], diverses formes d'attaques sont envisageables. En ce qui concerne la phase de transmission, il est possible d'usurper le signal pilote destiné à la charge, ce qui déclenche une attaque d'usurpation de signal pilote. Cette situation peut également se produire lorsque le dispositif EH émet explicitement une demande d'alimentation en envoyant un paquet de requête à la balise. Dans ce scénario, un attaquant peut intercepter ce message et simuler des balises d'alimentation, ce qui a pour effet de réduire les performances et la durée de vie du dispositif EH [32]. Les WPCN sont également vulnérables aux attaques de charge, qui peuvent être catégorisées en attaques de vampirisme, attaques voraces et attaques de débordement de charge. Les attaques de vampirisme sont des attaques au niveau physique où les dispositifs continuent de se charger sans émettre de demandes explicites, en exploitant les fuites d'énergie résultant de l'alimentation d'appareils voisins. Cette situation peut impacter la perception d'une balise d'alimentation, particulièrement si celle-ci s'efforce de maintenir la disponibilité énergétique des nœuds EH [4].

Les attaques voraces impliquent des dispositifs constamment gourmands en énergie, qui sollicitent continuellement la source, entravant ainsi la capacité des autres dispositifs à

solliciter de l'énergie. D'autre part, les attaques de débordement de charge impliquent un nœud EH compromis, qui fournit des mesures d'énergie incorrectes à la source d'alimentation, forçant ainsi un ajustement (augmentation ou diminution) du niveau de puissance de référence. Ce scénario peut aboutir à un déni de service (DoS) ou à une attaque de débordement de charge non autorisée. Dans le premier cas, la réduction du niveau de puissance du signal RF réduit la zone de réception du signal, éventuellement en excluant certains dispositifs de la réception d'une quantité suffisante d'énergie. Dans le second cas, l'augmentation du niveau de puissance du signal pilote accroît la zone de réception, offrant potentiellement aux dispositifs EH malveillants, contrôlés par l'attaquant, la possibilité d'être activés. De plus, il est à noter, comme en discutent les auteurs [4], que l'énergie récupérée peut subir d'importantes fluctuations en raison de la présence de personnes dans la zone de déploiement. Cette caractéristique pourrait permettre à un attaquant de déduire des informations sensibles concernant l'état de l'environnement physique environnant le réseau EH, telles que le nombre de personnes présentes, leurs mouvements et leur répartition temporelle, ce qui constitue une menace sérieuse pour la confidentialité.

2.8.4 Canal latéral (Lateral channel)

Les attaques par canal latéral permettent à un adversaire d'acquérir des informations pertinentes depuis un appareil, incluant des secrets tels que des clés ou des données privées. Ces attaques exploitent les fonctionnalités de la couche physique, notamment les émissions électromagnétiques et magnétiques involontaires, les données de synchronisation et la consommation d'énergie. Comme en discutent les auteurs dans les articles de référence [33]et [34], les attaques par canal latéral représentent également une menace pour les réseaux EH. Par exemple, les clés générées par les nœuds peuvent être révélées en corrélation avec la consommation d'énergie instantanée, en la mettant en relation avec les fuites électromagnétiques engendrées durant les opérations cryptographiques. Cette attaque a également été décrit par les auteurs dans l'article [31], où des logiciels malveillants puissants sont déployés sur le réseau. Ces logiciels malveillants extraient des informations sensibles de la victime et exploitent une carte d'interface réseau WiFi (NIC) pour contraindre les périphériques sans fil à rétrodiffuser les signaux RF environnants, créant ainsi un canal latéral discret pour la transmission clandestine d'informations.

2.8.5 Relecture et usurpation (Replay and Spoofing)

Relecture et usurpation. Comme le soulignent certaines contributions telles que [31] et [32], les signaux d'activation ABCN ne sont pas authentifiés, ce qui les rend sujets à une possible réutilisation et usurpation par un attaquant. Alors que les auteurs de l'article [32] ont contextualisé cette attaque dans le cadre d'un WBAN (Wireless Body Area Network).

2.8.6 Attaques de brouillage (Jamming)

Un autre type d'attaque vise à délibérément créer des interférences pour perturber la communication entre les ETs (Émetteurs d'Énergie) et les ERs (Récepteurs d'Énergie). Les nœuds malveillants peuvent déployer du brouillage sur un canal donné ou balayer l'ensemble des canaux de communication pour les rendre inutilisables. Lorsque les demandes d'alimentation des ERs sont bloquées, les ETs ne reçoivent pas les requêtes d'énergie, ce qui peut entraîner l'interruption de la transmission d'énergie. Cette situation peut engendrer une pénurie d'énergie et la cessation de leurs opérations.

La détection d'interférences constitue une étape essentielle pour contrer de telles attaques. Cette détection peut être mise en œuvre en interrompant périodiquement la transmission d'énergie et la communication, en surveillant le réseau pour identifier des transmissions RF suspectes et en évaluant la présence d'un attaquant externe au réseau (connu). Néanmoins, les attaquants pourraient également synchroniser leurs actions avec la période de détection des interférences pour éviter d'être repérés, ce qui complique la détection. C'est pourquoi il est nécessaire de développer des méthodes plus robustes et sophistiquées pour repérer efficacement les interférences.

Après avoir détecté les interférences, les ETs doivent ajuster de manière dynamique leurs paramètres de transmission pour que les ERs ne subissent pas l'impact des nœuds malveillants et puissent recevoir l'énergie de manière efficiente. La manière de réaliser cette adaptation et d'atteindre un consensus à l'échelle du réseau pour assurer un fonctionnement sécurisé reste une question ouverte.

Parmi les solutions prometteuses pour contrer les attaques de brouillage, on trouve des approches basées sur la gestion des interférences, comme l'alignement des interférences [5]. Cette technique permet aux ETs d'émettre des signaux alignés sur ceux de l'ER, de sorte que chaque récepteur puisse décoder le signal qui lui est destiné. Ainsi, l'impact des interférences agrégées est minimisé, voire éliminé. Bien que ces techniques offrent la

possibilité aux ERs de recevoir des paquets de données malgré la présence d'attaques de brouillage, leur mise en œuvre pratique et leur adaptation à des scénarios réels restent des défis non négligeables [4] . Le changement de canal est une approche fréquemment utilisée pour contrer les attaques de brouillage, où un attaquant perturbe la communication sur un canal spécifique. Cette stratégie implique de basculer vers un canal différent pour éviter les interférences créées par l'attaquant. Cependant, cela nécessite une détection rapide du brouillage et une prise de décision efficace pour migrer vers un canal moins perturbé. Le changement de canal est l'une des méthodes pour maintenir la communication malgré les tentatives d'attaques de brouillage, mais d'autres techniques telles que la détection des interférences, la modulation de puissance et l'utilisation de codes correcteurs d'erreur peuvent également être utilisées pour renforcer la résilience du réseau contre de telles attaques.

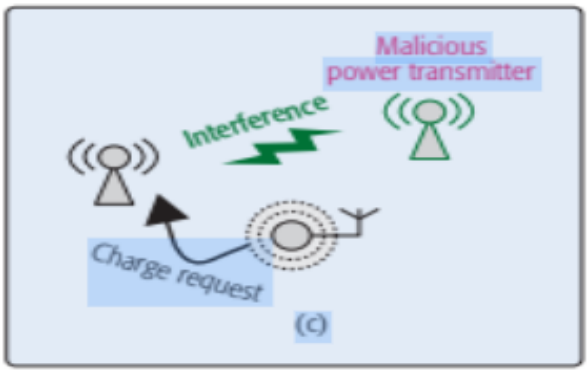

FIGURE 2.4 – Modèle de l'attaque Jamming [4] .

2.9 Contre-mesures de la couche physique

Au cours des dernières années, un grand nombre de contributions scientifiques ont proposé des solutions au niveau de la couche physique afin d'assurer la disponibilité des réseaux EH. Des références telles que [35] à [36] en sont des exemples. Les auteurs de l'article [4] ont également mis en évidence de manière qualitative différentes contre-mesures pouvant être utilisées contre divers types d'attaques dans le contexte des réseaux WPCN.

2.9.1 Contre mesures contre les attaques de brouillage

Pour faire face aux attaques de brouillage, les auteurs ont proposé diverses stratégies de défense. Parmi celles-ci, l'utilisation de schémas de modulation traditionnels tels que l'accès multiple par répartition en fréquence (FDMA : la bande de fréquences est divisée en plusieurs canaux/porteuses RF, chaque opérateur étant attribué à des utilisateurs différents), l'accès multiple par répartition dans le temps (TDMA) et le saut de fréquence ont été suggérés. En plus de cela, les principes d'alignement des interférences (beamforming) ont été explorés. Une autre approche consiste à mettre en œuvre des changements de canal réguliers, où les appareils de communication basculent vers un canal différent pour éviter les interférences causées par l'attaquant.

L'alignement des interférences

L'alignement des interférences est une stratégie novatrice en transmission sans fil, coordonnant les émetteurs pour aligner leurs interférences mutuelles avec le récepteur, simplifiant l'annulation des interférences. Dans les systèmes cellulaires, où les stations de base partagent des fréquences, les interférences réduisent le débit et causent des pannes. Dans les réseaux locaux, les interférences surviennent lorsque des points d'accès partagent des canaux. L'alignement d'interférences est une technique révolutionnaire en transmission sans fil qui vise à réduire les effets nuisibles de l'interférence. En coordonnant les émetteurs de manière à ce que leurs interférences mutuelles se combinent de manière constructive au récepteur, cette stratégie facilite l'annulation des interférences. Dans les réseaux cellulaires et locaux, les interférences limitent souvent les performances en réduisant la capacité de transmission. L'alignement d'interférences implique un codage multidimensionnel des signaux, alignant les signaux interférents observés par chaque récepteur dans un espace de dimensions réduites. Cette approche maximise le nombre de symboles non perturbés pouvant être transmis simultanément sur le canal perturbé, améliorant ainsi le débit. L'alignement d'interférences permet aux utilisateurs de décoder leurs messages sans être perturbés par les interférences en projetant le signal reçu dans un sous-espace orthogonal à l'interférence [5]. Les travaux initiaux sur cette technique ont montré que sa réussite dépend du nombre de dimensions de signal disponibles pour le codage. Une plus grande disponibilité de tranches de temps, de blocs de fréquence ou d'antennes pour le précodage accroît la capacité du système à gérer et à aligner les interférences de manière efficace

[37].

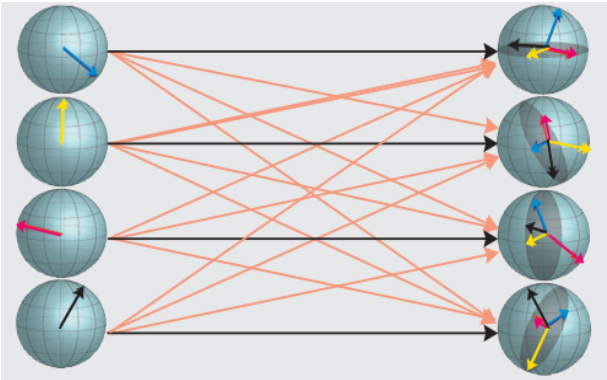

FIGURE 2.5 – Un schéma illustrant l'alignement des interférences [5] .

2.9.2 Contre mesure contre l'attaque d'usurpation d'identité

Les contre-mesures contre l'attaque d'usurpation d'identité visent à prévenir ou atténuer les risques liés à cette menace. Ces mesures comprennent l'authentification forte, la validation à plusieurs facteurs, l'utilisation de certificats numériques, la détection comportementale et l'analyse de l'intégrité des données pour garantir une sécurité renforcée et une identification fiable des utilisateurs.

2.9.3 Contre mesure contre les Attaques de surveillance

Pour détecter les attaques de surveillance, ils ont proposé d'écouter le canal de communication et de découvrir la présence de données échangées entre les nœuds récupérateurs d'énergie et d'éventuels nœuds malveillants.

2.9.4 Contre mesure contre les Attaques de charge pour DOS

En ce qui concerne les attaques de charge, les auteurs ont proposé d'effectuer des estimations régulières de l'énergie collectée par les nœuds dans le réseau, tout en détectant les anomalies dans le profil de charge.

2.9.5 Contre mesure contre les Applications malveillantes

Pour vaincre les applications malveillantes, les auteurs recommandent de vérifier les signatures des applications et de vérifier si elles sont dignes de confiance/valides. Alternativement, ils pointent la possibilité de concevoir des mécanismes sensibles à l'énergie afin que chaque application puisse tirer parti du budget énergétique à utiliser pour le calcul et la transmission.

2.9.6 Contre mesure contre les Problèmes de confidentialité

Pour répondre aux problèmes de confidentialité, ils proposent de collecter les empreintes RF de l'environnement et de les comparer aux empreintes acquises lors de l'exécution. Dans le contexte des réseaux IoT alimentés via rétrodiffusion, les auteurs dans [38] ont identifié la possibilité d'imposer l'authenticité de la communication par des signatures à propagation par trajets multiples, assurant ainsi les processus d'appariement et de communication de données. Ils ont découvert que l'interaction des sources RF avec l'environnement et l'emplacement d'un appareil particulier est unique. Ainsi, il peut être utilisé pour fournir une authentification probabiliste et dépendante de l'environnement, ainsi qu'un outil pour identifier les attaques de rejeu et de désauthentification.

2.9.7 Contre mesure contre les interférences malveillantes sources de brouillage

Pour faire face aux interférences malveillantes sources de brouillage, les contributions dans [35], [39],[40],[36] proposent d'utiliser des techniques bien connues de saut de fréquence et d'étalement de spectre. D'autres contributions, telles que [39], [35], [40] convertissent la puissance du signal de brouillage en puissance de transmission utile pour charger des appareils légitimes. Suivant les concepts de la théorie des jeux, ils modélisent l'interaction entre une paire de nœuds légitimes et un perturbateur comme un jeu à somme nulle, et trouvent une solution optimale (c'est-à-dire une condition d'équilibre) qui minimise l'impact du perturbateur et maximise efficacement l'énergie de restauration. récupération sur des appareils légitimes. Cette contre-mesure permet aux utilisateurs secondaires des réseaux radio cognitifs de contrer les attaques de brouillage, réduisant ainsi l'impact des attaques. Les auteurs dans [41] proposent une solution aux attaques de brouillage dans

les systèmes en boucle fermée, en abordant le problème d'optimisation de l'allocation d'énergie. Une stratégie optimale d'allocation d'énergie acausale permet au système d'estimer l'état du processus de contrôle (à l'aide d'un filtre de Kalman) tout en garantissant la disponibilité et la stabilité. De même, les auteurs de [36] ont envisagé des méthodes d'alignement des interférences (c'est-à-dire des stratégies de formation de faisceaux) pour atténuer les interférences indésirables. L'objectif principal de la solution anti-brouillage est de créer une flotte de brouillage du réseau qui comprend certains appareils légitimes (par exemple, des émetteurs et des nœuds EH), tandis que le reste des nœuds est dédié à la mission EH. Sur les appareils compatibles,Le signal d'interférence et le signal de brouillage sont tous deux considérés comme des sources de RF EH.

2.9.8 Contre mesure contre les Attaques par inondation

Les auteurs ont proposé un schéma de protection dans [42] pour garantir la disponibilité du réseau en cas d'attaques par inondation dans les scénarios WSN.Plus précisément, ils utilisent les concepts EH et la théorie des processus de Markov pour identifier les attaques d'inondation en cours. Ils modélisent l'état du trafic réseau via un processus de Markov et fournissent une estimation de la chute de débit du nœud capteur lors d'une attaque par inondation, qu'ils comparent à un seuil. Plus le degré de dégradation est élevé, plus la probabilité d'inondation continue est élevée.

2.9.9 Contre mesure contre les attaques Dos

Pour contrer les attaques par déni de service (DoS), les auteurs de l'article [43] ont élaboré un cadre visant à repérer les nœuds dissimulés et malveillants qui délibérément émettent des paquets pour provoquer une perte intentionnelle de paquets au sein d'un réseau EH. Ils ont utilisé la métrique Taux de Remise de Paquets (PDR) ainsi qu'une approche adaptative d'accusé de réception (AAA) pour détecter ces attaques de collision dissimulées. Dans la méthode AAA, chaque nœud envoie un paquet de données, surveille la transmission suivante de son nœud voisin de premier saut, et attend l'accusé de réception de ce même nœud voisin pour le deuxième saut. Si cet accusé de réception n'est pas reçu pendant la fenêtre de synchronisation, cela indique une forte probabilité d'attaque.

changement de canal

Les auteurs [44] et [45] ont proposé des méthodes pour atténuer les attaques DoS en

transmettant les demandes de puissance d'un nœud EH vers un périphérique envoyant des demandes réseau. Plus précisément, ils ont développé un canal alternatif, le Power-Positive-Networking (PPN), où chaque signal reçu permet de charger la batterie de l'appareil. Étant donné que le concept de ces canaux alternatifs est très similaire à celui des réseaux SWIPT, ils arrêtent les attaques DoS liées à l'alimentation, car tout signal de brouillage qui interrompt la charge sans fil entraînera la charge de l'appareil EH.

2.10 Techniques de cryptoghraphie pour les dispositifs EH et les réseaux

Une branche cruciale des recherches en matière de sécurité pour les réseaux EH se concentre sur l'application des techniques de cryptographie aux dispositifs EH, en adaptant le fonctionnement et la mise en œuvre des mécanismes de sécurité à la nouvelle génération de systèmes. Plus précisément, les contributions scientifiques dans ce domaine visent à optimiser l'implémentation et l'architecture logicielle/matérielle des approches de cryptographie bien établies, en prenant en compte les caractéristiques et les exigences spécifiques des réseaux de récupération d'énergie. L'objectif ultime est de proposer des variantes personnalisées des techniques de cryptographie, caractérisées par une consommation d'énergie moins gourmande, afin de les intégrer efficacement dans des dispositifs alimentés par des sources d'énergie récoltée.

Comparées au grand nombre de contributions scientifiques qui examinent les problèmes de confidentialité des données au niveau de la couche physique, les approches de cryptographie peuvent assurer la spécificité des services de sécurité de manière déterministe, tandis que les approches au niveau des données de la couche physique se basent sur une approche probabiliste.

En ce qui concerne la sécurité, ces approches impliquent généralement une charge plus élevée pour le système, ce qui nécessite la mise en place de mécanismes d'optimisation dédiés. En effet, bien que chacune de ces propositions soit spécifiquement conçue pour une technique EH particulière, nous soutenons que la logique et les stratégies de ces propositions peuvent être pleinement réutilisées même pour d'autres sources d'énergie EH et d'autres réseaux.

Dans l'article [46], les auteurs ont examiné les stratégies d'optimisation de la consom-

mation d'énergie pour équilibrer le traitement de la sécurité et la quantité d'énergie récoltée. Étant donné que pendant les périodes de récolte RF, les dispositifs EH ne peuvent ni transmettre ni recevoir, et que la disponibilité de la source RF est intermittente (irrégulière), les auteurs ont comparé l'efficacité de la transmission de paquets plus petits ou moins longs. Ils ont également étudié l'exécution d'algorithmes de sécurité en tenant compte de la disponibilité de récolte des dispositifs.

En prenant en compte l'hétérogénéité des capacités de récolte dans les réseaux RF EH, les auteurs de l'article [47] ont développé HELIOS, un protocole distribué permettant aux éléments de réseau ayant une disponibilité énergétique faible d'externaliser les opérations les plus énergivores vers d'autres nœuds du réseau qui sont alimentés par un surplus d'énergie disponible. En considérant également la présence d'appareils non fiables dans le réseau, les auteurs ont discuté de stratégies spécifiques pour atténuer l'impact de ces éléments non fiables en utilisant des mécanismes de vérification par lots. Les auteurs ont prolongé leur étude dans [48], se concentrant sur le célèbre protocole d'algorithme de signature numérique à courbe elliptique, ECDSA.

2.11 Stratégies de Sécurité Adaptative et Optimisation Ressource-Contrainte dans les Réseaux de Capteurs Sans Fil

2.11.1 Adaptation du service de sécurité dynamique

Dans le contexte des dispositifs EH, cette approche vise à ajuster les mécanismes de sécurité en fonction des conditions changeantes du réseau et des besoins en matière de sécurité. L'objectif est de maximiser l'efficacité de ces mécanismes tout en réduisant au minimum leur impact sur les ressources, comme la puissance de calcul, la mémoire et l'énergie. Cette adaptation dynamique permet de maintenir un niveau de sécurité adéquat même lorsque les ressources sont limitées. Par exemple, lorsque les niveaux d'énergie diminuent, les mécanismes de sécurité peuvent être ajustés pour économiser de l'énergie tout en préservant une protection minimale essentielle. Cependant, il est important de noter que ces systèmes peuvent présenter des vulnérabilités face aux attaques de brouillage, car un adversaire pourrait potentiellement abaisser le profil de charge d'un dispositif pour

réduire le niveau de sécurité correspondant [3] .

2.11.2 Optimisation des opérations de sécurité

Dans la même optique que celle déjà utilisée dans des environnements contraints comme les réseaux de capteurs sans fil (WSN), d'autres contributions abordent les limitations énergétiques dans les réseaux EH en réduisant la consommation globale d'énergie des protocoles cryptographiques. Cette réduction est accomplie en externalisant les opérations de sécurité les plus exigeantes et en optimisant les coûts énergétiques de certaines opérations dans les chiffrements par blocs, parfois au détriment d'une réduction du niveau de sécurité. Toutefois, bien que moins exposées aux attaques de brouillage, ces stratégies sont souvent caractérisées par un niveau de sécurité réduit, ce qui les rend inadaptées aux scénarios de déploiement où un adversaire pourrait exploiter des capacités illimitées [3].

2.12 Pré-calcul pour optimiser la consommation d'énergie dans les réseaux EH

L'une des stratégies les plus efficaces pour assurer la sécurité dans les réseaux EH est le précalcul. Cette approche tire parti des périodes où les dispositifs sont pleinement alimentés pour anticiper et exécuter les tâches les plus énergivores. Bien que l'intégration de cette technique nécessite des efforts d'ingénierie significatifs au niveau des protocoles cryptographiques, les méthodes logiques de précalcul peuvent maintenir un niveau de sécurité similaire aux solutions établies, réussissant ainsi à temporairement contrer les attaques de brouillage et les adversaires puissants. Cependant, il y a deux limitations majeures à considérer. Premièrement, lorsqu'un appareil fait face à une période prolongée de disponibilité d'énergie réduite, les valeurs précalculées peuvent s'épuiser, laissant l'appareil sans ressources pour exécuter les tâches de sécurité. Deuxièmement, la conception des stratégies de précalcul doit être soumise à la validation de la communauté scientifique, afin d'éviter la création de vulnérabilités dans les techniques de cryptographie largement acceptées [3].

2.13 Conclusion

Dans ce chapitre, nous avons examiné de manière approfondie les enjeux essentiels de sécurité, les vulnérabilités potentielles et les stratégies associées à la technologie de récupération d'énergie par radiofréquence (RF) pour les dispositifs de récupération d'énergie sans fil (WAD). Notre analyse a débuté en fournissant une vue d'ensemble des concepts fondamentaux de la récupération d'énergie à partir des signaux RF, tout en mettant en lumière les architectures majeures des réseaux électromagnétiques sans fil. Ensuite, nous avons brièvement abordé la question de la sécurité dans le contexte spécifique des dispositifs WAD.

Après cette exploration des considérations sécuritaires, nous avons examiné diverses attaques qui pourraient potentiellement être exécutées dans cet écosystème. En outre, nous avons examiné en détail les techniques de cryptographie utilisées pour renforcer la sécurité de ces dispositifs. En fin de compte, notre attention s'est portée sur une solution particulière, conçue pour contrer une attaque spécifique que nous approfondirons davantage dans les sections à venir.

Ce chapitre offre ainsi une vue d'ensemble complète de l'intersection entre la récupération d'énergie RF et la sécurité des dispositifs WAD. Les informations présentées serviront de fondement solide pour explorer en profondeur les aspects spécifiques de la sécurité dans ce domaine, ainsi que pour développer des solutions pratiques visant à prévenir les attaques potentielles et à garantir l'intégrité et la confidentialité des données dans les réseaux IoT basés sur la récupération d'énergie.

Chapitre 3

Les réseaux de Petri stochastiques généralisés

3.1 Introduction

Les réseaux de Petri offrent une représentation claire et performante des systèmes parallèles. Cependant, l'utilisation d'un réseau de Petri simple ne permet qu'une évaluation qualitative, sans considération du temps. Pour obtenir une évaluation quantitative, l'introduction d'une dimension temporelle au modèle de base s'avère nécessaire. C'est pourquoi le modèle de réseau de Petri stochastique voit le jour, introduisant un délai de franchissement aléatoire pour chaque transition. En outre, les Réseaux de Petri Stochastiques Généralisés (RDPSG) élargissent encore davantage les possibilités des RDPS en intégrant des caractéristiques plus complexes, ce qui permet de modéliser des systèmes encore plus diversifiés et réalistes.

3.2 Les réseaux de Petri

Un réseau de Petri est un outil mathématique formel qui offre la possibilité de représenter graphiquement un système de contrôle, tout en fournissant un solide support pour l'analyse et la vérification de ce système. Ses principaux composants comprennent des places, des transitions et des arcs, tandis que l'état actuel du système est indiqué par un ou plusieurs jetons. Son principal avantage réside dans sa capacité à refléter de manière naturelle les relations de concurrence présentes dans le système modélisé.

3.3 Réseaux de Petri Stochastiques

3.3.1 Définition informelle

Les Réseaux de Petri Stochastiques sont une extension des Réseaux de Petri traditionnels, où des éléments probabilistes sont introduits pour prendre en compte l'aspect aléatoire du comportement des systèmes [49]. Ils permettent de modéliser des systèmes où les transitions entre les états ne sont pas déterministes, mais suivent des lois de probabilité, ce qui les rend adaptés à la modélisation de systèmes soumis à des variations aléatoires ou des incertitudes temporelles. En résumé, les Réseaux de Petri Stochastiques intègrent des aspects probabilistes pour rendre compte de la variabilité et de l'incertitude dans la dynamique des systèmes modélisés.

3.3.2 Définition formelle

Un réseau de Petri Stochastique (RdPS) est un quadruplet (P, T, I, λ), où [49] :

— P est un ensemble fini de places.
— T est un ensemble fini de transitions.
— I : P $\times$ T $\rightarrow \mathbb{N}$ est une fonction d'incidence, où N représente les nombres naturels, décrivant le poids de l'arc allant de chaque place à chaque transition.
— λ : T $\rightarrow \mathbb{R}^+$ (ensemble des nombres réels strictement positifs) est une fonction qui attribue à chaque transition un taux de déclenchement positif réel, représentant le taux auquel la transition est déclenchée.

Ce formalisme permet de modéliser des systèmes où les transitions se produisent de manière aléatoire en fonction des taux de déclenchement, suivant des lois de probabilité exponentielle, et où la quantité de travail nécessaire pour activer une transition peut également être aléatoire.

3.3.3 Représentation graphique de RdP

Un réseau de Petri est un modèle mathématique composé d'un ensemble fini de places (P), d'un ensemble fini de transitions (T), et d'un ensemble d'arcs orientés qui relient les places aux transitions (P $\rightarrow$ T) et les transitions aux places (T $\rightarrow$ P). Chaque arc repré-

sente une relation d'incidence entre une place et une transition, ou entre une transition et une place. Les transitions du réseau peuvent évoluer d'un état à un autre en consommant des jetons présents dans les places d'entrée et en produisant des jetons dans les places de sortie, suivant des règles définies par le modèle [50].

3.4 Notion de marquage

Chaque place contient un nombre entier positif ou nul de jetons. Le marquage M définit l'état du système décrit par le réseau à un instant précis. Il est présenté par un vecteur colonne ou la dimension est le nombre de places dans le réseau. Le i^{me} élement du vecteur correspond au nombre de jetons qui se trouvent dans la place P_i [51]. **exemple :** la figure

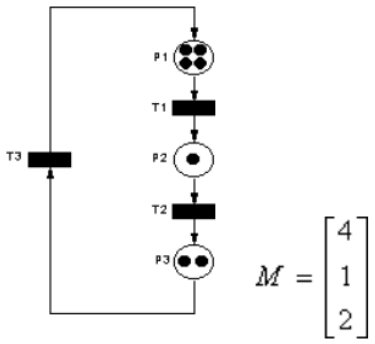

FIGURE 3.1 – Marquage d'un réseau de Petri

représente un réseau de petri marquée.
Les places P1,P2 et P3 contiennent des jetons
M0(P1)=4, est le nombre des jetons dans la place p1
M0(P2)=1, est le nombre des jetons dans la place p2
M0(P3)=2, est le nombre des jetons dans la place p3

3.5 Processus de marquage

Le marquage d'un Réseau de Petri Stochastique (RDPS) à l'instant t est représenté par le vecteur M(t), où chaque composante $M(p_i, t)$ correspond au marquage de la place p_i à l'instant t.
Pour une trajectoire $w = (X_0, t_0), ..., (X_n, t_n), ...$, le marquage atteint à l'instant t est

défini comme M(t, w), qui est également un vecteur avec des composantes M(p_i, t, w) pour chaque place p_i. Ce marquage à l'instant t est noté $X_n(w)$ pour tout t appartenant à l'intervalle $[t_n, t_n + 1]$.
L'ensemble des marquages à l'instant t forme un vecteur aléatoire N(t) qui dépend de la trajectoire w parcourant toutes les trajectoires possibles. Chaque composante de ce vecteur aléatoire, $M(p_i, t)$, représente une variable aléatoire indiquant le marquage de la place p_i à l'instant t.
La séquence de vecteurs aléatoires N(t) forme un processus aléatoire $M(t), t \geq 0$ appelé le processus de marquage. Ce processus de marquage représente l'évolution stochastique du marquage du RDPS au fil du temps, en tenant compte des transitions probabilistes et des différentes trajectoires possibles du système [51] [52].

3.6 Temps moyen de franchissement d'une transition

Le temps moyen de franchissement d'une transition, noté Tmft, est une variable aléatoire suivant une loi exponentielle. Il représente le temps attendu pour qu'une transition spécifique t soit franchie. Ce temps moyen est calculé à l'aide de la formule suivante : $Tmft = 1/\lambda_i(M_j)$. la formule précédente devient la suivante : $Tmft = 1/\lambda_i$, dans le cas ou les taux de franchissement des transitions sont indépendants du marquage.

Remarque : Lorsqu'il y a plusieurs transitions franchissables simultanément dans un réseau de Petri, la transition qui provoque le changement d'état du système est celle avec la durée de franchissement la plus courte parmi les transitions franchissables. Cette règle est importante pour déterminer la transition à exécuter lorsque plusieurs choix sont possibles [51], [52].

3.7 Règle de franchissement et graphe des marquages accessibles

3.7.1 Règle de franchissement

Une transition t est franchissable dans un marquage M si et seulement si : $\forall p \in P, M(p) \geq Pr(p, t)$. Le marquage M' obtenu après le franchissement de t est calculé par

la formule suivante :

$\forall p \in P, M'(p) = M(p)^{\smile} Pr(p,t) + Post(p,t)$[51][52].

Exemple 1 : T1 ne peut pas être franchissable car p2 ne contient aucun jeton

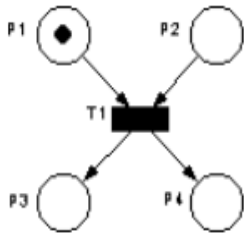

FIGURE 3.2 – Franchissement d'une transition

Exemple 2 : Le franchissement de la transition T1 implique la suppression d'un jeton

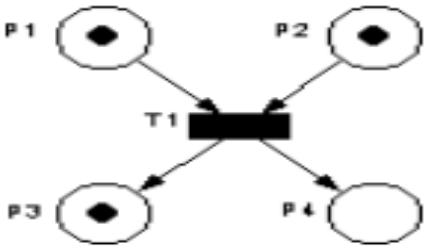

FIGURE 3.3 – Avant le franchissement d'une transition

de la place P1, la suppression d'un jeton de la place P2, ainsi que l'ajout d'un jeton dans la place P3 et d'un jeton dans la place P4.

La figure 3.4 représente le marquage M' obtenu après le franchissement de t est calculé par la formule suivante :

$$\forall p \in P, M'(p) = M(p)^{\smile} Pr(p,t) + Post(p,t);$$

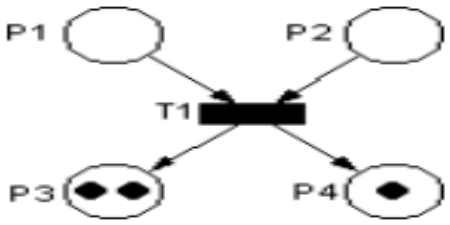

FIGURE 3.4 – exemple après le franchissement d'une transition

3.7.2 Graphe des marquages accessibles

.

— Marquage accessible : Soit un réseau marqué (R,Mo), un marquage M est dit accessible à partir du marquage initial M_0,
si et seulement si : $\exists S \in T * telque : Mo[S > M]$ (S étant une séquence de franchissement).

— Ensemble d'accessibilité : Soit (R,Mo) un RdP marqué. L'ensemble d'accessibilité noté A(R,Mo) est l'ensemble des marquages atteints ou accessibles par une séquence de franchissement depuis Mo [51] [52].
$A(R, Mo) = M/\exists S \in T * telque : Mo[S > M]$.
Cet ensemble, appelé "ensemble d'accessibilité", représente l'ensemble de tous les états possibles du système modélisé.

3.8 Temps moyen de séjour dans un marquage

Le temps moyen de séjour dans un marquage donné correspond à la durée de franchissement de la transition qui a provoqué le changement d'état. La valeur moyenne de ce temps de séjour est donnée par la formule ci-dessous [51] [52] : Tms $= 1/\sum \lambda_i(Mj)$i :t$_i \in E(M_j)$ où $E(M_j)$ est l'ensemble de toutes les transitions sensibilisées par le marquage M_j. Lorsque les taux de franchissement des transitions sont indépendants du marquage, la formule précédente devient : Tms $= 1/\sum \lambda_I telquei : t_i \in E(Mj)$

3.9 Analyse des RDPS

L'analyse des Réseaux de Petri Stochastiques (RDPS) comprend deux aspects essentiels. D'une part, il y a l'aspect qualitatif, qui consiste la vérification des propriétés structurelles du système modélisé. D'autre part, il y a l'aspect quantitatif, qui a pour objectif de calculer divers paramètres de performance pour évaluer le fonctionnement du système [51] [52].

3.9.1 Analyse qualitative

Dans cette section, l'objectif est d'examiner les propriétés qualitatives du système à analyser, telles que la vivacité, la bornitude, les états de blocage, etc. Il est important de noter que ces propriétés sont similaires à celles des Réseaux de Petri (RDP) simples et sont vérifiées de la même manière grâce à la correspondance entre le graphe des marquages accessibles d'un Réseau de Petri Stochastique (RDPS) et celui du RDP. Cependant, la différence clé réside dans le fait que les arcs du graphe des marquages accessibles d'un RDPS sont évalués en fonction des taux correspondant aux transitions. Cela signifie que les transitions dans le RDPS sont influencées par des taux stochastiques, ce qui peut avoir un impact significatif sur la dynamique du système par rapport à un RDP classique où les transitions sont déterministes. Par conséquent, l'analyse des propriétés qualitatives prend en compte cette composante stochastique pour évaluer la performance et le comportement du système [49, 51, 52].

Bornitude d'un réseau

L'évolution d'un réseau est caractérisée par différents états, également appelés marques d'accessibilité, que ce réseau peut atteindre. Si l'ensemble des marquages accessibles possibles qu'un Réseau de Petri (RdP) peut admettre est limité, on dit que le RdP est borné. La bornitude d'un RdP indique que le système ne peut pas atteindre un nombre infini d'états différents à partir de son état initial, ce qui est important pour l'analyse de la structure et du comportement du réseau. En d'autres termes, la bornitude signifie que le nombre d'états possibles est borné ou fini, ce qui peut avoir des implications importantes pour la gestion et la prévision du système modélisé.

Place borné

Une place p d'un réseau marqué $< R, Mo >$ est dite k-bornée ($k \in IN$) si pour tout marquage accessible$M \in A(R, Mo), onaM(p) \leq k$. Sinon, cette place est dite non bornée [52] .

Réseau borné

Si pour chaque place p du réseau, il existe un entier k tel que p soit k-bornée , le réseau marqué $< R, Mo >$ est dit borné.

3.9.2 La quasi-vivacité

Cette propriété indique la probabilité traverser chaque transition du réseau au moins une fois.

- Quasi-vivacité d'une transition : Soit (R,Mo) un RdP marqué. Une transition t de ce réseau est dite quasi-vivante s' il existe un marquage accessible M∈A(R,Mo) tel que M[t>.
- Quasi-vivacité d'un réseau : Un réseau de Petri <R, Mo> est quasi-vivant si : $\forall t \in T, \exists M \in A(R, Mo) tq : M[t >$. Si le réseau n'est pas quasi-vivant, alors il y a une transition t qui n'est jamais franchissable et par conséquent ne sont pas utile au fonctionnement du système modélisé.

La pseudo-vivacité

Est une propriété qui indique qu'à partir de n'importe quel marquage accessible dans un Réseau de Petri (RdP), il existe au moins une transition qui peut être activée. En d'autres termes, il y a toujours au moins une possibilité d'évolution ou d'action à partir de chaque état du système, garantissant ainsi une certaine dynamique dans le réseau [52]. Un RdP (R,Mo) est pseudo- vivant si : $\forall M \; inA(R, Mo)$, $\exists t \in T$ tq M[t >.

La vivacité

Cette propriété est fortement rattacher à la situation de blocage .Un RdP qui modélise un système non bloquant, doit être vivant. Cela signifie que pour tous les marquages

accessibles depuis Mo, n'importe quelle transition peut être franchit en procédant le long d'une séquence de franchissement [52].

Les Réseaux de Petri à arcs inhibiteurs (ou "Réseaux de Petri avec arcs inhibiteurs") sont une extension des Réseaux de Petri classiques qui permettent de modéliser des relations de type "empêchement" entre des places et des transitions. Dans un Réseau de Petri standard, une place doit contenir un certain nombre de jetons pour activer une transition. Cependant, dans un Réseau de Petri à arcs inhibiteurs, des arcs inhibiteurs spéciaux indiquent que la présence de jetons dans certaines places peut empêcher une transition de se déclencher.

3.9.3 Arc inhibiteur

Les arcs inhibiteurs sont représentés par des flèches en pointillés (ou d'une manière similaire) entre des places et des transitions. Ils indiquent que la présence de jetons dans une place donnée peut empêcher le déclenchement d'une transition, même si les autres conditions sont remplies [51, 52].

3.10 Réseaux de Petri stochastiques généralisés (RDPSG)

3.10.1 Définition

Les Réseaux de Petri Stochastiques Généralisés (RDPSG) sont un outil d'analyse des performances basé sur la représentation graphique des Réseaux de Petri classiques [51, 52]. Dans ces réseaux, certaines transitions sont soumises à une temporisation, tandis que d'autres peuvent se produire instantanément. Les transitions temporisées sont associées à des retards de déclenchement aléatoires suivant une distribution exponentielle, ce qui signifie que le moment de leur déclenchement est stochastique. En revanche, les transitions immédiates s'activent instantanément, sans délai. Il convient de noter que, dans les RDPSG, les transitions immédiates ont la priorité sur les transitions temporisées. Ainsi, si une transition immédiate est prête à être déclenchée, elle sera exécutée immédiatement, même si une transition temporisée est en attente. Les RDPSG sont utilisés pour modéliser et analyser des systèmes où les événements peuvent se produire avec des délais aléatoires, une situation courante dans de nombreuses applications réelles. Ils permettent de tenir

compte de la variabilité temporelle dans les processus et de calculer divers paramètres de performance, tels que les temps de réponse, les débits, les taux de congestion, etc. En conséquence, ils sont un outil précieux pour l'analyse et l'optimisation des systèmes soumis à des incertitudes temporelles [53].

3.10.2 Transitions temporisées

Ces transitions sont associées à une variable aléatoire qui détermine la durée de leur franchissement. La période de franchissement peut varier en fonction des valeurs aléatoires générées par cette variable. Ces transitions ne se produisent pas instantanément, car leur déclenchement est soumis à des délais aléatoires [51, 52].

3.10.3 Transitions immédiates (instantanées)

Ces transitions se caractérisent par le fait que leur période de franchissement est plus courte que celle des transitions temporisées. En réalité, elles ont un taux de franchissement associé infini, ce qui signifie que leur déclenchement est instantané dès que toutes les conditions sont remplies. En d'autres termes, il n'y a pas de délai de tir pour ces transitions [51, 52].

3.10.4 Analyse de performance des RDPSG

L'analyse de performance des Réseaux de Petri Stochastiques Généralisés (RDPSG) est une étape cruciale pour évaluer le comportement et les caractéristiques de performance des systèmes modélisés à l'aide de cette approche. Elle permet de quantifier et d'optimiser divers aspects du système, tels que la fiabilité, la disponibilité, les temps de réponse, les taux de congestion, etc. Voici quelques points clés concernant l'analyse de performance des RDPSG [51, 52] :

- **Simulation Stochastique :** L'analyse de performance des RDPSG implique souvent l'utilisation de simulations stochastiques. Ces simulations génèrent des résultats basés sur des échantillons aléatoires des variables aléatoires associées aux transitions temporisées. Les simulations permettent d'obtenir des estimations probabilistes des performances du système.
- **Collecte de Données :** Pour effectuer une analyse de performance, il est souvent

nécessaire de collecter des données sur le système réel ou sur le modèle RDPSG. Cela peut inclure des données sur les délais de déclenchement, les taux de franchissement, les temps d'arrêt, etc.

— **Paramètres de Performance :** Les paramètres de performance spécifiques à analyser dépendent des objectifs du modèle RDPSG et du système étudié. Par exemple, on peut s'intéresser au temps moyen de réponse, à la probabilité de congestion, au taux de disponibilité, au débit maximal, etc.

— **Méthodes Analytiques :** En plus des simulations, des méthodes analytiques peuvent être utilisées pour résoudre mathématiquement des modèles RDPSG et obtenir des expressions analytiques pour les paramètres de performance. Ces méthodes sont particulièrement utiles pour des modèles simples et bien définis.

— **Comparaisons et Optimisation :** L'analyse de performance permet de comparer différentes configurations de systèmes, de modèles RDPSG ou de politiques de gestion. Elle permet également d'optimiser ces systèmes en identifiant les paramètres qui maximisent ou minimisent les performances souhaitées.

— **Sensibilité aux Paramètres :** Il est courant d'analyser la sensibilité des performances par rapport aux paramètres du modèle RDPSG. Cela permet de comprendre comment les variations des paramètres affectent les résultats de performance.

— **Validation :** L'analyse de performance des RDPSG doit être validée pour s'assurer que les résultats reflètent fidèlement le comportement du système réel. Cela peut impliquer la comparaison des résultats de simulation avec des données réelles si disponibles.

— **Interprétation des Résultats :** Enfin, les résultats de l'analyse de performance doivent être interprétés et présentés de manière à fournir des informations utiles aux décideurs. Des graphiques, des rapports et des conclusions claires sont souvent nécessaires.

L'analyse de performance des RDPSG joue un rôle essentiel dans la compréhension et l'optimisation des systèmes stochastiques. Elle permet aux ingénieurs et aux chercheurs de prendre des décisions éclairées en matière de conception, de gestion et d'amélioration de systèmes complexes.

3.11 Conclusion

En conclusion, les Réseaux de Petri (RdP) sont un formalisme puissant pour la modélisation et l'analyse de systèmes complexes, en particulier lorsqu'il s'agit de traiter des problématiques liées à la concurrence, la synchronisation et le parallélisme. Ils offrent un cadre structuré pour spécifier le comportement des systèmes et permettent de mettre en évidence des propriétés importantes.

Les Réseaux de Petri Stochastiques Généralisés (RDPSG) élargissent encore d'avantage la capacité des RDPS en intégrant des caractéristiques plus complexes et en permettant de modéliser des systèmes encore plus diversifiés et réalistes.

Chapitre 4

Modélisation des appareils autonomes à RF-EH et sécurité de niveau physique dans le contexte d'IoT

4.1 Introduction

Dans le domaine des réseaux de capteurs sans fil avec récolte d'énergie (RCSFs) au sein de l'Internet des Objets, l'évaluation des performances et la garantie de la sécurité au niveau physique sont des enjeux cruciaux. Ce chapitre constitue une plongée approfondie dans ces aspects essentiels, visant à fournir une compréhension approfondie de la manière dont les RCSFs peuvent fonctionner de manière optimale et sécurisée dans un environnement exigeant. En parallèle, les réseaux de Petri sont fréquemment utilisés en tant qu'outils de modélisation au sein du domaine des systèmes de réseaux, offrant une évaluation préalable des performances avant leur déploiement concret.

4.2 Travaux connexes

Les réseaux de Petri sont largement utilisés comme outil de modélisation dans le domaine des réseaux informatiques pour évaluer leur comportement avant leur mise en place effective.

Bachira BOUTOUMI et Nawel GHARBI dans [54] ont présenté une technique visant à économiser l'énergie et à améliorer l'efficacité de la latence pour les nœuds de capteurs

sans fil full-duplex munis d'un tampon fini. Ils ont proposé une combinaison de vacances normales et d'une politique de vacances-travail à deux seuils (N1, N2) différents pour basculer le serveur de l'état inactif (état vacances ordinaire) à l'état semi-occupé (état vacances de travail), lorsque la taille de son tampon atteint le seuil N2. Cette transition déclenche la transmission des paquets en file d'attente à un taux réduit. Lorsque la taille du tampon atteint le seuil N1, le serveur passe à l'état occupé (état de service) avec un taux de transmission normal. Lorsque le tampon est vidé, l'état inactif est rétabli. L'utilisation des réseaux de Pétri stochastiques généralisés pour analyser les performances du modèle a démontré que la politique de vacances de travail à deux seuils est la plus efficace pour prolonger la durée de vie d'un capteur, réduire le délai de latence et minimiser la probabilité de blocage.

Patrick Wuchner et al [55] ont proposé une modélisation réseau de Petri pour un capteur communiquant avec ses voisins. Ils ont étudié le système en termes de temps de réponse moyen en prenant en compte l'orbite non fiable, mais n'ont pas inclus la modélisation de la batterie.

Oukas Nourredine et Boulif Menouar ont abordé une approche relativement peu explorée dans la littérature, comme détaillé dans leur travail [56]. Ils ont introduit une modélisation novatrice basée sur les réseaux de Petri stochastiques généralisés pour le processus de charge/décharge des batteries des capteurs au sein d'un RCSF avec capacité de récupération d'énergie renouvelable.

Dans leur démarche, les auteurs ont mis en œuvre un mécanisme de sommeil et ont appliqué le principe de quantification pour gérer la consommation d'énergie. Cette gestion est réalisée en utilisant des quantités discrètes, permettant ainsi aux capteurs de passer du mode actif ou d'écoute en mode veille lorsque le niveau quantique de la batterie descend en dessous d'un seuil préétabli. Cette stratégie permet d'économiser l'énergie et de l'augmenter par le biais de la capacité de récupération. Le modèle qu'ils ont développé s'est avéré capable de prédire avec précision le niveau moyen d'énergie de la batterie ainsi que le temps de réponse moyen, ce qui contribue à assurer la continuité du service au sein de l'ensemble du RCSF. En intégrant ces éléments, leur approche offre une méthodologie prometteuse pour optimiser l'utilisation de l'énergie dans le contexte des capteurs autonomes et des réseaux avec capacité de récupération d'énergie renouvelable.

Les auteurs de [18], ont élaboré une modélisation qui prend en compte le trafic de

communication des capteurs, la relation entre les voisins et l'état de la batterie au sein des réseaux de capteurs sans fil. Les opérations telles que l'émission, la réception, la détection et le traitement sont considérées comme des sources de consommation d'énergie. Les dispositifs considérés sont équipés de capteurs d'énergie solaire.

Dans [6], Oukas et al. ont introduit un modèle visant à simuler le comportement des batteries de dispositifs interactifs avec un réseau. Ce modèle intègre un mécanisme de veille sophistiqué pour anticiper le niveau de charge des batteries avant leur déploiement opérationnel. La méthode repose sur la formulation des réseaux de Pétri stochastiques généralisés pour évaluer les performances des AWD (Autonomous Wireless Devices) au sein de l'Internet des objets . Les chercheurs considèrent des AWD équipés à la fois d'un récepteur et d'un émetteur d'énergie rayonnante. Ces dispositifs jouent un rôle double en transmettant à la fois des informations et de l'énergie à leurs voisins. Le modèle intègre un mécanisme de veille sophistiqué, ce qui permet aux dispositifs d'ajuster leur consommation d'énergie de manière optimale en fonction des besoins du réseau. En utilisant cette approche novatrice, les chercheurs ont cherché à optimiser l'utilisation de l'énergie dans le contexte des dispositifs autonomes sans fil, tout en garantissant une communication efficace et une alimentation adéquate au sein de l'écosystème de l'IoT.

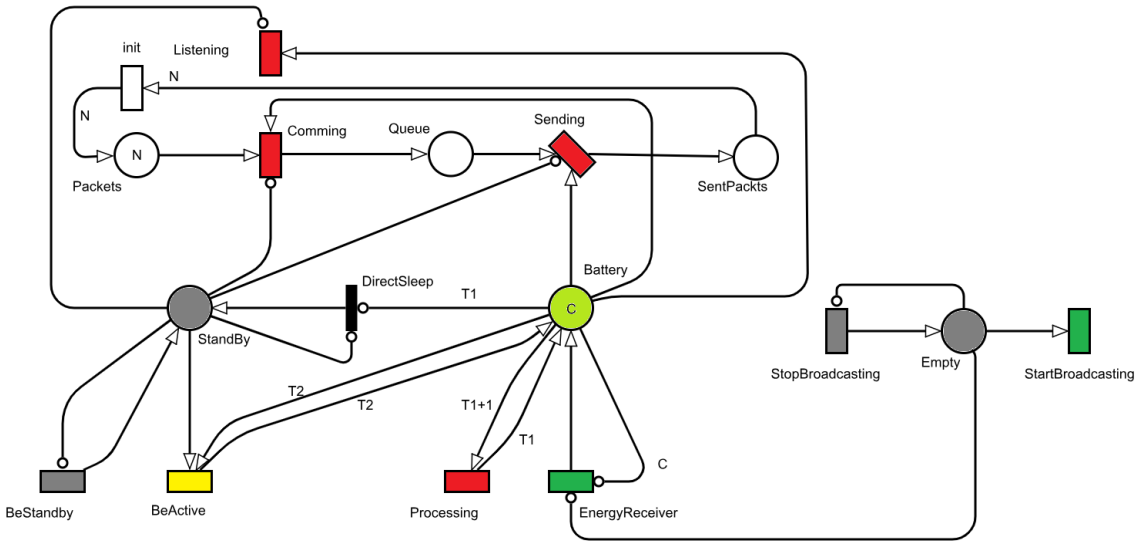

FIGURE 4.1 – Modèle basé sur les RdPSG pour un appareil RF-EH [6]

Dans [19], les auteurs proposent une amélioration du modèle [56]. Ils présentent une nouvelle modélisation GSPN qui prend en compte différents taux d'EH (Énergie Harvesting) pour la récolte d'énergie saisonnière, en raison de la disparité des niveaux d'ensoleillement.

Oukas et al. ont présenté dans [7] un modèle GSPN destiné aux dispositifs sans fil autonomes dans l'Internet des objets (see Figure 4.2). Les auteurs abordent le scénario où la récupération d'énergie RF est utilisée pour recharger les batteries à distance, tout en prenant en compte les attaques de brouillage. Dans ce contexte, un attaquant peut perturber le signal électromagnétique transportant l'information, ce qui ralentit le dispositif en raison de la réception de paquets erronés. Cela peut conduire à une surconsommation d'énergie, épuisant ainsi la batterie. L'évaluation des performances de tels dispositifs dans de telles circonstances, sans recourir à des dépenses excessives, nécessite la mise en place d'une modélisation et/ou d'une simulation. Les auteurs ont mené une analyse expérimentale pour démontrer que le modèle qu'ils proposent est capable d'évaluer les performances de ces dispositifs, de prédire leur comportement et ce, sans nécessiter un déploiement réel. Table 4.1 présente une comparaison entre les travaux connexes précédents.

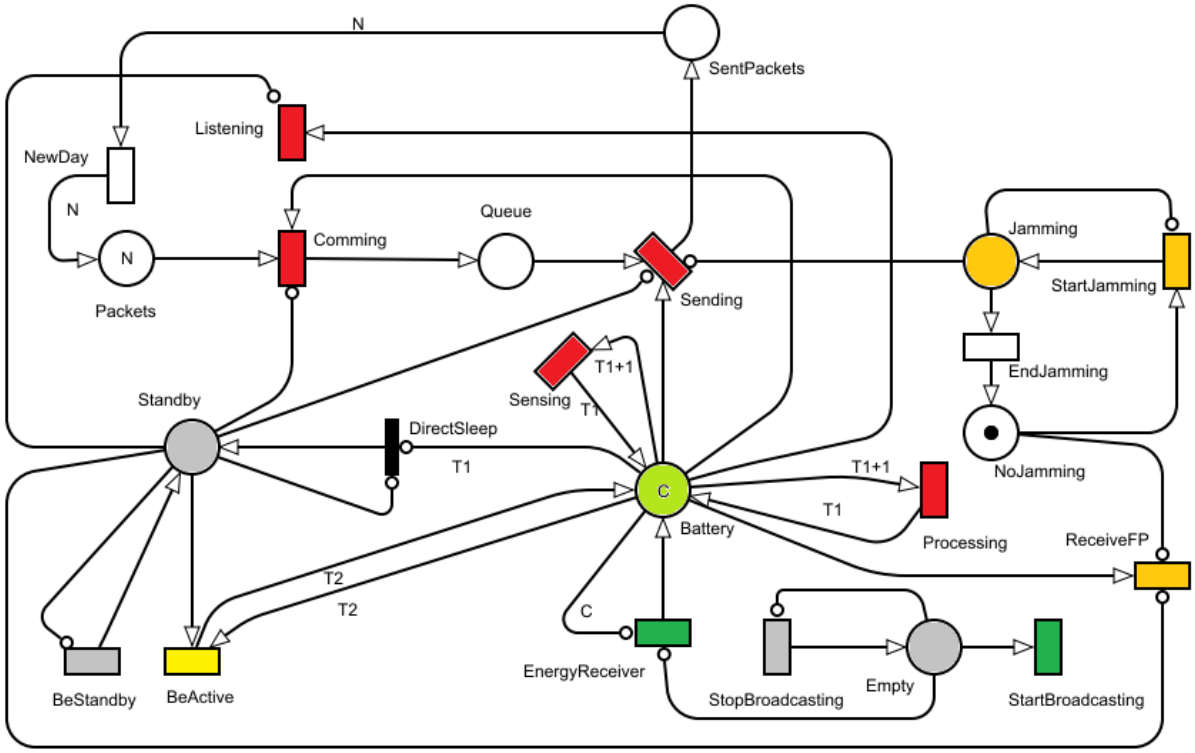

FIGURE 4.2 – Modélisation basée sur les RdPSG pour un RF-EH-AWD en présence d'une attaque de brouillage [7]

TABLE 4.1 – Comparaison entre les modèles des travaux connexes (Com. : Communication avec les voisins ; Form. : Formalisme de modélisation)

Réf.	Form.	Com.	Contraintes			Metrics
			EH	Sécurité	Attaque	
[54]	GSPN	oui		×		latence, énergie
[55]	GSPN	oui	×			énergie
[56]	GSPN	oui	×			énergie
[18]	GSPN	oui	×			énergie
[19]	GSPN	oui	×			énergie et pourcentage de sommeil
[7]	GSPN	oui	×	×	×	énergie , latence
[notre]	GSPN	oui	×	×	×	énergie , latence et pourcentage de sommeil

4.3 Approche proposée

Notre étude élargit les travaux présentés dans [7] en fournissant une description plus réaliste du système. Notre approche proposée vise à améliorer le modèle en intégrant une solution de sécurité contre les attaques de brouillage et DoS.

4.3.1 Description du Modèle

La Figure 4.3 représente un modèle basé sur les RdPSGs pour un RF-EH AWD avec une solution de sécurité au niveau physique repose sur l'utilisation du changement de canal. Équipé d'un système de recharge à distance avec une antenne de réception. Toutes les places du modèle sont expliquées dans la Table 4.2. Toutes les transitions du modèle sont décrites dans la Table 4.3.

Les transitions Comming, Sending, Sensing, Listening et Processing sont les opérations de base d'un appareil consommateur d'énergie. Un nœud servir N paquets par jour. La place packets contient les paquets quotidiens. Lorsqu'un paquet est reçu, il est stocké dans un tampon. La transmission (Sending) démarre lorsque la batterie est chargée et que

l'appareil est actif. De plus, un mécanisme de veille surveille l'alimentation de l'appareil. Ainsi, l'appareil passe périodiquement à l'état de veille (représenté par la présence d'un jeton à la place Standby). Le mécanisme accepté force l'appareil à se mettre en veille dès que la quantité d'énergie atteint le niveau T1 (transition DirectSleep). Le nœud reste jusqu'à ce que la charge de la batterie soit supérieure ou égale au seuil T2 (transition BeActive). De plus, les attaques de brouillage peuvent toucher des appareils autonomes. Les événements liés au processus de brouillage sont régis par des lois de probabilité appropriée (transitions StartJamming et EndJamming). La rénitialisation en mode normal est indiquée par la présence d'un jeton à la place de NoJamming. Un attaquant envoie de faux signaux pour provoquer un déni de service en vidant la batterie du réseau. StartJamming démarre le jeton au point de brouillage, l'appareil ne peut pas envoyer ses paquets (par le canal de *Sending*). Pendant ce temps, l'appareil perd de l'alimentation en raison de la réception des faux paquets (Transition ReceiverFP). l'apprail réalise un traitement pour changer le canal (ChannelChanging), qui est affecté par l'attaque. En même temps l'appareil établi un canal alternatif (AlternatifSending). Enfin quand on change le canal, le modèle est initie par deux transition une transition ReceiveFP sert a charger la batterie seulement et AlternatifSending pour envoyer les paquets.

TABLE 4.2 – Description des places du modèle

Place	**Description**	**Marquage initiale**
Packets	Contient des paquets hebdomadaires	N
Queue	Mémoire trompons de l'appareil	0
SentPackets	Paquets transmis	0
StandBy	État de veille	0
Battery	Batterie de l'appareil	C
Empty	RF-EH	0
Jamming	Indicateur de présence de brouillage	0
NoJamming	Indicateur d'absence de brouillage	0
ChanalChanging	changement de canal	1

TABLE 4.3 – Description des transitions du modèle

Transition	**Description**	**Paramètre**
Listening	Écouter le canal	1/listen_r
Comming	AWD reçoit un message	receive_d
BeActive	Activation intégrale reste éveillée	DSleep_d
BeStandby	AWD rejoint l'état active	DAwake_d
NewDay	initialisation du modèle pour une nouvelle journée	init_ d
Sensing	Surveiller l'environnement	1/work_r
Sending	Transmettre un paquet	send_d
StartBroadcasting	Démarrer la diffusion d'énergie RF	noEnergy_d
StopBroadcasting	Arrêter la diffusion d'énergie	energy_d
StartJamming	attaque par brouillage se produit	Sjamming_d
EndJamming	Fin de l'attaque de brouillage	jamming_d
Processing	Consommateur de CPU	1/work_r
ReceiveFP	Recevoir des faux paquets	receiveFP_d
AttackTreatement	traite l'attaque	/
RFEHarvesting	Rechargement de la batterie	1/harvest_r
AlternatifSendig	Transmettre un paquet sur un canal alternatif	/

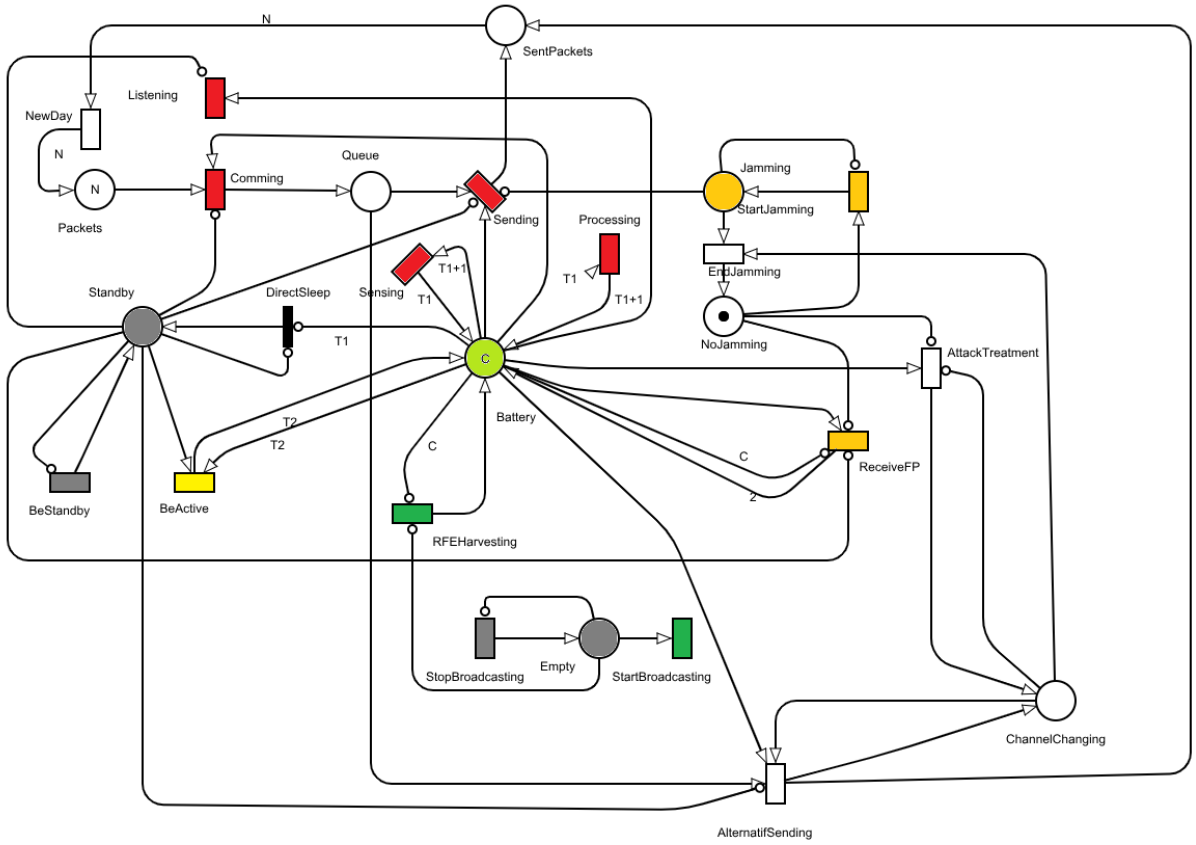

FIGURE 4.3 – Modèle basé sur le changement de canal pour contrer les attaques de brouillage.

En fin, le modèle proposée est basé sur le changement de canal pour les attaques de brouillage, cette méthode est déjà mentionné dans le chapitre 2.9.9. Cette solution vis à :

— Sauver la batterie.

— Recharger la batterie via le signal d'attaque.

— Continuer de transmettre des paquets via le canal alternatif.

4.4 Conclusion

Notre avons commencé par une exploration des travaux connexes, nous permettant de situer nos recherches au sein du paysage scientifique actuel. Cette revue de littérature a mis en lumière les multiples approches adoptées pour préserver la batterie et garantir une efficacité optimale dans les réseaux des objets autonomes, tout en rehaussant leur sécurité face aux attaques de brouillage.

Cette évaluation approfondie nous a permis de mettre en avant les avantages distinctifs de notre approche, notamment en termes de gestion de l'énergie par le biais du changement de canal, et ce grâce à l'intégration d'un réseau de Petri stochastique généralisé, ce qui s'avère être une stratégie prometteuse pour contrer les attaques de brouillage. L'étape cruciale de notre exploration a été l'analyse comparative des modèles existants et de nos propositions innovantes. Cette analyse a mis en avant les avantages distincts de notre approche, en particulier en termes de gestion énergétique via le changement de canal.

Dans le chapitre suivant, nous allons détailler évaluer les performances de l'approche proposée.

Chapitre 5

Évaluation des performances

5.1 Introduction

Dans ce chapitre, nous présentons une évaluation des performances par simulation des solutions proposées dans le chapitre 04, dans le but de démontrer la capacité des modèles proposés à anticiper le comportement d'un RCSFs avant son déploiement réel, ainsi que l'efficacité de nos approches pour assurer une gestion efficace de l'énergie.

Pour ce faire, nous alimentons les modèles avec des valeurs réelles de différents paramètres d'entrée. Les résultats obtenus sont minutieusement analysés, en mettant particulièrement l'accent sur le niveau de la batterie, exprimé en pourcentage d'énergie résiduelle par rapport à l'énergie initiale. Toute l'analyse est conduite dans l'environnement TimeNet 4.5 . Le choix de cet outil permet d'évaluer les performances d'un modèle hybride de manière précise et informative.

5.2 Outil logiciel

5.2.1 Description du logiciel TimeNet 4.5

TimeNet 4.5 est un logiciel de modélisation et de simulation basé sur des réseaux de Petri temporels et stochastiques. Il permet de créer et d'analyser des systèmes complexes en intégrant des aspects temporels et probabilistes. Les utilisateurs peuvent concevoir des modèles graphiques représentant les relations entre les éléments du système, puis effectuer des simulations pour évaluer les performances du système en utilisant des paramètres de temps, de probabilité et d'autres facteurs. TimeNet 4.5 est un outil essentiel pour les

professionnels et chercheurs travaillant sur la conception et l'optimisation de systèmes variés [57].

5.2.2 Fonctionnalités du TimeNet 4.5

TimeNet 4.5 est un logiciel de pointe pour la modélisation, l'analyse et la simulation de systèmes complexes à l'aide de réseaux de Petri temporels et stochastiques. Ses fonctionnalités clés incluent la modélisation graphique, la prise en compte du temps et de la probabilité, la simulation avancée avec des paramètres personnalisables, l'analyse des performances, la visualisation des résultats, la génération de rapports détaillés et l'utilisation de modèles prédéfinis. Le logiciel offre une interface conviviale et est largement utilisé dans la recherche et l'optimisation de systèmes variés. L'outil est disponible gratuitement pour une utilisation non commerciale, telle que dans un cadre pédagogique, pour des mémoires de master, des projets de recherche scientifique ou académique, ou à des fins personnelles. Cependant, les entreprises ou les individus souhaitant utiliser l'outil dans un contexte commercial ou pour des projets payants doivent contacter Armin Zimmermann pour obtenir une licence appropriée.

5.2.3 Interface graphique du TimeNet 4.5

La nouvelle version de TimeNet présente une interface graphique interactive développée en utilisant le langage JAVA, et elle est compatible avec le système d'exploitation Windows. Cette interface graphique générique de TimeNet 4.5 offre la possibilité de visualiser les résultats des évaluations et des analyses sous forme de graphiques. La fenêtre de l'interface graphique de TimeNet 4.5 est divisée en quatre sections distinctes, comme illustré dans la Figure 5.1 :

— Une barre de menu en haut.
— Une zone de dessin à gauche.
— Une zone des attributs à droite.
— Une barre d'outils spécifique à la classe du RDP en bas.

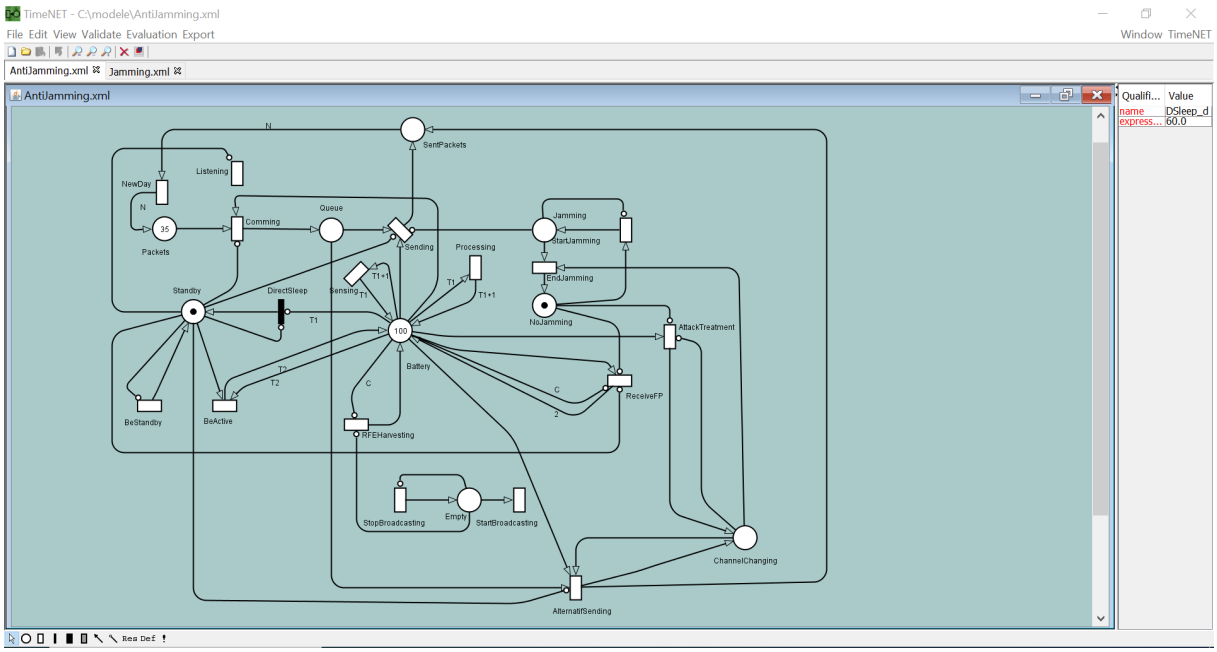

FIGURE 5.1 – Interface graphique du TimeNet 4.5 sous Windows

5.2.4 Les méthodes d'analyse de TimeNet 4.5

Le menu Évaluation de l'interface graphique nous permet d'accéder aux fonctions d'évaluation de performance du modèle. Plusieurs méthodes d'évaluation sont disponibles, nous citons :

— L'analyse stationnaire.

— La simulation stationnaire.

— L'analyse transitoire.

— La simulation transitoire.

5.3 Paramètres de simulation

Afin de démontrer la validité du modèle proposé et d'évaluer les performances du réseau, nous avons employé l'outil TimeNet pour mener une analyse stationnaire et différentes simulations. Pour cela, nous avons modifié certains paramètres d'entrée, tels que le nombre de messages, le délai de brouillage (c'est-à-dire la durée de l'attaque de brouillage) ainsi que le taux de récupération d'énergie. D'autres paramètres ont également été pris en considération pour cette analyse. Les valeurs adoptées dans cette étude sont présentées dans le tableau 5.1.

TABLE 5.1 – Valeur des paramètres d'entrées

Paramètre	**Valeur**	**Explication**
N	20	Nombre de message hebdomadaire
C	100	La capacité de la batterie
T1	10	Seuil
T2	40	Dormir à seuil élevé
DAwake_d	60s	Délai d'activation
DSleep_d	60s	Délai de veille
Jamming_d	600	Repos avant l'attaque de brouillage
SJamming_d	600	Durée de l'attaque de brouillage

5.4 Étude expérimentale

La Table 5.2 décrit les modèles considérés pour l'étude comparative.

TABLE 5.2 – Les modèles a comparées

Modèle	**référence**	**Explication**
RFBattery	[6]	Modèle GSPN pour les appareils sans fil autonomes avec RF-EH sans considération de l'aspect sécurité
Jamming	[7]	Modèle GSPN pour les appareils sans fil autonomes avec attaque de brouillage
AntiJamming	[this]	Modèle GSPN pour les appareils sans fil autonomes avec une solution au niveaux physique d'anti-brouillage

5.4.1 Comparaison des modèles par rapport au nombre de paquets hebdomadaire

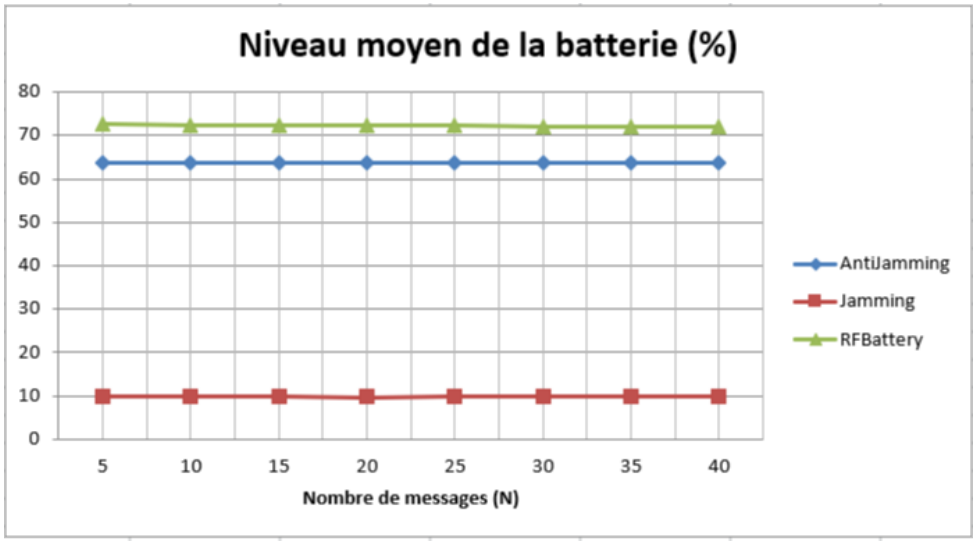

FIGURE 5.2 – Niveau moyen de la Batterie par rapport au nombre de Message

La Figure 5.2 représentent le niveau moyen de la batterie par rapport au nombre de messages (N). Ce graphe présente une comparaison, en termes de niveau de consommation de la batterie par rapport au nombre de messages, entre trois modèles : Antijamming, jamming et RFBattery. On observe que pour le modèle "jamming", qui ne contient aucune solution de sécurité, son niveau de batterie est toujours bas (10%) à cause de l'attaque qui provoque l'envoi de faux paquets et, par conséquent, une perturbation du canal, entraînant ainsi une consommation importante de l'énergie dela batterie. En ce qui concerne le modèle "RFBattery", on remarque que le niveau de batterie reste toujours élevé (70%) quel que soit le nombre de messages. Cependant, il est important de noter que ce modèle ne comporte pas de protection contre les attaques, ce qui le rend peu réaliste. Quant au modèle "Antijaming", il se maintient dans la médiane en ce qui concerne la consommation de la batterie. Malgré l'augmentation du nombre de messages, le niveau de batterie reste stable, dépassant les 60%. Cela suggère que le modèle "Antijaming" est le plus adaptable parmi les trois modèles comparés.

La Figure 5.3 présente une comparaison entre trois modèles que nous avons précédemment étudiés, en examinant le pourcentage de temps de sommeil par rapport au nombre de messages. On remarque que le modèle "jaming" affiche le pourcentage de sommeil le plus élevé, principalement en raison d'attaques subies. Étant donné que ce modèle ne dispose pas de mesures de défense, il consomme une quantité significative d'énergie. En conséquence, le niveau de la batterie chute en dessous d'un seuil critique, ce qui entraîne

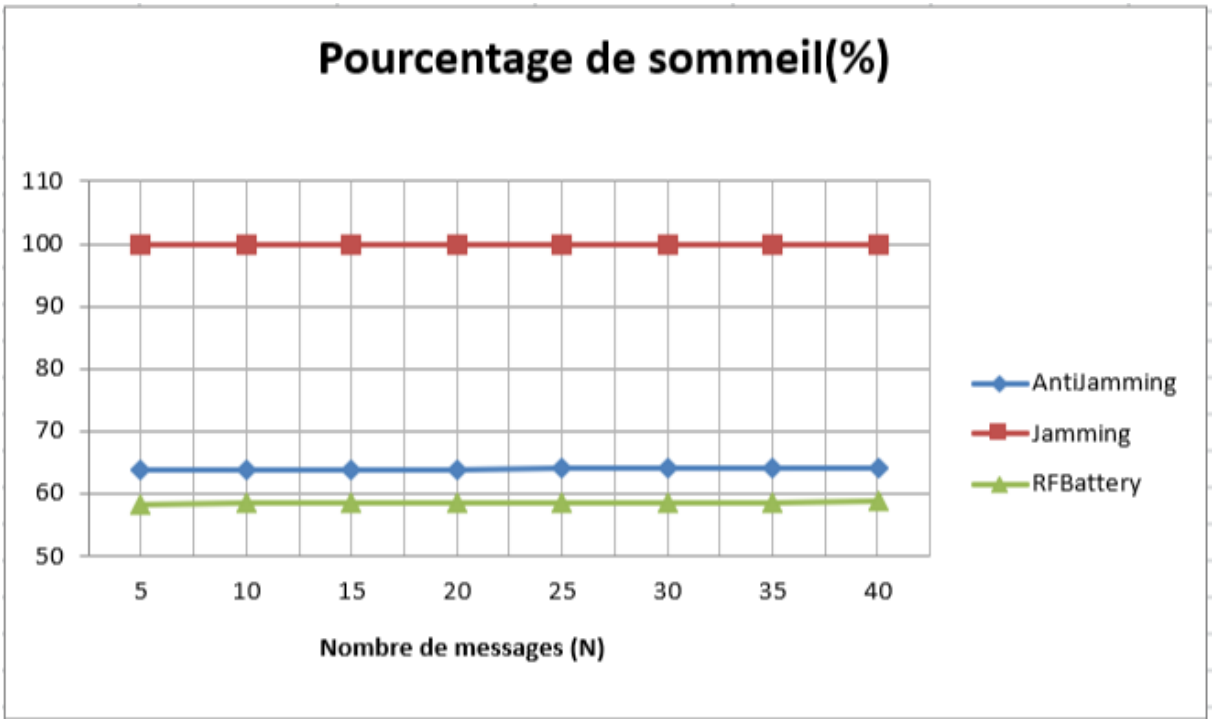

FIGURE 5.3 – Pourcentage de sommeil par rapport au nombre de Message (N)

l'arrêt du système. Les modèles "AntiJamming" et "RFBattery" se distinguent par leur capacité à maintenir un état actif plus stable. En ce qui concerne "AntiJamming", peu importe le nombre de messages, son pourcentage de sommeil reste constant à un niveau élevé (plus de 60%). Ce modèle utilise une technique de récolte d'énergie par radiofréquence en conjonction avec des contre-mesures efficaces pour faire face aux attaques. En conséquence, il parvient à maintenir une disponibilité constante sans être affecté par les tentatives d'attaque. Quant au modèle "RFBattery", il présente également une stabilité notable en ce qui concerne la période de sommeil. Cela peut s'expliquer par sa capacité à optimiser l'utilisation de l'énergie de manière efficace, évitant ainsi que le niveau de la batterie ne chute en dessous du seuil critique, ce qui prévient l'endormissement du modèle.

AntiJaming est donc plus résilient face aux attaques et plus efficaces dans la gestion de sa consommation d'énergie, ce qui le rend plus fiables dans des environnements sujets aux attaques.

La Figure 5.4 présente les temps de réponse de trois modèles en fonction du nombre de messages. Pour le modèle de brouillage "Jamming", le temps de réponse est légèrement lent, mais il reste stable à environ 8 unités. En revanche, les modèles "AntiJamming" et

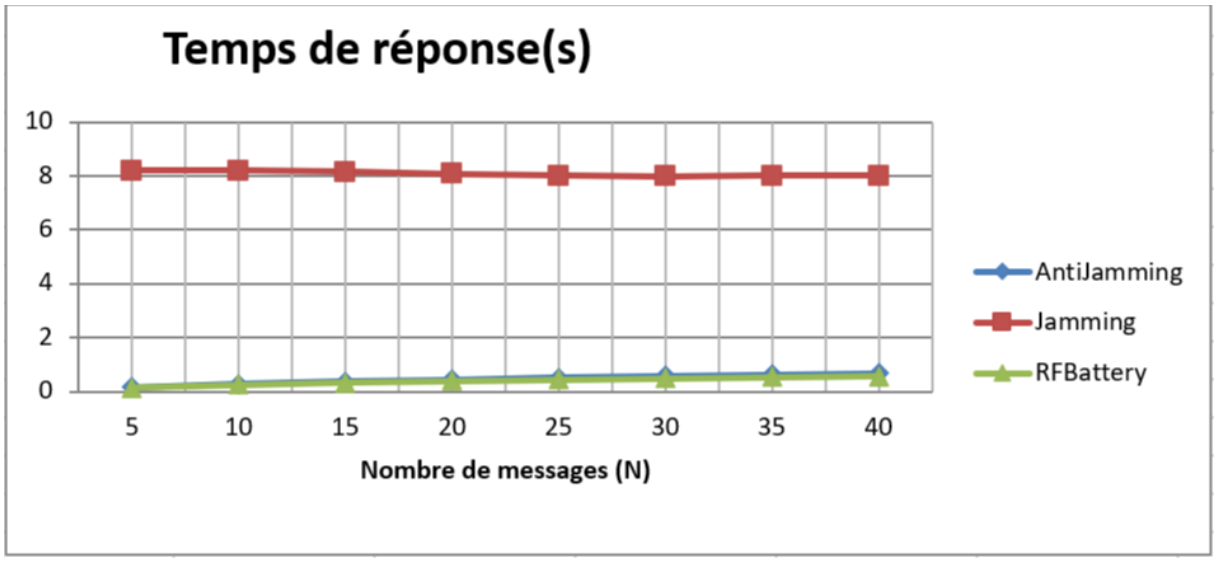

FIGURE 5.4 – Temps de réponse par rapport au nombre de Message (N)

"RFBattery" affichent des temps de réponse rapides, avec une légère augmentation progressive lorsque le nombre de messages augmente. Cependant, le nouveau modèle proposé "AntiJamming" intègre des techniques de défense, ce qui en fait le choix optimal en termes de sécurité et de temps de réponse.

5.4.2 Comparaison des modèles en fonction du taux de récolte d'énergie

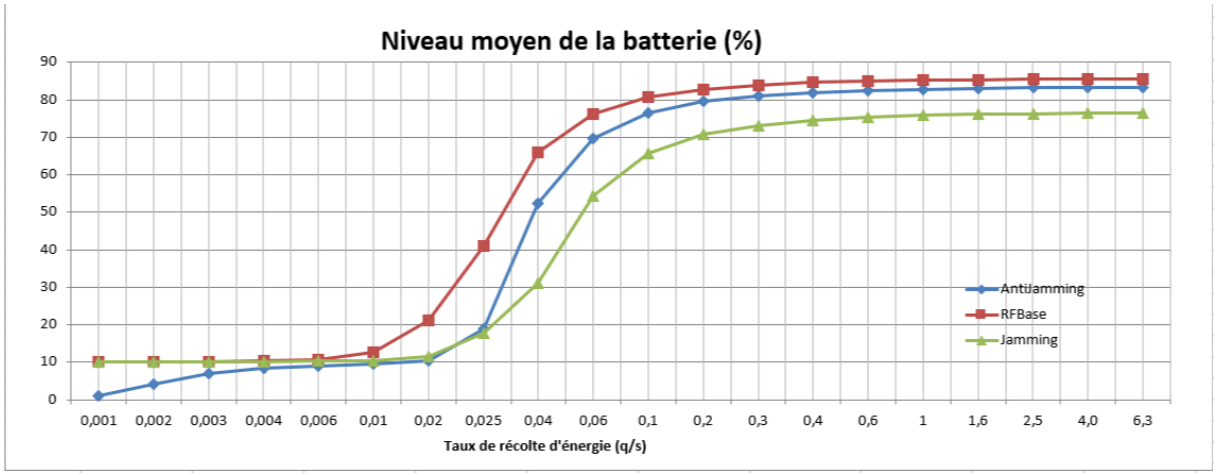

FIGURE 5.5 – Niveau moyen de la Batterie par rapport au taux de récolte d'énergie (q/s)

La Figure 5.5 représente l'évolution du niveau moyen de la batterie en fonction du taux de récolte d'énergie (q/s). En comparant les trois modèles en termes de niveau de batterie,

on constate que le modèle AntiJamming affiche initialement le niveau de batterie le plus bas par rapport aux deux autres modèles. Cependant, ce niveau de batterie augmente progressivement à mesure que le taux de récolte d'énergie augmente pour les trois modèles. Cette augmentation est principalement due à l'amélioration de la récolte d'énergie, ce qui permet aux modèles de reconstituer leur batterie au fil du temps.

Le modèle Jamming présente le niveau de batterie le plus bas parmi les trois, avec un niveau inférieur à 80% à la fin.

En ce qui concerne le modèle RFBattery, initialement, son niveau de batterie est similaire à celui du modèle Jamming (10 %). Cependant, il atteint plus de 80% à la fin de la période, mais il ne prend pas en compte les attaques ni la sécurité. Cela signifie que bien qu'il puisse bénéficier de l'augmentation du taux de récolte d'énergie, il ne garantit pas la sécurité du système.

En revanche, le modèle AntiJamming se trouve entre les deux autres modèles en termes de niveau de batterie, avec un niveau initial de 0 %. Toutefois, il augmente également avec l'augmentation du taux de récolte d'énergie. De plus, le modèle AntiJamming est capable de gérer les attaques de brouillage et de mettre en œuvre des techniques de défense, ce qui en fait le modèle le plus fiable en termes de sécurité tout en bénéficiant d'une augmentation du niveau de batterie grâce à la récolte d'énergie. Cet état persiste jusqu'à la fin de la période de récolte.

le graphe de la figure 5.6 représente le pourcentage de sommeil des modèles AntiJaming, Jamming et RFBattery en fonction du taux de récolte d'énergie (q/s). Dans un premier temps, le pourcentage de sommeil est de 100% pour les trois modèles. Ensuite, il commence à diminuer rapidement, puis continue à décroître progressivement jusqu'à atteindre une stabilisation, qui perdure jusqu'à la fin de la période de récolte d'énergie. En comparant les trois modèles, on observe que le modèle Jamming présente la tendance à s'endormir le plus fréquemment par rapport aux deux autres modèles. Cette propension à l'endormissement est attribuable à l'impact de l'attaque de brouillage sur la batterie, poussant ainsi le modèle à entrer en mode veille. Pour ce qui est du modèle RFBattery, il connaît le moins de périodes de sommeil, mais il ne tient pas compte des attaques et de la sécurité. En revanche, le modèle AntiJamming se positionne entre les deux autres modèles, avec un pourcentage de sommeil modéré. À la fin de la période de récolte, il affiche un taux de

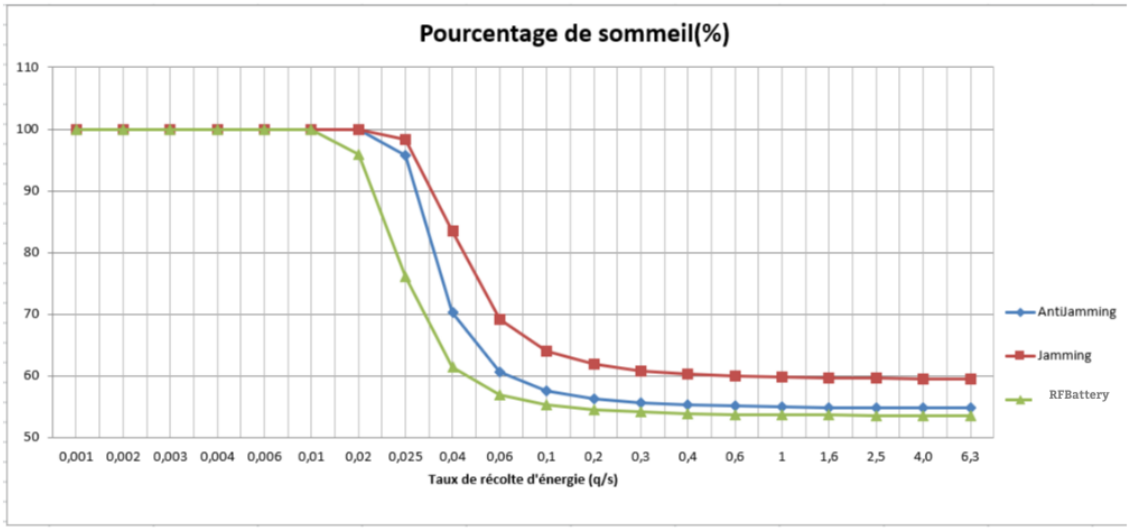

FIGURE 5.6 – Pourcentage de sommeil par rapport au taux de récolte d'énergie(q/s)

sommeil inférieur à 60%. De plus, il est capable de prendre en charge les attaques de brouillage et dispose de techniques de défense, ce qui en fait le modèle le plus fiable en termes de sécurité.

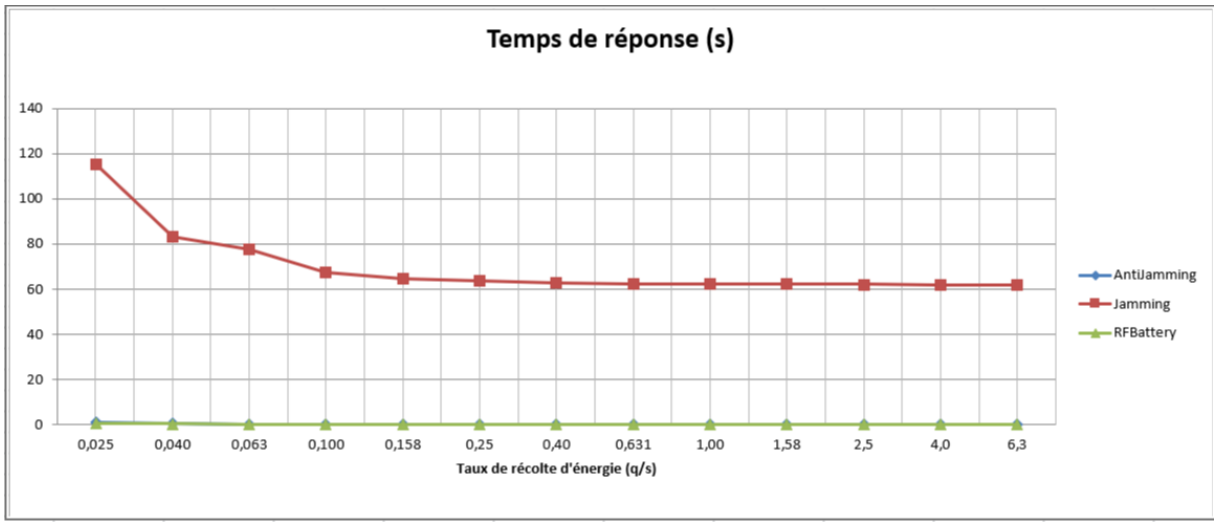

FIGURE 5.7 – Temps de réponse en fonction du taux de récolte d'énergie

La Figure 5.7 représente le temps de réponse en fonction du taux de récolte d'énergie. Nous observons que, pour les modèles "Jamming" et "RF Battery", le temps de réponse reste pratiquement stable et significatif. Dans le cas du modèle "Jamming", le temps de réponse diminue lorsque le taux de récolte d'énergie augmente.

5.4.3 Comparaison des modèles par rapport au délai de brouillage

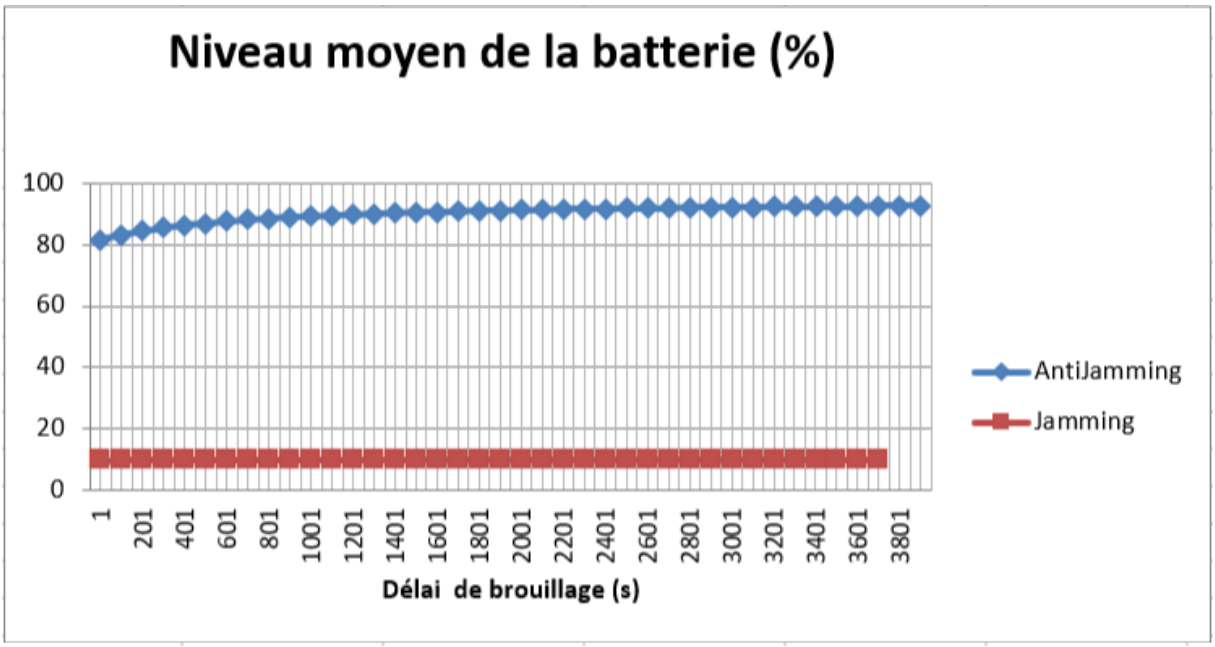

FIGURE 5.8 – Niveau moyen de la Batterie par rapport au délai de brouillage(s)

La Figure 5.8 illustre un graphique décrivant la corrélation entre le niveau de la bat-

terie et le délai de brouillage. Il est notable que le modèle Jamming affiche un niveau de batterie inférieur à 20%, ce qui s'avère insuffisant pour assurer le bon fonctionnement de l'appareil. En revanche, pour le modèle AntiJamming, étant donné qu'il considère des mesures de défense contre l'attaque de brouillage, celle-ci n'a qu'un impact limité sur le niveau de la batterie.

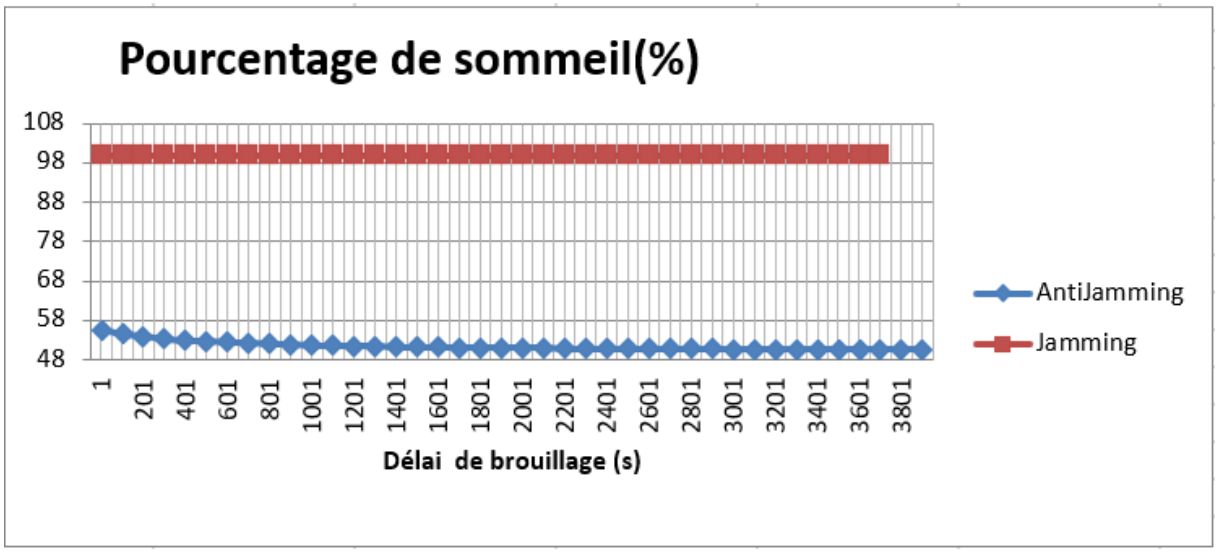

FIGURE 5.9 – Pourcentage de sommeil par rapport au délai de brouillage(s)

La Figure 5.9 représente un graphique décrivant la corrélation entre le pourcentage de sommeil et le délai du brouillage. On peut constater que, dans le cas d'AntiJamming, le pourcentage de sommeil reste en dessous de 58% malgré la persistance de l'attaque. Cette diminution du temps de sommeil est attribuée à l'utilisation de contre-mesures par le modèle. Cependant, ces contre-mesures permettent d'obtenir des résultats satisfaisants.

En ce qui concerne le modèle Jamming, son pourcentage de sommeil chute à 98% dès le début de l'attaque. Cela signifie que le modèle Jamming se trouve dans un état de sommeil la plupart du temps pendant l'attaque, ce qui rend son comportement insatisfaisant.

5.5 Conclusion

Dans ce chapitre, nous avons examiné l'impact de diverses contraintes réelles sur la charge de la batterie. L'analyse que nous avons menée démontre que le modèle est en me-

sure de déterminer la configuration optimale, favorisant ainsi l'atteinte de performances maximales au sein du réseau. Cette capacité sera un atout pour les utilisateurs qui pourront identifier les paramètres d'entrée adéquats pour obtenir le comportement souhaité du réseau.

Conclusion générale

Après une analyse approfondie, notre exploration du domaine de la Modélisation et de l'Évaluation des performances des Appareils Autonomes à Récupération d'Énergie Radiofréquence (RF-EH) ainsi que de la Sécurité de Niveau Physique au sein de l'Internet des Objets (IoT), à l'aide des Réseaux de Petri, a permis de générer des connaissances cruciales pour la conception, le déploiement et la protection de systèmes IoT avancés.

Nous avons élaboré un modèle innovant basé sur les Réseaux de Petri stochastique généralisé pour les objets autonomes connectés dans les réseaux sans fil à ressources limitées, en incluant la récupération d'énergie RF. Pour appliquer et tester numériquement ce modèle, nous avons fait appel à l'outil logiciel TimeNet.

Dans cette perspective, chaque appareil pourrait assumer un double rôle, celui de la transmission d'énergie et d'information. En outre, nous avons abordé la question de la sécurité en analysant la stratégie de changement de canal, servant de prévention contre les attaques de brouillage. Cette approche vise à optimiser les performances globales du réseau et à accroître sa résilience face aux menaces potentielles.

En résumé, cette étude a éclairé les tendances émergentes de l'IoT, avec un accent particulier sur les RF-EH. Elle a souligné les avantages et les précautions nécessaires pour garantir le fonctionnement optimal et la sécurité de ces systèmes. Les Réseaux de Petri se sont révélés des outils précieux pour la modélisation et l'évaluation de ces systèmes complexes, simplifiant leur conception et leur optimisation. En définitive, cette recherche contribue à l'évolution continue et à l'amélioration de l'IoT, en jetant les bases d'une intégration plus efficace et sécurisée des RF-EH dans nos environnements connectés.

En dernier lieu, il est important de reconnaître que, bien que ce projet ne soit pas parfait, il a ouvert des perspectives stimulantes pour des recherches futures. Nous prévoyons d'étendre nos résultats à travers diverses analyses expérimentales et d'explorer la modélisation proposée dans le contexte de différentes méthodes de récupération d'énergie.

Bibliographie

[1] Somia Sahraoui. *Mécanismes de sécurité pour l'intégration des RCSFs à l'IoT (Internet of Things)*. PhD thesis, Université de Batna 2, 2016.

[2] Sadika Khouni. *Gestion optimale des WSN (Wireless Sensor Network), Application aux IOT (Internet Of Things)*. PhD thesis, 2023.

[3] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. Security in energy harvesting networks : A survey of current solutions and research challenges. *IEEE Communications Surveys & Tutorials*, 22(4) :2658–2693, 2020.

[4] Qingzhi Liu, Kasım Sinan Yildirim, Przemysław Pawełczak, and Martijn Warnier. Safe and secure wireless power transfer networks : Challenges and opportunities in rf-based systems. *IEEE Communications Magazine*, 54(9) :74–79, 2016.

[5] Omar El Ayach, Steven W Peters, and Robert W Heath. The practical challenges of interference alignment. *IEEE Wireless Communications*, 20(1) :35–42, 2013.

[6] Oukas Nourredine and Menouar Boulif. Modeling and performance assessment of autonomous wpt-devices in wireless powered communication networking using petri nets. 12 2022.

[7] Oukas Nourredine, Menouar Boulif, Hakim Boudjelaba, and Abderrezak Djouabri. A new petri-nets-model for autonomous rf-devices in iot considering jamming attacks.

[8] Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé, et al. Vision and challenges for realising the internet of things. *Cluster of European research projects on the internet of things, European Commision*, 3(3) :34–36, 2010.

[9] Alex Mouapi. Radiofrequency energy harvesting systems for internet of things applications : A comprehensive overview of design issues. *Sensors*, 22(21) :8088, 2022.

[10] Keyur K Patel, Sunil M Patel, and P Scholar. Internet of things-iot : definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5), 2016.

[11] Imad Saleh. Internet des objets (ido) : Concepts, enjeux, défis et perspectives. *Revue Internet des objets*, 2(10.21494), 2018.

[12] EL-HADI ZAZOUA. Modèles de prédiction à apprentissage automatique pour les réseaux de capteurs sans fil à énergie renouvelable. 2022.

[13] Subramanian Balaji, Karan Nathani, and Rathnasamy Santhakumar. Iot technology, applications and challenges : a contemporary survey. *Wireless personal communications*, 108 :363–388, 2019.

[14] Abdelkarim Fatmi, Abdelkader Koulla, and REDHA REBHI. Étude et réalisation d'un système de présence par la technologie rfid et gsm géré par arduino. 2022.

[15] ZOUAI Meftah. *Une approche cloud computing basée IoT pour le smart House*. PhD thesis, Université de mohamed kheider biskra, 2021.

[16] Imourane Abdoulaye. *Minimisation de la consommation énergétique dans un réseau de capteurs sans fil en utilisant une application basée sur des réseaux de neurones*. PhD thesis, LEAT, 2022.

[17] Rudd JM Vullers, Rob Van Schaijk, Hubregt J Visser, Julien Penders, and Chris Van Hoof. Energy harvesting for autonomous wireless sensor networks. *IEEE Solid-State Circuits Magazine*, 2(2) :29–38, 2010.

[18] Oukas Nourredine and Boulif Menouar. A petri net modeling for wsn sensors with renewable energy harvesting capability. In *Smart Energy Empowerment in Smart and Resilient Cities : Renewable Energy for Smart and Sustainable Cities*, pages 524–534. Springer, 2020.

[19] Nourredine Oukas, Menouar Boulif, and Lyes Badis. A new gspns-model for sensors in solar ehwsns, considering seasonal sunshine levels and sleeping mechanism based on channel polling schedule. In *Advances in Computing Systems and Applications : Proceedings of the 5th Conference on Computing Systems and Applications*, pages 177–186. Springer, 2022.

[20] Amina Hentati. *Réseaux de capteurs sans fil avec récolte d'énergie : techniques de transmission pour les applications sensibles au délai.* PhD thesis, Polytechnique Montréal, 2021.

[21] Suzhi Bi, Yong Zeng, and Rui Zhang. Wireless powered communication networks : An overview. *IEEE Wireless Communications*, 23(2) :10–18, 2016.

[22] Michal Prauzek, Jaromir Konecny, Monika Borova, Karolina Janosova, Jakub Hlavica, and Petr Musilek. Energy harvesting sources, storage devices and system topologies for environmental wireless sensor networks : A review. *Sensors*, 18(8) :2446, 2018.

[23] Sangkil Kim, Rushi Vyas, Jo Bito, Kyriaki Niotaki, Ana Collado, Apostolos Georgiadis, and Manos M Tentzeris. Ambient rf energy-harvesting technologies for self-sustainable standalone wireless sensor platforms. *Proceedings of the IEEE*, 102(11) :1649–1666, 2014.

[24] Tharindu D Ponnimbaduge Perera, Dushantha Nalin K Jayakody, Shree Krishna Sharma, Symeon Chatzinotas, and Jun Li. Simultaneous wireless information and power transfer (swipt) : Recent advances and future challenges. *IEEE Communications Surveys & Tutorials*, 20(1) :264–302, 2017.

[25] Suzhi Bi, Chin Keong Ho, and Rui Zhang. Wireless powered communication : Opportunities and challenges. *IEEE Communications Magazine*, 53(4) :117–125, 2015.

[26] Jiawen Kang, Rong Yu, Sabita Maharjan, Yan Zhang, Xumin Huang, Shengli Xie, Hanna Bogucka, and Stein Gjessing. Toward secure energy harvesting cooperative networks. *IEEE Communications Magazine*, 53(8) :114–121, 2015.

[27] Wade Trappe, Richard Howard, and Robert S Moore. Low-energy security : Limits and opportunities in the internet of things. *IEEE Security & Privacy*, 13(1) :14–21, 2015.

[28] Quang Vinh Do, Insoo Koo, et al. Optimal power allocation for energy-efficient data transmission against full-duplex active eavesdroppers in wireless sensor networks. *IEEE Sensors Journal*, 19(13) :5333–5346, 2019.

[29] Tri Gia Nguyen, Chakchai So-In, Dac-Binh Ha, et al. Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer. *IEEE Access*, 5 :25196–25206, 2017.

[30] Alessio Di Mauro, Davide Papini, and Nicola Dragoni. Security challenges for energy-harvesting wireless sensor networks. In *PECCS*, pages 422–425, 2012.

[31] Zhice Yang, Qianyi Huang, and Qian Zhang. Nicscatter : Backscatter as a covert channel in mobile devices. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pages 356–367, 2017.

[32] Zhiqing Luo, Wei Wang, Jiang Xiao, Qianyi Huang, Tao Jiang, and Qian Zhang. Authenticating on-body backscatter by exploiting propagation signatures. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3) :1–22, 2018.

[33] Yusuke Nozaki and Masaya Yoshikawa. Tamper resistance evaluation method for energy harvester. In *2018 3rd International Conference on Computational Intelligence and Applications (ICCIA)*, pages 200–204. IEEE, 2018.

[34] Michael Moukarzel and Matthew Hicks. Reap what you store : Side-channel resilient computing through energy harvesting. In *Proceedings of the Fifth ACM International Workshop on Energy Harvesting and Energy-Neutral Sensing Systems*, pages 21–26, 2017.

[35] E Veronica Belmega and Arsenia Chorti. Protecting secret key generation systems against jamming : Energy harvesting and channel hopping approaches. *IEEE Transactions on Information Forensics and Security*, 12(11) :2611–2626, 2017.

[36] Jing Guo, Nan Zhao, F Richard Yu, Xin Liu, and Victor CM Leung. Exploiting adversarial jamming signals for energy harvesting in interference networks. *IEEE Transactions on Wireless Communications*, 16(2) :1267–1280, 2016.

[37] Meisam Razaviyayn, Gennady Lyubeznik, and Zhi-Quan Luo. On the degrees of freedom achievable through interference alignment in a mimo interference channel. *IEEE Transactions on Signal Processing*, 60(2) :812–821, 2011.

[38] Zhiqing Luo, Wei Wang, Jun Qu, Tao Jiang, and Qian Zhang. Shieldscatter : Improving iot security with backscatter assistance. In *Proceedings of the 16th ACM conference on embedded networked sensor systems*, pages 185–198, 2018.

[39] E Veronica Belmega and Arsenia Chorti. Energy harvesting in secret key generation systems under jamming attacks. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2017.

[40] Gada Rezgui, E Veronica Belmega, and Arsenia Chorti. Mitigating jamming attacks using energy harvesting. *IEEE Wireless Communications Letters*, 8(1) :297–300, 2018.

[41] Steffi Knorn and André Teixeira. Effects of jamming attacks on a control system with energy harvesting. *IEEE Control Systems Letters*, 3(4) :829–834, 2019.

[42] Vladimir Shakhov, Sangyep Nam, and Hyunseung Choo. Flooding attack in energy harvesting wireless sensor networks. In *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, pages 1–5, 2013.

[43] Cong Pu, Sunho Lim, Byungkwan Jung, and Manki Min. Mitigating stealthy collision attack in energy harvesting motivated networks. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 539–544. IEEE, 2017.

[44] Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, Bao Anh N Tran, Sreejaya Viswanathan, Younghee Park, and Yih-Chun Hu. Power-positive networking using wireless charging : Protecting energy against battery exhaustion attacks. In *Proceedings of the 10th ACM conference on security and privacy in wireless and mobile networks*, pages 52–57, 2017.

[45] Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, Yih-Chun Hu, and Younghee Park. Power-positive networking : Wireless-charging-based networking to protect energy against battery dos attacks. *ACM Transactions on Sensor Networks (TOSN)*, 15(3) :1–25, 2019.

[46] Xiaolin Fang, Ming Yang, and Wenjia Wu. Security cost aware data communication in low-power iot sensors with energy harvesting. *Sensors*, 18(12) :4400, 2018.

[47] Giuseppe Ateniese, Giuseppe Bianchi, Angelo T Capossele, Chiara Petrioli, and Dora Spenza. Helios : Outsourcing of security operations in green wireless sensor networks. In *2017 IEEE 85th vehicular technology conference (VTC spring)*, pages 1–7. IEEE, 2017.

[48] Giuseppe Ateniese, Giuseppe Bianchi, Angelo T Capossele, Chiara Petrioli, and Dora Spenza. Low-cost standard signatures for energy-harvesting wireless sensor networks. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(3) :1–23, 2017.

[49] M Ajmone Marsan. Stochastic petri nets : an elementary introduction. In *Advances in Petri Nets 1989 9*, pages 1–29. Springer, 1990.

[50] Mohamed Rédha Bahri and Allaoua Chaoui. Une approche intégrée mobile-uml/réseaux de pétri pour l'analyse des systèmes distribués à base d'agents mobiles. 2017.

[51] G Florin and S Natkin. Les réseaux de petri stochastiques. *Technique et science informatiques*, 4(1) :143–160, 1985.

[52] Michel Diaz. *Les réseaux de Petri : modèles fondamentaux*. Hermès science publications, 2001.

[53] Giovanni Chiola, Marco Ajmone Marsan, Gianfranco Balbo, and Gianni Conte. Generalized stochastic petri nets : A definition at the net level and its implications. *IEEE Transactions on software engineering*, 19(2) :89–107, 1993.

[54] Bachira Boutoumi and Nawel Gharbi. Two thresholds working vacation policy for improving energy consumption and latency in wsns. In *Queueing Theory and Network Applications : 13th International Conference, QTNA 2018, Tsukuba, Japan, July 25-27, 2018, Proceedings 13*, pages 168–181. Springer, 2018.

[55] Patrick Wüchner, János Sztrik, and Hermann De Meer. Modeling wireless sensor networks using finite-source retrial queues with unreliable orbit. In *Performance Evaluation of Computer and Communication Systems. Milestones and Future Challenges : IFIP WG 6.3/7.3 International Workshop, PERFORM 2010, in Honor of Günter Haring on the Occasion of His Emeritus Celebration, Vienna, Austria, October 14-16, 2010, Revised Selected Papers*, pages 73–86. Springer, 2011.

[56] Nourredine Oukas and Menouar Boulif. Sensor performance evaluation for long-lasting eh-wsns by gspn formulation, considering seasonal sunshine levels and dual standby strategy. *Arabian Journal for Science and Engineering*, 48(2) :1677–1691, 2023.

[57] TimeNET.

[58] Alex Mouapi. *Prédiction et gestion de l'énergie dans un réseau de capteurs sans fil récolteurs d'énergie vibratoire pour les applications industrielles de l'internet des objets*. PhD thesis, Université du Québec en Abitibi-Témiscamingue, 2021.

[59] Bhavneet Sidhu, Hardeep Singh, and Amit Chhabra. Emerging wireless standards-wifi, zigbee and wimax. *World Academy of Science, Engineering and Technology*, 25(2007) :308–313, 2007.

[60] Angela M Lonzetta, Peter Cope, Joseph Campbell, Bassam J Mohd, and Thaier Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3) :28, 2018.

[61] Adel Ismail Al-Alawi. Wifi technology : Future market challenges and opportunities. *Journal of computer science*, 2(1) :13–18, 2006.

[62] Nawel Gharbi. *Evaluation des performances et de la fiabilité des systèmes multi-classes avec rappel à l'aide des réseaux de petri stochastiques colorés*. PhD thesis, Alger, 2007.

Webographie

[Web1] http ://www.mytopschool.net,Date de la dernière visite 13/04/2022.

[Web2] http ://www.tinyos.net,Date de la dernière visite 10/05/2022.

[Web3] http ://www.alertsystems.org, dernière visite 14/03/2022. [Web4] https ://timenet.tu-ilmenau.de//,Date de la dernière visite 28/08/2023.