République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université de kasdi Merbah Ouargla

Faculté des Nouvelles Technologies de l'information et la Communication

Département de l'informatique et Technologies de l'information

Mémoire présenté en vue de l'obtention du diplôme Master

L'impact des attaques de type topologie sur les réseaux RPL

Réalisé par :

MANSOUR Marwa

BOUGHEBACHE Besma

Encadré par :

Dr BOUKHAMLA Akram Zine Eddine

Dr Benkadeur Med Kamel	**Président**	**Univ ouargla**
Dr Boukhamla Akram	**Encadrant**	**Univ ouargla**
Dr Hemrouni Bessma	**Examinateur**	**Univ ouargla**

Année universitaire 2023-2024

Remerciements

Nous exprimons notre gratitude envers ALLAH de nous avoir accordé la santé et le courage nécessaires pour réussir cette tâche. Ce travail marque la fin d'une longue période où nous avons bénéficié de l'encadrement, de l'encouragement et du soutien de nombreuses personnes, à qui nous souhaitons exprimer notre profonde et sincère gratitude.

Encadrant « Monsieur Boukhamla Akram », pour avoir accepté de collaborer avec nous et pour ses conseils précieux et ses orientations. Nous avons eu la chance de faire partie de votre équipe et de reconnaître vos qualités, votre sérieux et votre expertise. Merci infiniment aux membres du jury d'avoir accepté de donner leur avis sur notre travail. Nous tiens à exprimer notre gratitude envers toutes les personnes qui nous ont accordé leur amitié, leur attention, leurs encouragements, leur soutien et leur aide pour que nous puissont mener à bien cette tâche.

À la fin de ce travail. Nous tenons également à exprimer nos gratitude envers nos parents qui nous ont soutenu, qui nous ont enseigné à travailler avec honnêteté et qui nous ont toujours soutenu tout au long de nos longues années d'études.

Résumé

L'Internet des Objets (IdO) est un secteur en plein essor, où les appareils connectés sont employés afin de recueillir et de transmettre des informations. Dans les réseaux de capteurs sans fil IdO, le protocole RPL est fréquemment employé afin de garantir une communication efficace entre les appareils. Le protocole RPL a été développé spécifiquement pour les réseaux à faible consommation d'énergie et à pertes. Toutefois, l'emploi du protocole RPL dans l'IdO peut aussi engendrer des menaces pour la sécurité.

Dans ce mémoire, notre attention se porte d'abord sur la question de sécurité et sur le fonctionnement de RPL. Par la suite, nous examinerons les travaux existants sur les attaques RPL et leur classification. Ensuite, nous mettrons en place deux attaques (Blackhole et Sinkhole) en utilisant le simulateur Cooja afin d'analyser les conséquences des attaques sur les paramètres tels que la consommation d'énergie et le PDR. Nous examinerons ensuite leurs impacts sur le réseau et le fonctionnement du protocole de routage RPL. Enfin, nous discuterons des résultats obtenus.

Mots-clés: Internet des Objet, RPL,consommation d'énergie, LLN, Cooja,PDR, Simulation, mécanismes de sécurité ,Attaques, sécurité.

Abstract

The Internet of Things (IoT) is a fast-growing sector in which connected devices are used to collect and transmit information. In wireless IoT sensor networks, the RPL protocol is frequently used to ensure efficient communication between devices. The RPL protocol was developed specifically for low-power, lossy networks. However, the use of the RPL protocol in the IoT can also lead to security threats.

In this thesis, we focus first how RPL works and also the RPL security issue. We will then review existing work on RPL attacks and their classification. Next, we will implement two attacks (Blackhole and Sinkhole) using the Cooja simulator in order to analyse the consequences of the attacks on parameters such as power consumption and PDR. We will then examine their impact on the network and the operation of the RPL routing protocol. Finally, we will discuss the results obtained.

Keywords: Internet of Things, RPL,energy consumption, LLN, Cooja,PDR, Simulation, security mechanisms ,Attacks, security.

الملخص

إنترنت الأشياء (IoT) هو قطاع سريع النمو تُستخدم فيه الأجهزة المتصلة لجمع المعلومات ونقلها. في شبكات مستشعرات إنترنت الأشياء اللاسلكية، كثيراً ما يُستخدم بروتوكول RPL لضمان كفاءة الاتصال بين الأجهزة. طُوِّر بروتوكول RPL خصيصاً للشبكات منخفضة الطاقة وذات الفقدان. ومع ذلك، فإن استخدام بروتوكول RPL في إنترنت الأشياء يمكن أن يؤدي أيضًا إلى تهديدات أمنية.

في هذا الموجز، سنركز أولاً على مشكلة الأمان وكيفية عمل بروتوكول RPL. سنقوم بعد ذلك بمراجعة العمل الحالي على هجمات RPL وتصنيفها. بعد ذلك، سنقوم بتنفيذ هجومين (Blackhole و Sinkhole) باستخدام محاكي Cooja من أجل تحليل عواقب الهجمات على معلمات مثل استهلاك الطاقة ومعدل سرعة الاستجابة السريعة. سنقوم بعد ذلك بفحص تأثيرها على الشبكة وتشغيل بروتوكول توجيه RPL. وأخيراً، سنناقش النتائج التي تم الحصول عليها.

الكلمات الرئيسية: إنترنت الأشياء، RPL، واستهلاك الطاقة، وشبكة LLN، وCooja، ومعدل سرعة الشبكة PDR، والمحاكاة، وآليات الأمان، والهجمات، والأمن.

Table des matières

Liste des figures

Liste des abréviations

6LoWPAN: IPv6 Low power Wireless Personal Area Network

CoAP: Constrained Application Protocol

DAG: Directed Acyclic Graph

DAO: DODAG Advertisement Object

DAO-Ack : DODAG Advertisement Object Acknowledgment

DIO : DODAG Information Object

DIS : DODAG Insformation Sollicitation

DODAG : Destination Oriented Direct Acyclic Graph

DODAG : Destination Oriented Directed Acyclic Graph

IdO : Internet des Objets

IDS : Intrusion Detection System

IEEE : Institute of Electrical and Electronics

IETF : International Engineering Task Force

IoT : Internet of Things

IPv6 : Internet Protocol Version 6 Engineers

LLN : Low Power and Lossy Network

MIT : Massachusetts Institute of Technology

MP2P: Multi-Point to Point

ND: Neighbours Discovery

P2MP: Point to Multi-Point

P2P : Point to Point

RFID : Radio Frequency Identification

RoLL: Routing over Low-power and Lossy Network

RPL IPv6: Routing Protocol for Low-power and Lossy Network

Introduction générale

Introduction Générale

Aujourd'hui, la technologie a beaucoup progressé et continue de progresser. Nous avons assisté à l'émergence de l'internet, une source immense de diverses informations.

L'Internet des Objets (IdO) a vu le jour grâce à la connexion de certains objets physiques à internet, ce qui suscite un intérêt et une expansion dans différents domaines tels que les villes intelligentes, l'agriculture intelligente, la santé, le transport et l'éducation. La plupart de ces déploiements nécessitent principalement la création d'infrastructures de réseau sous-jacentes pour des communications économes en énergie et à faible consommation. De cette manière, les réseaux à faible puissance et à perte (LLN) répondent à cette demande en proposant des déploiements abordables et moins contraignants. Les LLN offrent une connexion efficace entre de nombreux dispositifs IdO de petite taille et à ressources limitées qui sont reliés entre eux sans fil. L'Internet des Objets (IdO) représente l'un des éléments essentiels. L'Internet des Objets (IdO) est l'un des nouveaux paradigmes de réseau les plus rapides, offrant une multitude d'applications bénéfiques pour l'humanité. Grâce aux avancées technologiques dans les systèmes embarqués et à l'IPv6 compressé, il est maintenant possible de prendre en compte la pile IP dans les appareils intelligents hétérogènes à déficit de ressources. Toutefois, l'interconnexion mondiale et les ressources restreintes des appareils intelligents les ont exposés à diverses attaques internes et externes, ce qui met en péril la sécurité et la confidentialité des utilisateurs. Différents menaces liés à l'IdO entravent son développement et entravent l'adoption mondiale de ses applications. Le groupe de travail ROLL de l'IETF a défini le protocole de routage IPv6 pour les réseaux à faible puissance et avec perte (RPL) afin de simplifier le routage dans les réseaux IPv6 LoW Power. Les réseaux de zone sans fil (6LoWPAN), tout en prenant en considération leurs limites. Comme les ressources des nœuds dans l'IdO sont limitées, RPL est exposé à de nombreuses attaques qui consomment les ressources du nœud et altèrent les performances du réseau.

Le protocole RPL est fréquemment utilisé pour assurer une communication efficace entre les appareils. Les réseaux RPL (Routing Protocol for Low-Power and Lossy Networks) sont couramment utilisés dans l'Internet des Objets (IdO) en raison de leur capacité à s'adapter aux contraintes des réseaux à faible puissance et à perte. L'énergie est une ressource majeure pour les appareils IdO intelligents, car la plupart des applications sont alimentées par des batteries ou utilisent une technologie de récolte d'énergie. Il n'est donc pas judicieux de gaspiller de l'énergie pour la transmission de données. La sécurité est également l'un des principaux défis de l'IdO. De nombreux appareils IdO disposent de ressources informatiques limitées, ce qui rend difficile leur sécurisation par des protocoles de cryptage complexes. Cependant, ces réseaux sont vulnérables aux attaques par manipulation de la topologie telles que les attaques de Sinkhole et Blackhole, qui peuvent avoir un impact significatif sur leur fonctionnement et la consommation de leurs ressources.

Ce mémoire vise principalement à mettre en place différentes attaques de type topologie pour évaluer l'impact de ces attaques sur le protocole RPL, aussi bien les conséquences de ces attaques.
Cette évaluation nous a permit de conclure que ces attaques de type topologie dégradent d'une façons catastrophique le bon fonctionnement de réseau RPL. les résultats expérimentaux de cette evaluation par simulation, montrent bien la degradation de taux bas de PDR aussi bien la consommation élevée d'énergie.
Notre travail se concentre principalement sur quatre chapitres, dont le premier traite de l'internet des objets et de ses principales caractéristiques, ainsi que des différents protocoles. Le deuxième chapitre traitera du protocole RPL, de ses concepts clés et de ses différents domaines d'application. Le troisième chapitre portera sur les attaques et les mécanismes de sécurité de protocole RPL en général. Enfin, le chapitre 4 analysera les mesures causées par certaines attaques sur le réseau RPL.

Chapitre I: Généralité sur l'Internet des Objets

I .1 Introduction

Internet des Objets est une connexion mondiale d'objets qui se produit lorsque plus de « choses ou d'objets » sont connectés à internet que de personnes, chaque objet possédant une adresse unique. Un élément comme (ordinateurs, capteurs, appareils mobiles) aura la capacité de transmettre des données et il est possible de recevoir des commandes.

De nos jours, l'Internet des Objets (IdO) représente la prochaine évolution d'internet et permettra d'améliorer considérablement sa capacité, ouvrant ainsi la voie à de nombreux scénarios basés sur l'interconnexion entre le monde réel et digital. Dans ce chapitre, nous prenons comment cette nouvelle technologie a pu influencer son histoire depuis son invention jusqu'à nos jours. Ensuite, nous examinerons l'organisation des IdO, leur fonctionnement, les divers domaines d'application et les défis liés à l'IdO.

I .2 Internet des Objets

I .2.1 Définitions d'Internet des Objets

La définition de l'Internet des Objets (IdO) (en anglais Internet of Things, IoT) reste encore indécise, ce qui s'explique par la nouveauté de ce concept en constante évolution. Il y a de nombreuses définitions et entités impliquées dans la réflexion, le développement ou la normalisation de ce nouveau paradigme.

Le groupe de travail Internet of Things Global Standards Initiative (IoT-GSI), piloté par l'International Télécommunication Union (ITU), définit l'IdO comme « une infrastructure mondiale au service de la société de l'information » permettant « d'offrir des services évolués en interconnectant des objets (physiques et virtuels) grâce à l'interopérabilité de technologies de l'information et de la communication existantes ou en évolution ». [1]

D'autre côté, l'IEEE définit l'IdO comme un « réseau d'éléments chacun muni de capteurs qui sont connectés à Internet ». [1]

Le CERP-IoT « Cluster des projets européens de recherche sur l'Internet des Objets » définit l'Internet d'Objet comme : « une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'autoconfiguration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente ». [2]

Figure I.1: Internet des Objets.

I .2.2 Historique de l'IdO

En 1999, le concept "d'Internet des Objets" est apparu. Le MIT (Massachusetts Institute of Technology), à travers Kevin Ashton, un chercheur britannique spécialisé dans le domaine de l'IdO. Une initiative a été lancée par ses collègues afin de favoriser la connectivité ouverte. La RFID (Radio Frequency Identification) est utilisée par tous les objets. L'émergence du nouveau protocole IPv6 a rapidement permis à des secteurs tels que l'aéronautique de se détacher du concept de l'Internet des Objets et de s'impliquer dans les recherches. Il est devenu très populaire en 2007. Par la suite, nous envisageons de développer un Internet mondial des Objets.

I .2.3 L'évolution d'Internet des Objets

En 1990, la connexion initiale a été réévaluée. Ces produits comprennent des grille-pains, des machines à café ou d'autres éléments de la vie quotidienne.

En 2000, la société LG a présenté un nouveau produit industriel appelé "électroménager connecté avec Internet". Durant cette même année, les premiers essais d'appareils connectés à Internet pour la recherche automatique d'informations ont été effectués.

En 2003, il y avait environ 6,3 milliards de personnes à travers le monde et 500 millions d'appareils connectés à Internet [3]. Le calcul du nombre d'appareils en fonction de la population mondiale (0,08) révèle un nombre limité d'appareils connectés par habitant. D'après Cisco IBSG(Internet Business Solutions Group), l'Internet des Objets n'était pas présent en 2003 en raison de le nombre d'objets connectés limité.

En 2010 avec l'émergence des smartphones et des tablettes, le nombre d'appareils et de personnes connectées à Internet a atteint 12,5 milliards, tandis que la population mondiale s'élève à 6,8 milliards. C'est la raison pour laquelle il y a pour la première fois plus d'un appareil connecté par personne (1.84). Dans son livre blanc IoT, Cisco expose comment le nombre d'objets a évolué. [04]

De nos jours, il dépasse largement la population mondiale, et comme mentionné précédemment, il devrait continuer à augmenter pour atteindre 50 milliards.

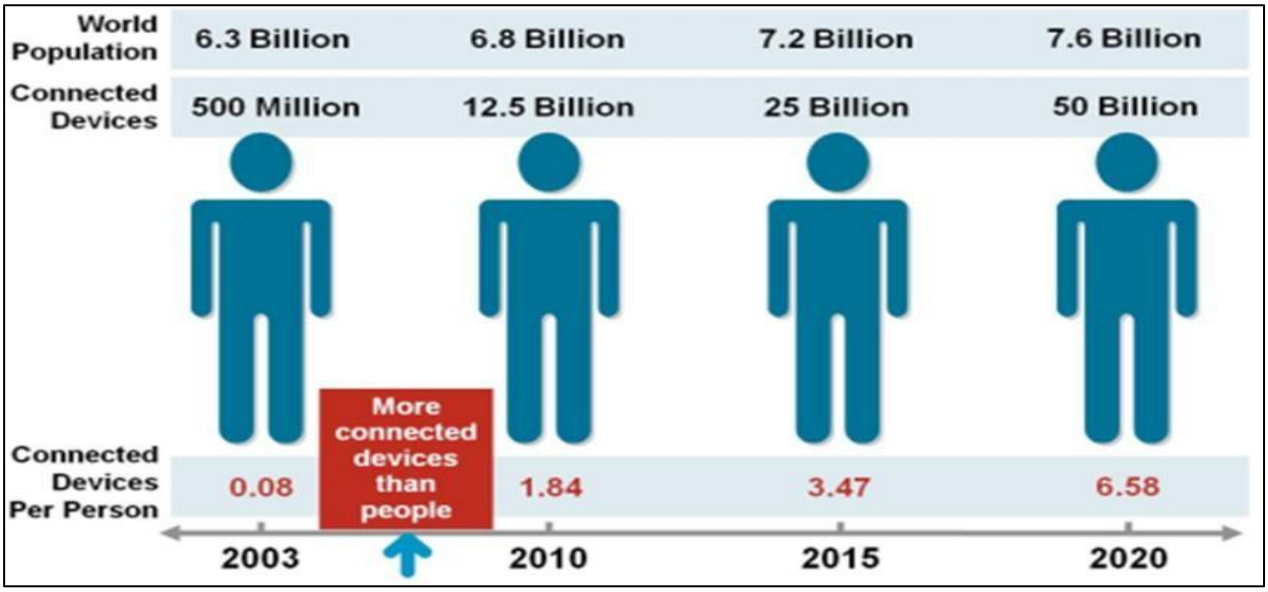

Figure I.2: L'évolution d'Internet des Objets.

I .2.5 Domaines d'applications d'IdO

L'Internet des Objets est employé dans différents domaines tels que l'agriculture, l'environnement, la domotique, et bien d'autres encore.

Santé:

En santé, l'IdO surveillera les signes fournir des cliniques aux patients en créant des réseaux personnels et des capteurs médicaux surveiller les constantes biologiques telles que la température corporelle, Tension artérielle et activité respiratoire [05]. Afin de faciliter la surveillance et d'apporter des solutions, notamment aux personnes à mobilité réduite, dans le domaine de la santé, leurs activités dans leur milieu de vie sont surveillées grâce à des capteurs portables (accéléromètres, gyroscopes, etc..) ou fixes.

Domotique :

La domotique est un ensemble de technologies qui offrent à la maison une intelligence, une capacité de pensée autonome et la possibilité de contrôler différents équipements depuis la même interface (téléphone, panneau) grâce à l'Internet des Objets, qui a simplifié et rendu possible la communication entre les appareils électroménagers et les a dirigés. Avec la diffusion de l'Internet des objets, nous atteignons les villes à distance.[05]

Agriculture:

Dans le domaine de l'agriculture, il est possible d'utiliser des réseaux de capteurs interconnectés à l'Internet des Objets afin de surveiller l'environnement des cultures [7]. Grâce à eux, ces réseaux peuvent être utilisés pour combattre les dommages et les catastrophes, ainsi que pour améliorer l'utilisation l'eau d'irrigation. De plus, ils permettent de planifier les travaux agricoles et d'améliorer la qualité de l'environnement en général.

Villes intelligentes (Smart City) :

Le concept de villes intelligentes est employé pour décrire l'écosystème de la cybernétique [7]. Avec l'utilisation de services de pointe, il est possible d'optimiser l'utilisation de l'infrastructure physique de la ville (routes, réseaux électriques, etc..), ce qui améliore la qualité de vie des habitants.

Industriel :

Dans le domaine de l'IdO industriel, il sera possible d'assurer un suivi global des produits, en surveillant de la production à la distribution, en réglementant les conditions de fourniture, en luttant contre la contrefaçon, la fraude et la criminalité dans l'économie transfrontalière.

environnement:

Dans ce domaine, la capacité à repérer et à gérer les phénomènes naturels, tels que le vent, les hauteurs des rivières, etc.., joue un rôle essentiel. En outre, une intégration fluide de ces données variées. [05]

Sécurité de la surveillance :

La surveillance est essentielle pour assurer la sécurité d'un bâtiment d'entreprise, d'un centre commercial, d'une usine, d'un parking et d'autres lieux publics. En préservant la confidentialité des utilisateurs [05]. Pour obtenir et développer une grande capacité de sécurité de manière facile et rapide. Différents capteurs sont employés pour la surveillance, tels que des capteurs ambiants qui peuvent être utilisés pour surveiller la présence de substances chimiques dangereuses, ainsi que des capteurs de surveillance du comportement des individus pour repérer les individus qui agissent de manière suspecte.

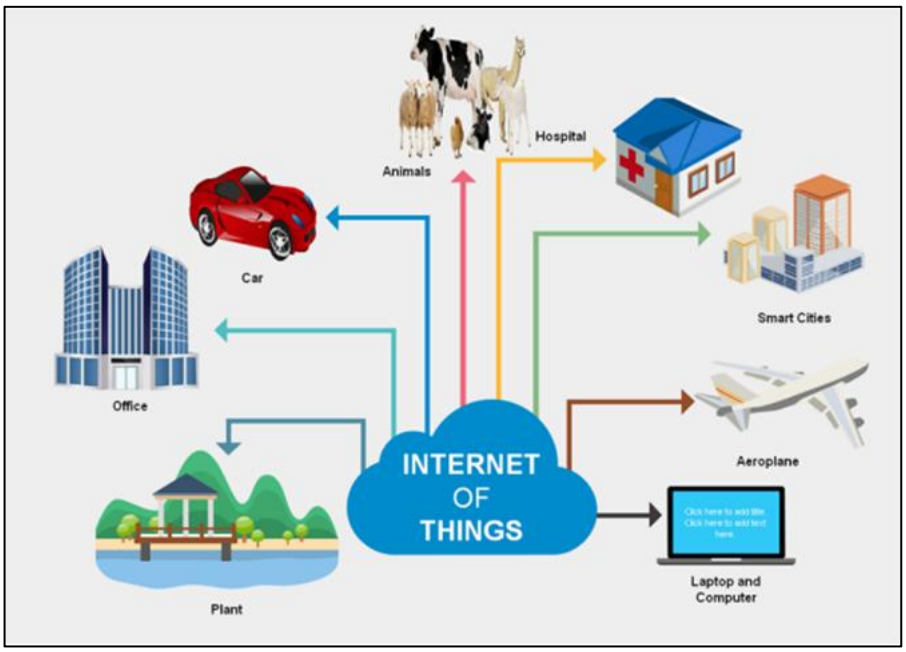

Figure I.3: Domaine d'applications de l'IdO.

I .2.6 Les Composantes de l'IdO

L'IdO est constitué de quatre éléments. Dans un premier temps, un objet connecté désigne un objet qui a une fonction mécanique et/ou électrique particulière. Il est possible qu'il soit conçu de manière directe pour être connecté, ou bien qu'il soit déjà existant et qu'il soit connecté ultérieurement. L'objet connecté vise à collecter des informations provenant de capteurs, à les traiter et à les transmettre grâce à une fonction de connectivité, ainsi qu'à recevoir des consignes pour réaliser une action. D'ordinaire, ces fonctions de l'objet connecté nécessitent une source d'énergie, surtout lorsque les données sont intégrées directement dans celui-ci. [06]

- **Capteur**

Les capteurs sont des instruments qui transforment une mesure physique observée (telle que la température, la luminosité, le mouvement, etc..) en une mesure numérique qui peut être utilisée par des logiciels. On retrouve de nombreux capteurs de diverses catégories, les objets connectés ont souvent pour objectif de repérer ces dimensions physiques sur leurs lieux d'utilisation.
On retrouve différents types de capteurs tels que la lumière, la présence, la position, le déplacement, l'accélération, la température, l'humidité, le son, les vibrations, l'électricité, le gaz, la force, la pression, etc.. [06]

- **Réseaux de capteurs**

Les capteurs sont munis de dispositifs sans fil qui facilitent la transmission et la réception de données afin de satisfaire leurs besoins de communication. Néanmoins, cela n'assure pas l'accès à un ensemble de capteurs, du moins de manière interopérable, transparente et compacte. Afin d'y parvenir, il est indispensable que les capteurs se structurent. Les éléments d'un réseau de capteurs se distinguent par leur taille réduite et leur capacité de transmission sans fil. [07]

- **Le nuage de l'IdO (**le cerveau de la révolution des données**)**

Les plateformes cloud jouent un rôle essentiel dans l'IoT. Elles offrent un espace de stockage évolutif pour les données collectées par les dispositifs IoT. De plus, elles proposent des services d'analyse avancée, d'apprentissage automatique et de traitement des données, ce qui permet d'exploiter au maximum le potentiel des informations collectées.

- **Actionneurs**

Les actionneurs représentent des dispositifs capables de transformer une information numérique en un phénomène physique pour produire un effet. Ils incarnent un peu le contraire du capteur. Exemples de produits investis : écrans, systèmes d'alarme, caméras, enceintes, lampes, moteurs, pompes et ventilateurs. [06]

- **Connectivité**

L'objet est connecté grâce à une petite antenne radiofréquence qui facilite la communication avec un ou plusieurs réseaux. D'un côté, les objets pourront recueillir des données telles que leur identité, leur état, une alerte ou les données des capteurs, et de l'autre, recevoir des informations telles que

des instructions d'action et des données. Il est également possible de gérer le « cycle de vie de l'objet », c'est-à-dire l'identification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau. [06]

I.2.7 Architecture d'Internet des Objets:

Une architecture technique est un cadre créé pour permettre aux concepteurs et aux développeurs de considérer le système dans son ensemble et de le décomposer en sections. Selon les normes mondiales 1 (GS1), « une architecture de référence est une fondation pour permettre l'intégration des diverses technologies dans les applications IdO ».
Il existe de nombreuse proposition d'architectures pour l'IdO parmi les architectures qui ont été proposées, il y'a l'architecture a cinq couches et a trois couches proposées par IEEE. En ce moment y'a pas une architecture universellement acceptée. [9]

A. L'architecture à trois couches : Cette architecture se compose de :

- **La couche application (application layer):** est chargée de fournir des services spécifiques à l'application à l'utilisateur. Il définit diverses applications dans lesquelles l'Internet des Objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente.

- **La couche réseau (abstract layer) :** est responsable de la connexion à d'autres objets intelligents, périphériques réseau et serveurs. Ses fonctionnalités sont également utilisées pour la transmission et le traitement des données des capteurs.

- **La couche perception (things layer) :** est la couche physique, qui possède des capteurs pour détecter et recueillir des informations sur l'environnement. Il détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement.

B. L'architecture à quatre couches :
Étant donné le développement constant de l'Internet des Objets, il est impossible de répondre à toutes les exigences de l'Internet des Objets. C'est pourquoi une architecture à quatre couches a été suggérée. Cette architecture comprend trois couches similaires à l'architecture précédente, mais elle inclut également une couche supplémentaire appelée couche de support. L'objectif de cette couche est de garantir la sécurité.
Dans une structure à quatre niveaux, les données sont transmises à la couche réseau qui est obtenue à partir de la couche réception. La couche de support remplit deux fonctions. Elle garantit que les données sont transmises par un utilisateur authentique et utilise des techniques d'authentification afin de prévenir les risques. La seconde tâche consiste à transmettre des données à la couche réseau. [10]

C. L'architecture à cinq couches : Cette architecture a cinq couches se compose de:

- **La couches d'application :** est chargée de fournir des services spécifiques à l'application à l'utilisateur. Il définit diverses applications dans lesquelles l'Internet des Objets peut être déployé, par exemple, les maisons intelligentes, les villes intelligentes et la santé intelligente.

- **La couche de transport (transport layer) :** transfère les données du capteur de la couche de perception à la couche de traitement et vice versa via des réseaux tels que sans fil, 3G, LAN, Bluetooth, RFID et NFC.

- **La couche perception (things layer) :** est la couche physique, qui possède des capteurs pour détecter et recueillir des informations sur l'environnement. Il détecte certains paramètres physiques ou identifie d'autres objets intelligents dans l'environnement.

- **La couche de traitement (processing layer) :** est également appelée couche middleware. Il stocke, analyse et traite d'énormes quantités de données provenant de la couche transport. Il peut gérer et fournir un ensemble diversifié de services aux couches inférieures. Il utilise de nombreuses technologies telles que les bases de données, le cloud computing et les modules de traitement des méga données.

- **La couche commerciale (business layer) :** convertit les données stockées en informations exploitables. Les chefs d'entreprise, les directeurs techniques, etc. peuvent utiliser ces rapports. Ils les aident à prendre des décisions pour améliorer la productivité.Cette couche comprend principalement des intégrations d'applications d'entreprise. Par exemple, les planificateurs de ressources d'entreprise (ERP), les applications de veille stratégique (BI), les applications de visualisation de données, etc.. [9]

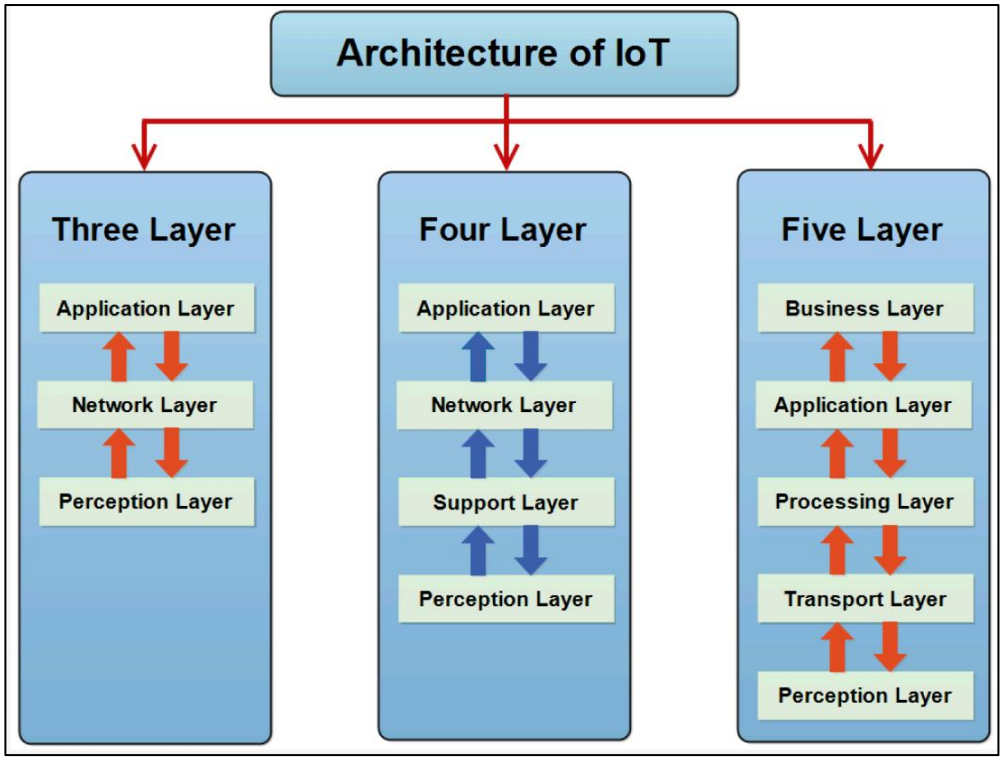

Figure I.4 : Architectures d'IdO.

I .2.8 Protocoles d'Internet des Objets

De nombreuses normes IdO sont proposées pour faciliter et simplifier les tâches des programmeurs d'applications et des fournisseurs de services, et l'IdO ambitionne de faire communiquer chaque système avec tous les autres au moyen de protocoles communs. La mise en application à une large échelle du concept d'IdO apparaît largement tributaire d'une standardisation de la communication entre objets dite M2M.

- **Au niveau de la couche de liaison :** le standard IEEE 802.15.4 est plus adapté que l'Ethernet aux environnements industriels difficiles.

- **Au niveau réseau :** le standard 6loWPan a réussi à adapter le protocole IPV6 aux communications sans fil entre nœud à très faible consommation.

- **Au niveau routage :** l'IETF a publié en 2011 le standard RPL.

- **Au niveau de la couche application :** le protocole CoAP(Constrained Application Protocol) qui tente d'adapter HTTP, beaucoup trop gourmand aux contraintes des communications entre nœuds à faible consommation. [9]

I.2.9 Les défis et les menaces d'IdO

I.2.11.1 Les défis d'IdO :

- La sécurité: est l'un des principaux défis de l'IdO. Plusieurs dispositifs IdO ont des ressources informatiques restreintes, ce qui rend leur sécurité difficile avec des protocoles de chiffrement complexes. Cela accroît leur risque de piratage informatique et d'intrusion cybernétique.

- Intégrité des données: il est essentiel de garantir l'exactitude et la fiabilité des données collectées par les appareils IdO afin d'assurer leur intégrité. Il est nécessaire de mettre en œuvre des dispositifs afin d'assurer l'intégrité des données et d'éviter toute manipulation.

- Consommation d'énergie: Des milliards d'appareils et des réseaux très variés ont été développés grâce à l'internet des objets. La ressource énergétique est perçue comme essentielle pour les appareils intelligents de l'IdO, car la majorité des applications sont alimentées par des batteries ou utilisent une technologie de récupération d'énergie. Il est donc préférable de ne pas gaspiller de l'énergie en transmettant des informations. Ainsi, il demeure un défi majeur pour les réseaux IdO de concevoir une architecture de réseau économe en énergie et un mécanisme de routage intelligent. [10]

I.2.11.2 les menaces d'IdO :

Les cyberdélinquants peuvent attaquer le hardware ou le software de n'importe quel composant au sein d'un système d'IdO. Parmi les types de cyberattaques par l'IdO les plus courants figurent :

- **Attaques par force brute :**

Les attaques par force brute consistent à essayer de deviner le mot de passe d'un appareil IdO. Il peut également être très efficace contre les appareils avec des mots de passe faibles. [11]

- **Attaques par injection de code :**

Inclut du code malveillant dans un appareil IdO. Ce code a la capacité de prendre le contrôle de l'appareil, de voler des informations ou de lancer d'autres attaques. [12]

- **Attaques par déni de service (DoS) :**

Les attaques par déni de service (DoS) visent à empêcher les utilisateurs d'accéder à l'appareil et peuvent également perturber les services dépendants de l'appareil. [13]

- **Attaques de l'homme du milieu (MitM) :**

Les attaques de l'homme du milieu (MITM) consistent à intercepter la communication entre l'appareil IdO et un autre appareil ou service. Cela permet à l'attaquant d'espionner les communications ou de modifier les données qui sont transmises. [14]

- **Attaques de logiciels malveillants :**

Les attaques de logiciels malveillants consistent à infecter un appareil avec un logiciel malveillant.

Ce logiciel malveillant peut ensuite être utilisé pour prendre le contrôle de ciel malveillant peut ensuite être utilisé pour prendre le contrôle de l'appareil, voler des données ou lancer d'autres attaques. [15]

- **Attaques de botnet :**

Les attaques de botnet consistent à utiliser un groupe d'appareils infectés pour lancer une attaque contre-attaque contre un autre appareil ou service. Ces attaques peuvent être très puissantes et peuvent être difficiles à arrêter. [16]

I.2.10 Les avantages et les inconvénients du réseau IdO

- **Les avantages :**

L'Internet des objets (IdO) est une nouvelle technologie qui intègre les objets connectés, encourage la création d'un réseau mondial et nous apporte des avantages quotidiens. On peut la considérer comme une notion qui a des répercussions sur les technologies et la société dans divers secteurs tels que les secteurs privés, étatiques et industriels. En l'utilisant, l'environnement sera relié et nous pourrons entrer en communication avec lui.

- L'efficacité est améliorée par les interactions entre machines, ce qui permet aux individus de gagner du temps pour se concentrer sur d'autres tâches.

- L'automatisation permet d'uniformiser les tâches, ce qui peut améliorer la qualité des services et diminuer la nécessité d'intervention humaine.

- La diminution des dépenses : une augmentation de l'efficacité et de l'automatisation permet de diminuer à la fois les déchets et les dépenses liées à la main-d'œuvre, ce qui rend la production et la livraison des marchandises plus abordables.

- La communication entre les appareils est améliorée grâce à l'IdO, ce qui permet un contrôle de qualité plus efficace.

- L'accès aux informations depuis n'importe quel endroit, à tout moment et sur n'importe quel appareil peut faciliter la prise de décision et renforcer la transparence.

- **Les inconvénients :**

- L'automatisation accélérée par l'IdO pourrait entraîner la suppression de postes qualifiés sur le marché du travail.

- En raison de la grande taille du réseau de l'IdO, qui dépend de nombreux appareils, une seule panne logicielle ou matérielle pourrait entraîner des conséquences considérables.

- La confidentialité et la sécurité sont essentielles : avec un nombre élevé d'appareils connectés à internet, une grande quantité d'informations est disponible en ligne. Les dangers pour la vie ce qui met la sécurité en danger privé et la sécurité en découlent. [17]

I .3 Conclusion

L'IdO est une technologie en plein essor qui a le potentiel de transformer de nombreux aspects de notre vie. L'IdO offre de nombreux avantages, mais il existe également des défis à relever, tels que l'interopérabilité, la sécurité et la confidentialité
Dans ce chapitre, nous avons défini l'Internet des Objets (l'IdO), Nous avons cité brièvement les domaines d'applications et leurs composants, par la suite, nous avons parlé de la motivation , l'architecture et les différents protocoles de l'IdO. Dans le prochain chapitre, nous présentons le protocole de routage pour les réseaux à faible consommation et à perte (RPL) et nous expliquerons son fonctionnement, puis nous parlerons de ses défis ainsi que ses avantages et ses inconvénients .

Chapitre II: Protocole de routage pour les réseaux avec perte et faible consommation d'énergie

II.1 Introduction:

Le protocole RPL est un protocole de routage proactif basé sur le protocole IPv6 (Internet Protocol version6). Le groupe de travail ROLL de l'IETF l'a développé en 2012 pour les LLN. Le bon déroulement de ce protocole est assuré par la création d'un graphe nommé DODAG (Graphe Directement Orienté Destination Acyclique). Dans ce chapitre, nous allons discuter du fonctionnement de la RPL en citant la procédure de construction et en citant les modes de fonctionnement « ne pas stocker », « mode de stockage », formulaires de contact, puis nous expliquerons les étapes et les défis de la simulation RPL et les applications du protocole RPL en mentionnant les avantages et les inconvénients RPL.

II.2 Définition du protocole RPL

Le Protocole de routage pour les réseaux sans fil à faible énergie et à faible bande passante (RPL) est spécialement développé pour répondre aux exigences d'énergie et de bande passante des réseaux sans fil. Il utilise une méthode proactive afin de créer une arborescence de réseau appelée graphique acyclique direct (DAG) orientée vers la destination (DODAG). RPL a pour mission de déterminer la meilleure façon de transmettre les données entre les différents appareils du réseau. [18]

II.3 Fonctionnements du protocole RPL

II.3.1 Les graphes DAG et DODAG

DAG (graphe orienté acyclique) est un graphe orienté qui ne possède pas de circuit. Il décrit les liens orientés entre les nœuds, se terminant à un ou plusieurs nœuds racines. RPL s'appuie sur la notion de DODAG (graphe acyclique orienté vers la destination), DODAG est un DAG a une seule destination à la racine c'est-à-dire à une seule racine DAG. [19]

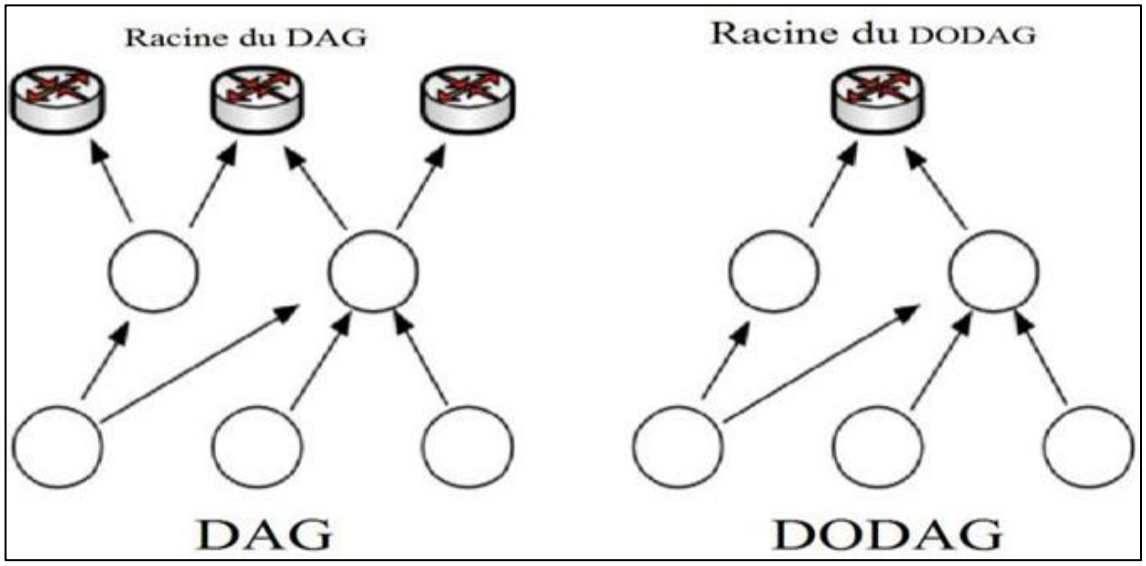

Figure II.1 : Les graphes DAG et DODAG.

II.3.2 Les messages de contrôle dans RPL

Il existe principalement quatre types de message de contrôle décrits comme suit :[20]

1. **DIO**: Le message initial est connu sous le nom de DIO (DODAG Information Object), il sert à générer des routes ascendantes afin de permettre à un nœud de localiser une instance RPL et de la rejoindre. Seuls les paramètres requis pour établir la topologie sont fournis par la racine RPL, tandis que les autres nœuds ne sont que des relais. Les DIO sont diffusés en sens inverse dans le réseau et sont par défaut diffusés en multidiffusion, mais peuvent aussi être diffusés en monodiffusion sur demande d'un nœud spécifique.

2. **DIS** (Sollicitation Information DODAG): Le deuxième message, connu sous le nom de DIS (DODAG Information Sollicitation), est utilisé par un nœud afin de se connecter à la topologie (diffusion en multidiffusion) afin de demander des informations de configuration plus récentes sur le DODAG. Chaque nœud qui reçoit un DIS répond à l'initiateur en diffusant un paquet DIO en monodiffusion. En d'autres mots, il sollicite un message de Dieu.

3. **DAO** (Destination Annonce Objet): Le troisième message, appelé DAO (DODAG Advertisement Object), est utilisé exclusivement lorsque des routes descendantes sont requises (par exemple, pour le trafic point à point).
Autrement, il peut être désactivé afin de faire des économies de ressources. Le DAO est envoyé à la racine RPL en mode de fonctionnement non-conservation, tandis qu'en mode de conservation, il est envoyé aux parents. À la différence des autres messages de contrôle RPL, le DAO doit toujours être envoyé en monodiffusion et doit être confirmé par le destinataire.

4. **DAO-ACK**: Le message DAO-Ack (DAO-Acknowledgment) est le quatrième message que le nœud parent envoie au nœud fils en réponse à son message DAO reçu afin de confirmer la réception. En cas d'absence de DAO-Ack, la source a la possibilité de réémettre le DAO initial.

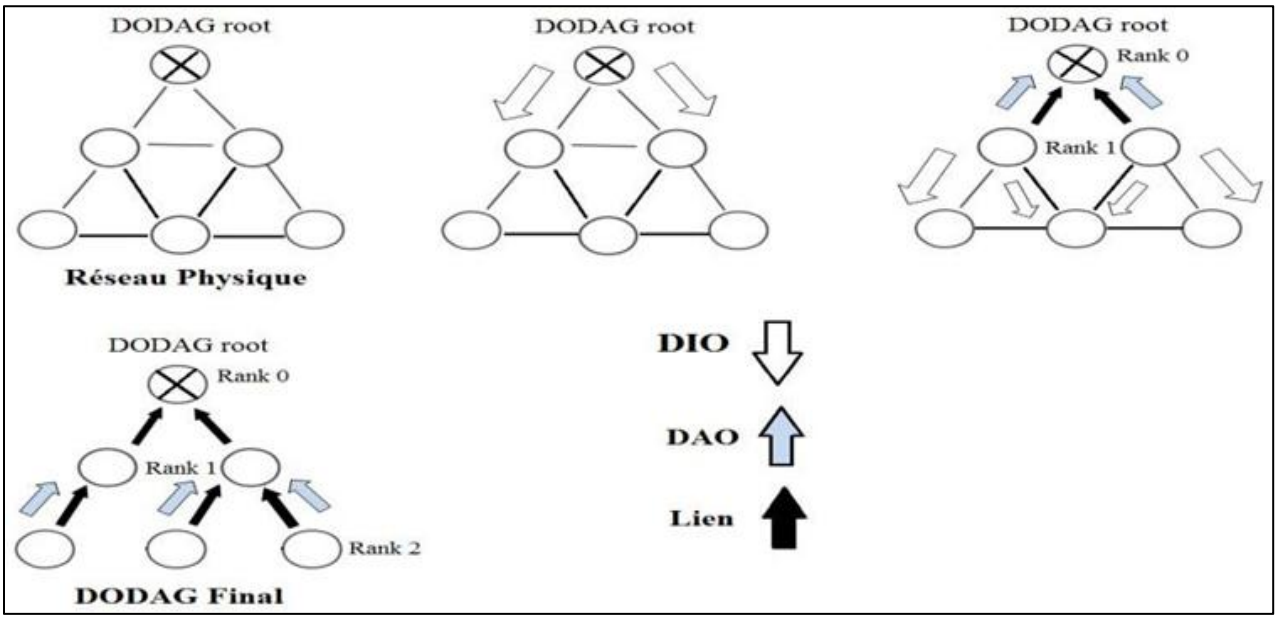

Figure II.2 : L'envoie des messages DIO et DAO et la construction de DODAG.

II.3.3 Les types des nœuds dans RPL

1. Routeurs de bordure à faible consommation d'énergie et à perte(LBR)

Il s'agit du root d'un DODAG qui représente un point de collecte dans le réseau et a la capacité de construire un DAG. Le LBR agit comme un dispositif de routage ou l'agrégateur et agit comme une passerelle (ou routeur périphérie) entre internet et le LLN. [21]

2. Routeur

Il s'agit d'un appareil qui peut transférer et générer du trafic. Un tel routeur n'a pas la possibilité de créer un nouveau DAG, mais de s'associer à un existant. [21]

3. Hote

Il s'agit d'un périphérique final capable de générer du trafic de données, mais qui n'est pas en mesure de transférer le trafic. [21]

II.3.4 Identifiants RPL et procédure de construction

Le DODAG est construit en utilisant le protocole de découverte des voisins (ND) utilisé avec l'IPv6. Le graphe DODAG est élaboré de manière progressive : [22]

• **Etape 1:** La racine du DODAG commence le processus de construction de DODAG en diffusant régulièrement un message DIO à tous ses nœuds voisins. Ce message communique des informations essentielles telles qu'un DODAGID, sa fonction Objectif, ainsi que des données pour permettre aux nœuds de déterminer leur position dans le DODAG, afin de créer et maintenir le graphe DODAG. La position d'un nœud dans le graphe est calculée en fonction de sa position par rapport à la racine et doit toujours être supérieure au rang de ses parents.

• **Etape 2:** Quand un nœud RPL reçoit un message DIO, il doit d'abord prendre la décision de l'accepter ou non. Si il ne répond pas à certains critères définis par RPL, il sera renvoyé. Autrement, le nœud effectue la manipulation du message DIO.

• Étape **3:** Après avoir reçu un premier message DIO et choisi de rejoindre le DODAG, un nœud ajoute l'adresse de l'émetteur DIO à sa liste de parents et calcule son rang. Ensuite, il communique le message DIO contenant les données de mise à jour du rang à ses voisins. En se basant sur sa liste de parents, le nœud choisit un parent privilégié qui devient la passerelle première à utiliser lorsque des données doivent être transmises vers la base du DODAG.

• **Étape 4:** Lorsqu'un nœud est déjà lié à un DODAG et reçoit un autre message DIO, il effectue le calcul de son nouveau rang et le compare à l'ancien. En cas d'infériorité du nouveau rang, le nœud ajoute l'expéditeur du message à sa liste de parents et le sélectionne comme nouveau parent favori. Après cela, le nœud actualise le message DIO en utilisant le nouveau rang et le communique à ses voisins. Sinon, si le nouveau rang calculé est supérieur à l'ancien, le nœud ne met pas à jour le rang ni ne transmet pas de message DIO.
Il garde l'ancien parent préféré.

• **Étape 5:**Un nœud qui n'a pas reçu de message DIO et qui n'est pas lié à un DODAG a la possibilité de demander des informations sur le réseau en envoyant régulièrement des messages DIS aux voisins.

• **Étape 6:** À la fin de cette procédure, tous les nœuds impliqués dans le graphe DODAG ont une trajectoire par défaut en direction de la racine du DODAG.

II.3.5 Maintenance de la topologie

Si un lien est rompu, le DODAG peut être réparé de deux manières différentes: [23]
Réparation globale : La reconstruction complète du DODAG est effectuée par la racine en utilisant les messages DIO, afin de distinguer les DODAG anciens et nouveaux. Les numéros de séquence sont utilisés pour distinguer les DODAG anciens et nouveaux.

Réparation locale : Le nœud atteint se penche sur une nouvelle source dans ses environs. Une nouvelle optimisation ne peut être obtenue que par une réparation globale.

II.3.6 Le fonctionnement de l'algorithme trickle timer

RPL utilise le Trickle Timer pour réduire la surcharge des messages de contrôle en ne transmettant les mises à jour que lorsque des incohérences sont détectées dans le réseau. Si un nœud entend des mises à jour DIO de ses voisins qui sont cohérentes avec sa propre compréhension de la topologie de réseau, un compteur de redondance est incrémenté. Si le nombre de mises à jour cohérentes entendues dans un intervalle de temps particulier dépasse le nombre de redondances, le nœud ne transmet aucune mise à jour et la période d'écoute est doublée. Toutefois, si une mise à jour incohérente est entendue, Trickle Timer est réinitialisé et une mise à jour est rapidement propagée. [24]

II.4 les modes d'opération du protocole RPL

II.4.1 Fonctionnement en « Non-Storing mode »

Tous les messages descendants doivent d'abord passer par le nœud racine, puisque seule la racine possède des informations de routage descendantes. [25]

II.4.2 Fonctionnement en « Storing mode »

Dans ce mode, les nœuds intermédiaires ont la capacité de stocker des informations de routage afin de pouvoir rediriger les données reçues vers la destination appropriée. [25]

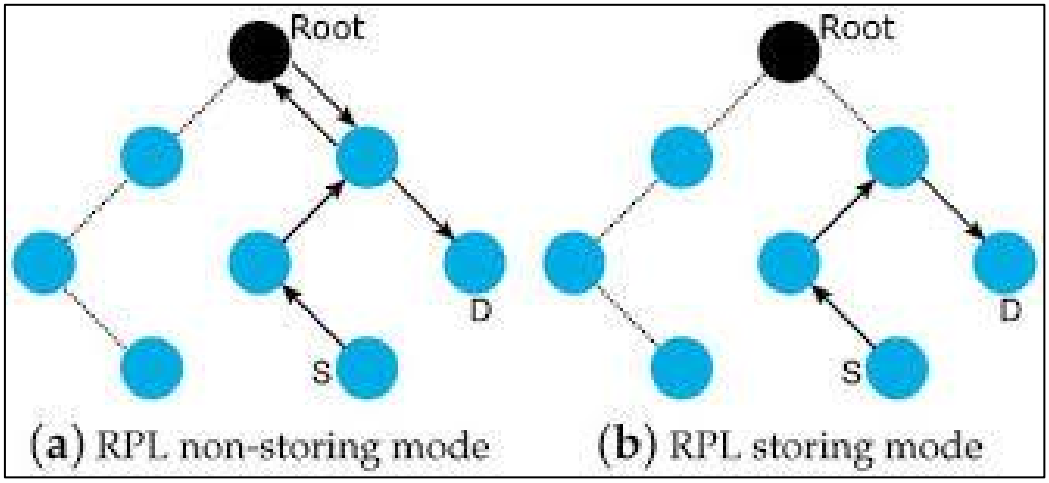

Figure II.3 : Les modes d'opération du protocole RPL .

II.5 Les paradigmes de communication du protocole RPL

Multipoint à point (MP2P) :

Le RPL a été développé principalement dans le but d'améliorer le flux de trafic multipoint à point (MP2P). Cette communication MP2P a été fournie par les constructions de routes à partir de chaque nœud vers la racine DODAG en utilisant le DIO du parent préféré d'un nœud, appelé "Routes ascendantes". Les destinations des flux MP2P sont des nœuds désignés qui ont une certaine importance pour l'application, tels que la fourniture de connectivité à l'Internet ou au réseau IP privé principal. [26]

Point à multipoint (P2PM) :

Il s'agit de Routes descendantes (Downward Routes), RPL prend en charge le trafic P2MP il utilise un mécanisme de publicité de destination qui prévoit des itinéraires descendants de la racine vers d'autre nœuds. [26]

Point à point (P2P) :

Paquet se la construction des routes pour le trafic P2P est influencée par le fonctionnement du protocole RPL. Si le paquet se dirige vers une racine en mode non-storing, la racine effectuera le routage vers la destination. Lorsque le mode STORING est activé, le paquet se déplace vers la racine jusqu'à ce qu'il atteigne un ancêtre dont la route vers la destination est connue. Cela peut être l'ancêtre commun de DODAG. Dans d'autres cas, il peut s'agir d'un nœud plus proche de la source ou de la destination. [26]

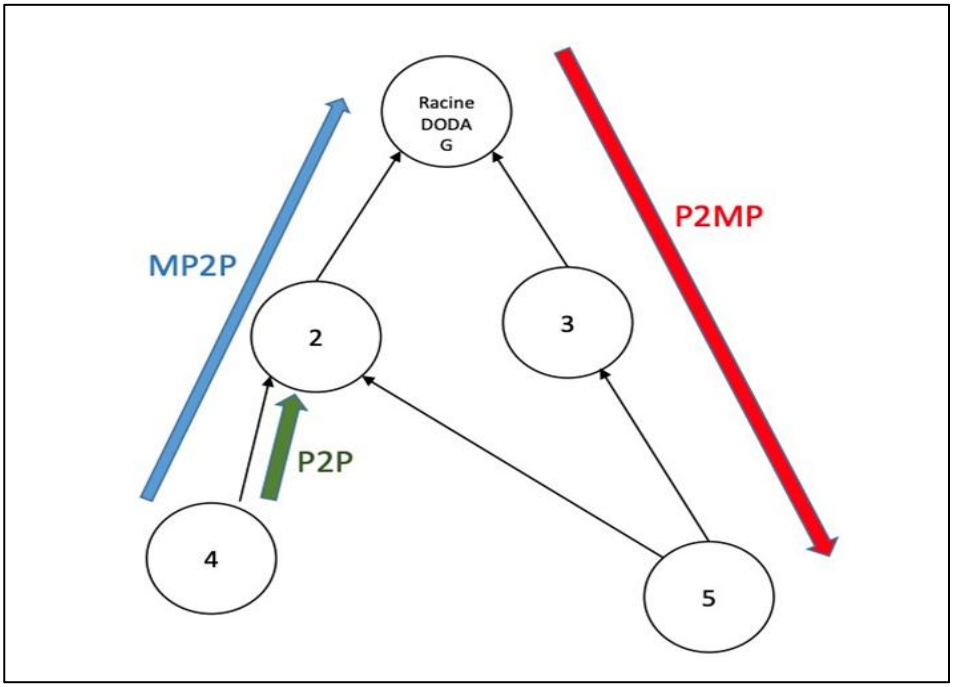

Figure II.4 : Modèles de communication .

II.6 limite du protocole RPL

De nombreuses études ont prouvé que RPL fait face à des obstacles qui limitent son efficacité et son domaine d'application. :

La réglementation RPL demande que chaque nœud qui utilise un mode "storing " maintienne l'état de routage de tous les nœuds de son sous-DODAG. Même si RPL a été spécialement développé pour les nœuds avec une mémoire limitée, son objectif est de gérer des réseaux denses qui englobent jusqu'à des milliers. Dans de tels réseaux à forte densité, il est fort probable que la capacité de stockage de ces périphériques contraints dépasse la capacité de routage nécessaire. Donc, un nœud débordé ne sera pas en mesure de gérer toutes les entrées de routage qui doivent être conservées dans sa table de routage, ce qui rend plusieurs destinations de son sous-DODAG inaccessibles par la racine DODAG.

Lorsque le mode de non-stockage est utilisé, il est nécessaire que la racine ait un en-tête de route source (la liste des différents nœuds relayeurs vers la destination) pour chaque paquet de données transmis dans la direction basse. Toutefois, le RPL est spécialement conçu pour être utilisé sur des couches de liaison avec une unité de transmission maximale MTU (Maximum Transmission Unit) restreinte, ce qui permet une longueur de chemin maximale de huit sauts, de la source à ce point de destination. Cela entraîne une limitation rigoureuse de la transmission à sauts multiples.

L'évolution de RPL pose toujours de nombreux défis, notamment dans les réseaux bidirectionnels à grande échelle. Cela implique que les deux méthodes d'exploitation spécifiées pour les itinéraires descendants ne sont pas efficaces.

II.7 La sécurité du protocole RPL

Dans sa version classique, RPL inclut des dispositifs de sécurité afin de garantir une bonne fonctionnalité du réseau.Trois modes de sécurité de base sont proposés par RPL : [27]

• Aucun mécanisme de sécurité n'est utilisé pour envoyer les messages de contrôle RPL, ce qui ne signifie pas que le réseau RPL n'est pas sécurisé. Il est possible d'utiliser d'autres éléments de sécurité pour assurer la sécurité des applications, comme la sécurité de la couche liaison.

• Avec des clés préinstallées : Les nœuds qui souhaitent connecter une instance RPL ont la possibilité de générer des messages sécurisés.

• Authentification : à l'instar du mode préinstallé, les nœuds possèdent des clés préinstallées qui ne peuvent être utilisées que pour se connecter à une instance RPL en tant que feuille. Il est nécessaire d'obtenir une clé d'autorité d'authentification afin de rejoindre une instance RPL authentifiée en tant que routeur.

II.8 Conclusion

Le protocole de routage RPL a été créé par le groupe de travail ROLL afin de satisfaire les contraintes très particulières des réseaux LLN. Le protocole a été élaboré dans le but d'être extrêmement adaptable aux diverses fluctuations des ressources du réseau.
Ce chapitre a abordé la définition du protocole RPL. Après avoir brièvement mentionné leur fonctionnement et leur mode d'opération, nous avons ensuite abordé ses défis ainsi que les avantages et les inconvénients. Dans le chapitre suivant, nous exposons Les attaques et les mécanismes de sécurité de protocole RPL.

Chapitre III: Les attaques et les mécanismes de sécurité de protocole RPL

III.1 Introduction

Le protocole RPL est exposé à diverses attaques de sécurité lors du transfert de paquets de données entre les appareils. Les caractéristiques des réseaux LLN, telles que les ressources limitées, le manque d'infrastructure, la sécurité physique limitée, les topologies dynamiques et les liaisons peu fiables, les rendent particulièrement vulnérables et difficiles à défendre contre les attaques. Ça peut-être bien que spécifique au protocole RPL, il s'applique également aux réseaux de capteurs sans fil, et aux réseaux filaires. [25]
Dans ce qui suit nous présenterons les attaques courantes sur RPL.

III.2 Les attaques du protocole RPL

Il existe trois type d'attaque

III.2.1 Les attaques basées sur les ressources

Ces genres d'attaques sont de deux types :
1. Les attaques directes
2. Les attaques indirectes

III.2.1.1 Les attaques directes

Attaque Hello Flooding (DIO Flooding) :

L'attaque Hello Flooding est une forme d'attaque de déni de service (DDoS) qui cherche à rendre un serveur indisponible pour le trafic légitime en utilisant toutes les ressources disponibles sur le serveur. Le principe de cette technique est de submerger le réseau de messages "Hello" falsifiés provenant d'un nœud malveillant. Le pirate peut ainsi submerger tous les ports disponibles sur une machine serveur ciblée, ce qui contraint l'appareil ciblé à répondre lentement au trafic légitime ou l'empêche complètement de communiquer. [28]

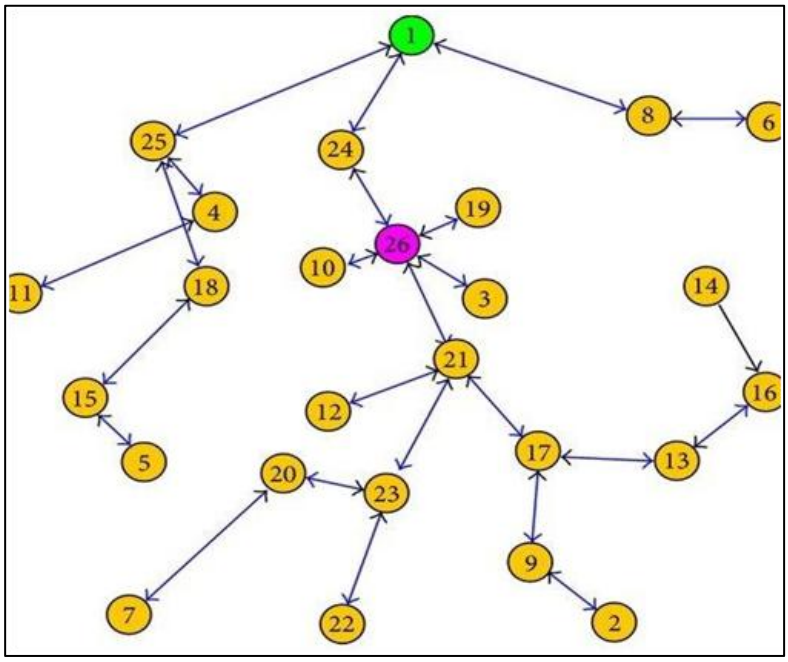

Figure III.1 : Attaque Hello flooding

III.2.1.2 Les attaques indirectes

Attaque Decrease Rank :

Les attaques de decrease rang sont l'une des attaques les plus graves qui peuvent être lancées contre le protocole RPL dans le cadre de la norme de communication IdO 6LowPAN [29]. La propriété de rang joue un rôle crucial dans la construction et l'optimisation des chemins de routage dans les réseaux RPL, ce qui constitue un type d'attaque ciblant les WSN. Un acteur malveillant manipule illégalement la propriété de rang et diffuse à ses nœuds voisins des DIO (DODAG information object) avec une fausse valeur de rang faible. Cela peut inciter les nœuds cibles à modifier leurs parents préférés et à choisir l'attaquant comme prochain saut vers la racine. [30]

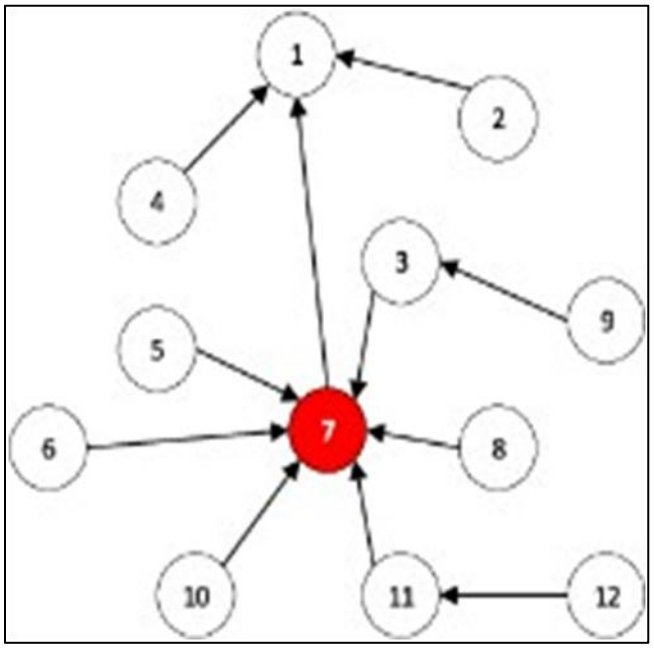

Figure III.2 : Attaque Decrease Rank

Attaque numéro de version:

Une attaque par numéro de version est une tactique malveillante utilisée pour perturber les protocoles de routage de réseau, ciblant spécifiquement le protocole de routage pour faible puissance et perte (RPL) commun dans les réseaux de l'Internet des Objets (IdO). Il doit être diffusé le numéro de version sans modification tout au long du DODAG. Seule la racine a la capacité de le modifier pour générer une nouvelle version du DODAG afin de confirmer l'intégrité du réseau et de permettre une réparation globale. En incrémentant illégalement le champ correspondant dans ses messages DIO, un attaquant peut modifier la version du DODAG avant de les transmettre à ses voisins. Cela entraînera la possibilité de créer des boucles dans le graphe et la reconstruction complète du DODAG, ce qui entraînera l'épuisement de la batterie des nœuds. [31]

III.2.2 Les attaques basées sur la topologie

Ces genres d'attaques qui sont de types :

III.2.2.1 Les attaques de sous-optimisations

Attaque Sinkhole

Une attaque de type « sinkhole » est une tactique malveillante utilisée pour perturber le flux de trafic dans un réseau. Dans les attaques de type « sinkhole » [33], un nœud malveillant annonce un chemin d'acheminement bénéfique artificiel et attire de nombreux nœuds proches pour acheminer le trafic par ce chemin. [34]

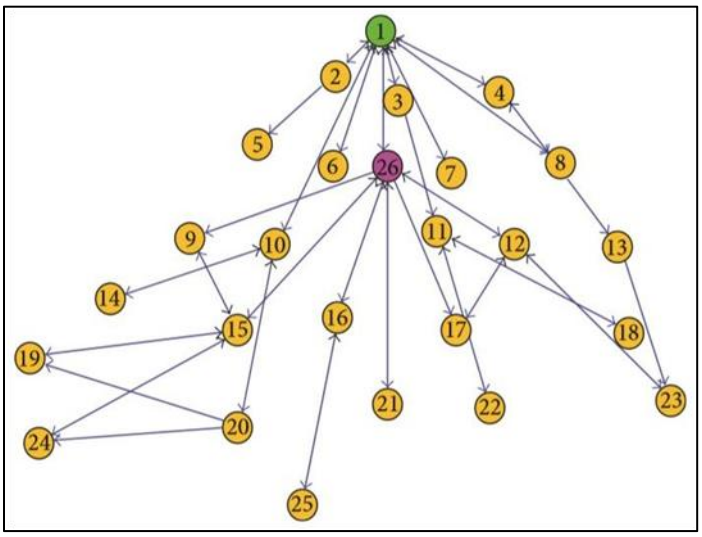

Figure III.3 : Attaque SinkHole

III.2.2.2 Les attaques d'isolements

Attaque Black-Hole:

Dans une attaque Blackhole, un noeud malveillant a pour seule mission de ne pas transférer de données, créant ainsi une sorte de trou noir dans le réseau. On peut la qualifier d'une forme d'attaque par déni de service. En cas de position stratégique de l'attaquant dans le graphique, il a la capacité d'isoler plusieurs nœuds du réseau. Il est essentiel que les nœuds communiquent de manière appropriée afin de créer un DODAG légal sans difficulté. De plus, lorsqu'une attaque blackhole est lancée, le nœud malveillant ne produit aucun message de contrôle [35]. Il est possible d'organiser une attaque Blackhole en utilisant un seul nœud malveillant ou un groupe de nœuds malveillants qui collaborent afin de rendre l'attaque plus difficile à repérer. [36]

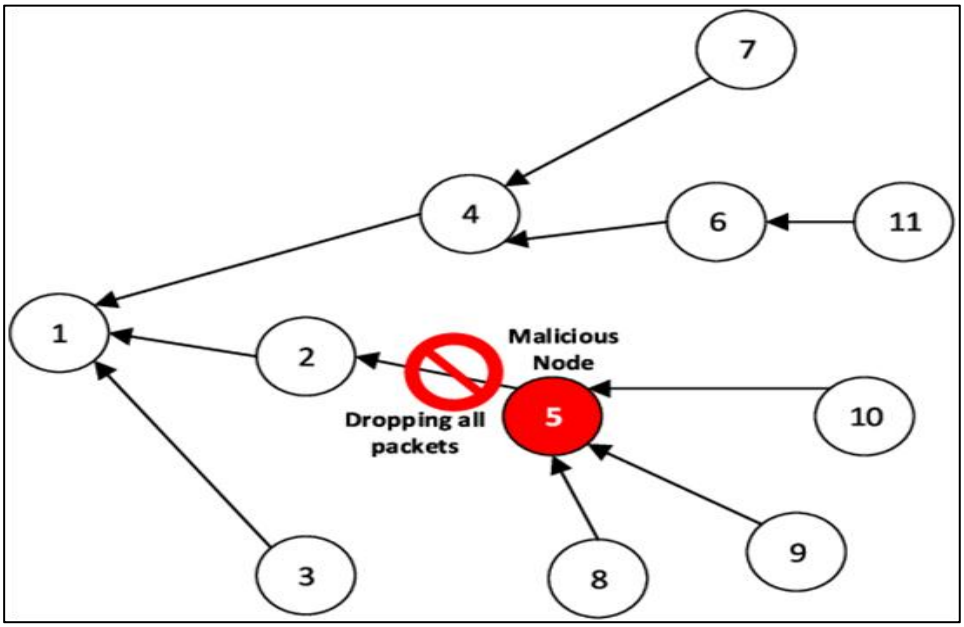

Figure III.4 : Attaque Black Hole

III.2.3 Les attaques basées sur le trafic

Ici également ces types d'attaques sont de deux types

III.2.3.1 Les attaques d'écoute :

Attaque analyse de traffic :

La technique d'attaque par analyse du trafic consiste à intercepter et analyser les messages afin de déduire des informations à partir de modèles de communication. Dans une opération d'analyse de trafic, un adversaire a la possibilité d'analyser la fréquence et le moment des paquets du réseau IdO afin d'obtenir des données essentielles. [37]

III.2.3.2 Les attaques d'imitations :

Attaque Sybil :

Sybil est aussi connue sous le nom d'attaque "un seul nœud avec plusieurs identités". Le nœud malveillant présente une identité distincte et peut être présent à plusieurs endroits simultanément, et il a la forme d'un cœur ordinaire. Il a également la possibilité d'utiliser le mécanisme de transmission DIS pour attaquer le réseau. En cas de création et de diffusion de nombreux messages DIS superposés avec différentes identités fictives, tous les nœuds récepteurs seront convaincus que de nouveaux nœuds souhaitent rejoindre le réseau, ce qui entraînera un redémarrage répété de l'algorithme Trickle et une diffusion excessive de messages DIO. Les performances du système sont altérées par cette attaque. [38]

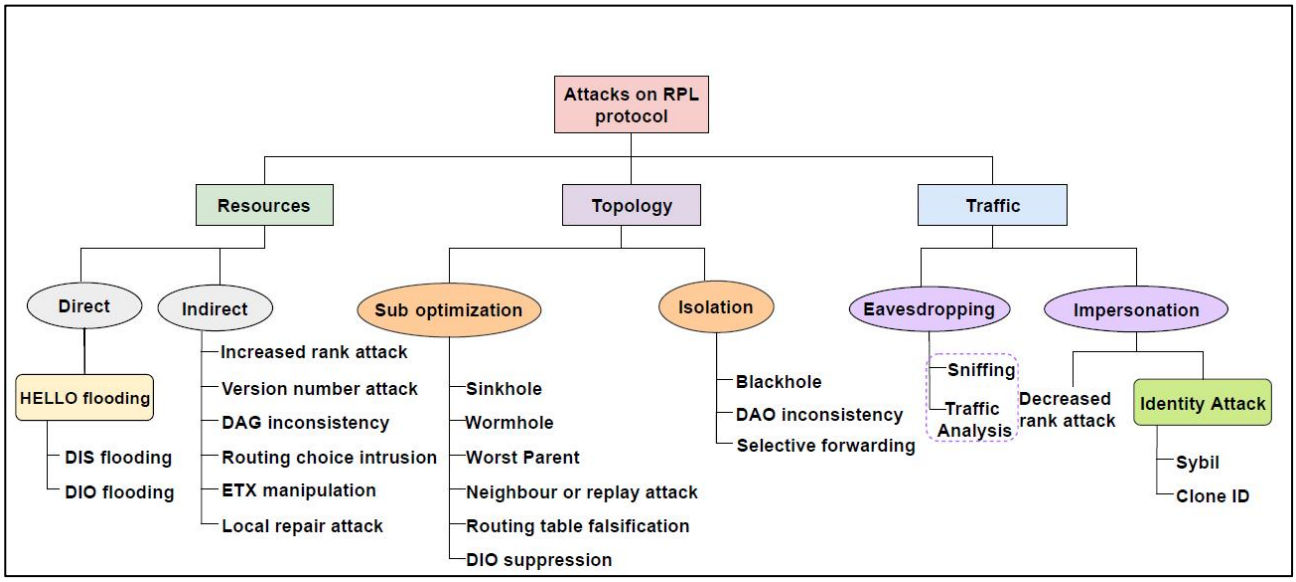

Figure III.5: Les types des attaques de protocole RPL.

III.3 Les mécanismes de sécurité du réseau RPL

Plusieurs mécanismes de défense intégrés sont disponibles dans le protocole RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) afin de protéger les réseaux maillés à faible puissance contre différentes menaces. On peut regrouper ces mécanismes en trois catégories principales.

III.3.1 Solutions basées sur le protocole sécurisé

III.3.1.1 Mécanismes de sécurité basés sur la cryptographie :

Authentification des nœuds : Les signatures numériques sont utilisées par RPL afin d'authentifier les nœuds et de garantir que seuls les nœuds autorisés peuvent accéder au réseau. Cela prévient l'infiltration de nœuds non autorisés ou malveillants dans le réseau et la perturbation de son fonctionnement.

Chiffrement des données: Il est possible d'utiliser le chiffrement des données afin de garantir la confidentialité des échanges entre les nœuds. Cela assure que des parties non autorisées ne peuvent pas intercepter et lire des données sensibles, comme les informations d'identification des utilisateurs ou les données de capteur.

Protection contre les paquets falsifiés: Les systèmes de vérification de signature utilisés par RPL permettent d'identifier et de rejeter les paquets falsifiés ou altérés. Les attaquants ne peuvent pas injecter de faux paquets dans le réseau afin de perturber le routage, voler des données ou mener d'autres attaques. [39]

III.3.1.2 Mécanismes de sécurité basés sur la confiance :

Système de réputation des nœuds: Chaque noeud peut recevoir un score de réputation selon son comportement précédent et sa fiabilité, selon RPL. Le routage des paquets est préféré à des nœuds ayant des scores de réputation élevés, tandis que les nœuds ayant des scores de réputation faibles sont évités. Cela réduit les conséquences des nœuds malveillants ou compromis sur le réseau.

Détection des nœuds malveillants: RPL a la possibilité d'utiliser des méthodes de détection d'anomalies afin de repérer les nœuds qui présentent des comportements suspects. Par la suite, il est possible d'isoler ou de mettre en quarantaine ces nœuds afin d'éviter qu'ils ne nuisent au réseau. [40]

III.3.1.3 Mécanismes de sécurité basés sur des seuils:

Seuils de durée de vie des messages:Un seuil de durée de vie maximale pour les messages est établi par RPL. En cas de dépassement de ce seuil, un message est supprimé afin d'éviter qu'il ne circule indéfiniment dans le réseau et ne provoque des collisions.

Seuils de nombre de sauts:Le seuil maximal pour le nombre de sauts qu'un message peut faire avant d'atteindre sa destination est établi par le RPL. En cas de dépassement de ce seuil, un message est supprimé afin d'éviter les boucles infinies et d'assurer une livraison efficace des paquets.

Outre ces dispositifs de protection intégrés, RPL peut aussi être combiné avec d'autres solutions de sécurité externes, comme des pare-feu ou des systèmes de détection d'intrusion, afin de garantir une protection encore plus solide.
Grâce à l'association de ces mécanismes de défense, il est possible de concevoir un réseau RPL sécurisé et fiable, capable de faire face à diverses menaces. Les mécanismes de défense les plus appropriés sont sélectionnés en fonction des besoins particuliers du réseau et des exigences de sécurité.[40]

III.3.2 Solutions basées sur le système de détection d'intrusion

Il est impossible d'appliquer directement les solutions IDS classiques à l'IdO. Les solutions IDS traditionnelles sont irréalisables en raison des nœuds limités en ressources utilisés dans le réseau, des différentes topologies de réseau et de la connectivité basée sur IP. Cela nécessite des solutions de détection d'incendie légères en ce qui concerne la surcharge de calcul, de communication, de mémoire et d'énergie. Plus spécifiquement dans le protocole RPL, l'IDS désigne la deuxième ligne de défense, chargée de détecter les anomalies dans le fonctionnement RPL. On peut classer ces solutions de défense en Signature, Anomalie, Spécification et Hybride. [41]

III.4 Conclusion

Au cours de ce chapitre, nous avons examiné les diverses attaques contre le protocole RPL, leur nature et leur classement, à savoir une attaque qui cible la topologie, les ressources ou le trafic. De plus, nous avons abordé la sécurité, les préventions telles que les IDS, etc..
En raison des milliards de dispositifs connectés en réseau, il est essentiel de sécuriser et de protéger ces dispositifs contre différentes attaques et menaces. Il est donc primordial de proposer des solutions légères de surveillance des performances et de sécurité afin de garantir la sécurité des réseaux basés sur RPL. Dans le chapitre suivant, nous allons examiner de manière plus approfondie quelques attaques, leur mise en œuvre et leur impact sur les ressources des réseaux RPL.

Chapitre IV:
Impact des attaques de type topologie sur le réseau RPL

IV.1 Introduction

La majorité des attaques IdO visent à perturber le fonctionnement du réseau, tandis que d'autres visent à l'espionner. Dans la majorité des situations, elles ont un impact sur les mesures des nœuds du réseau RPL. Dans ce chapitre, qui constitue le cœur de notre travail, examine et explique les effets de certaines attaques IdO sur les données des nœuds d'un réseau RPL. Le but est de créer des scénarios réalistes pour approfondir notre compréhension des mécanismes, des vulnérabilités et des répercussions de ces attaques sur les réseaux IdO.

IV.2 Outils d'implémentations

IV.2.1 VMware

VMware Workstation Pro est un logiciel développé par VMware, une entreprise leader dans le domaine de la virtualisation. Grâce à ce logiciel, les utilisateurs peuvent répliquer des postes de travail, des serveurs et des environnements de smartphones sur une machine virtuelle qui existe sur l'ordinateur de l'utilisateur. Il permet également aux utilisateurs de créer et d'exécuter des machines virtuelles simultanées à partir d'un seul PC principal.

La virtualisation offre de nombreux avantages. Elle permet aux développeurs de créer et de tester des applications multiplate-formes, et aux informaticiens d'avoir un accès illimité à un outil puissant. En outre, les étudiants peuvent explorer et apprendre à utiliser différents systèmes d'exploitation, et les entreprises peuvent réduire les coûts de matériel et faire fonctionner plusieurs machines virtuelles à l'aide d'ordinateurs portables dont les ressources système sont limitées. [43]

IV.2.2 Contiki OS

Contiki est un système d'exploitation basé sur un modèle d'exploitation hybride pour les réseaux à mémoire limitée tels que les LLN. Ce système a été conçu en 2004 par un groupe de développeurs de l'industrie Adam Dunkels de l'institut Suédois d'informatiques. [23]

Contiki est un logiciel open source facile à utiliser, qui met en place la pile protocolaire et une librairie complète du protocole RPL (contikiRPL), et qui est interprété en langage c.

Contiki propose un simulateur de réseau appelé Cooja.

IV.2.3 Cooja

Ce simulateur offre la possibilité de simuler divers capteurs sur lesquels un système d'exploitation et des applications seront chargés. Cooja offre également la possibilité de simuler les connexions réseaux et de communiquer avec les capteurs.

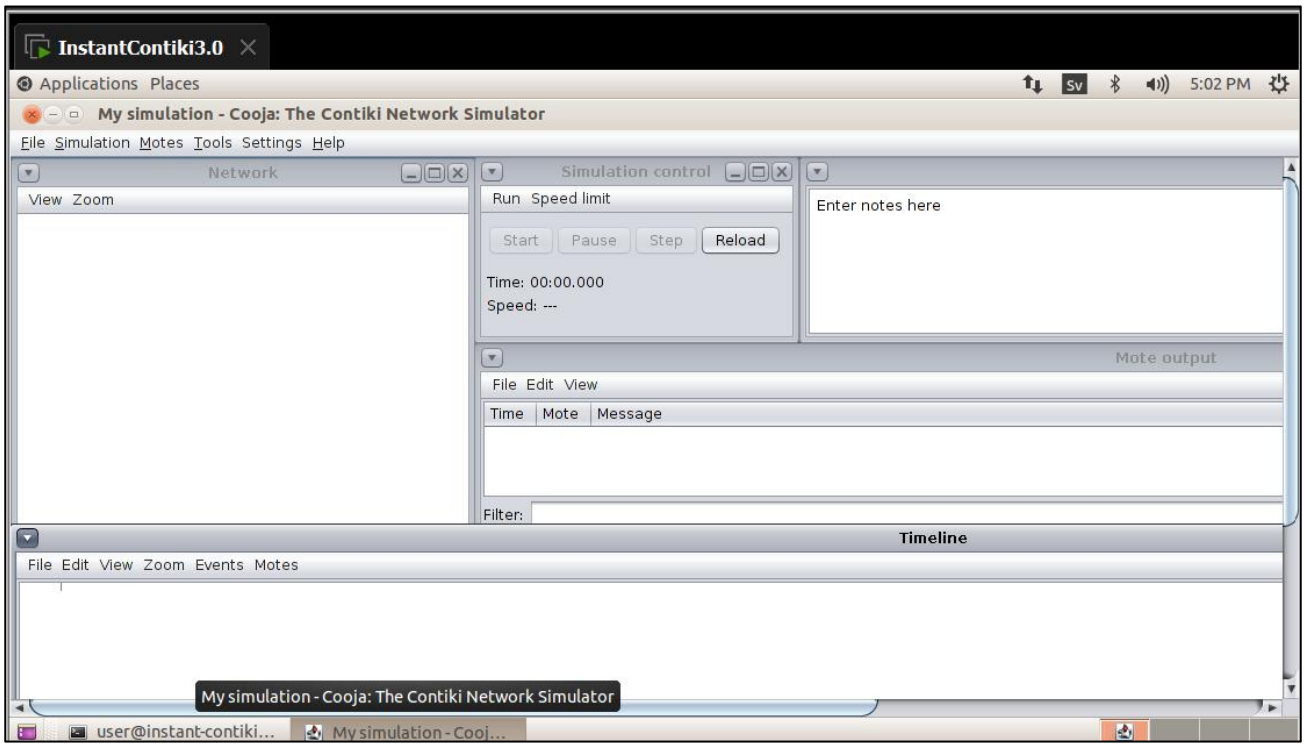

Figure IV.1 : Interface de Simulation Cooja

IV.3 Les différentes métriques d'un nœud en RPL

Les métriques sont des paramètres de test utilisés pour évaluer les performances du protocole de routage. Dans notre recherche, nous avons considéré les Métriques suivantes :

• **PDR(Packet Delivery Ratio)** : Le taux de distribution des paquets (PDR) correspond au rapport entre le nombre de paquets de données livrés à la base et le nombre de paquets envoyés par les différents nœuds du DODAG.
Le fait d'avoir un PDR élevé témoigne d'une performance accrue de la RPL.

PDR = Σ Messages reçus par la racine / Σ Messages envoyés par les nœuds de DODAG.

• **Délai de bout en bout** : Différence entre la création du paquet par l'expéditeur et la réception du paquet par le récepteur. Le retard E2E, aussi appelé délai unidirectionnel, désigne la durée requise pour que le paquet soit transmis à travers le réseau de l'expéditeur au récepteur.

Retard E2E = Somme de (Retard à l'émetteur + Retard au récepteur + Délai aux nœuds intermédiaires).

• **Énergie :** représente l'énergie consommée par l'ensemble des nœuds du réseau.

RADIO ON : La consommation d'énergie au niveau du nœud est indiquée.
RADIO TX : la transmission consomme de l'énergie.
RADIO RX : l'énergie consommée par le nœud lors de la réception.

Ces valeurs sont généralement exprimées en pourcentage.

IV.4 Implémentation et études

IV.4.1 Le cas normal

Scenario 1:
Créer un nœud serveur, illustré en jaune dans Figure IV.2, ainsi que 5 nœuds clients, illustrés en vert, puis de lancer la première simulation 8 minutes.

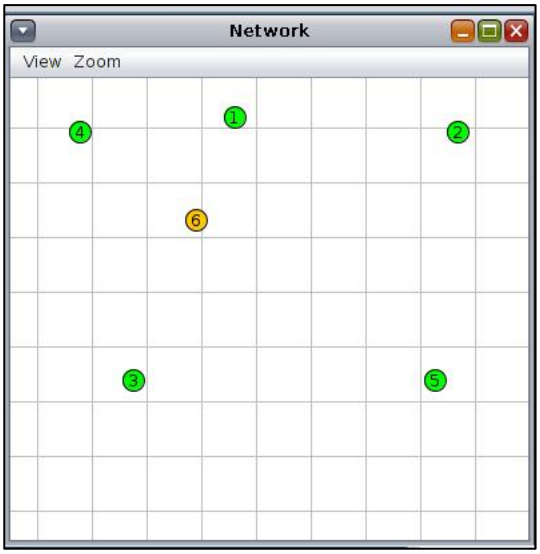

Figure IV.2 : Topologie de réseau en Scenario 1 .

Scenario 2:
Créer un nœud serveur, illustré en jaune dans Figure IV.3, ainsi que 15 nœuds clients, illustrés en vert, puis de lancer la première simulation 8 minutes.

Figure IV.3 : Topologie de réseau en Scenario 2 .

Scenario 3:
Créer un nœud serveur, illustré en jaune dans Figure IV.4, ainsi que 25 nœuds clients, illustrés en vert, puis de lancer la première simulation 8 minutes.

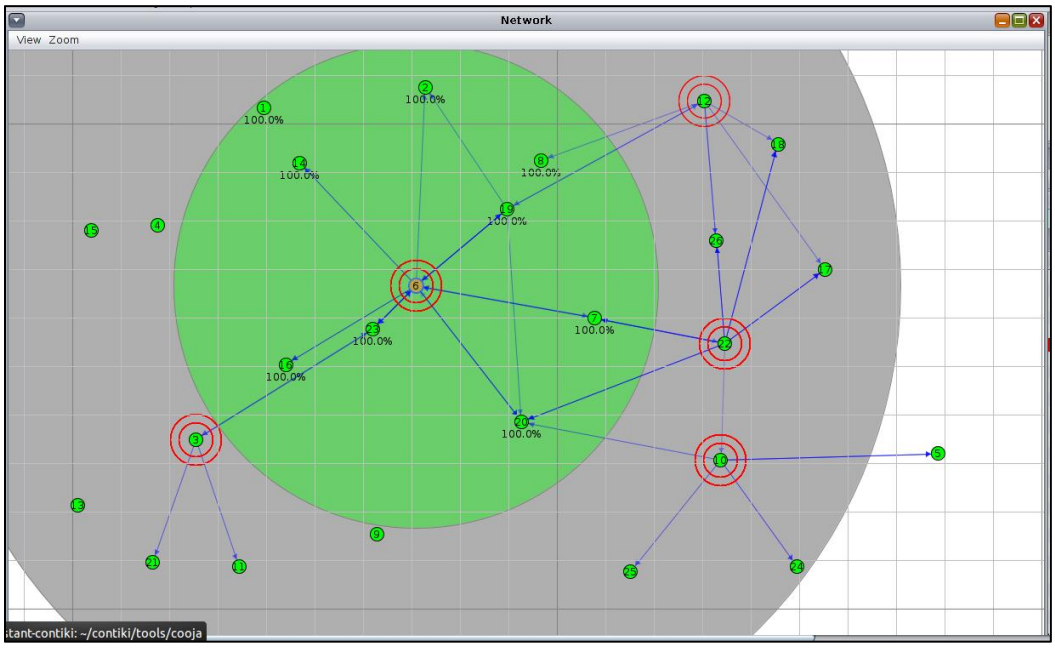

Figure IV.4 : Topologie de réseau en Scenario3 .

IV.4.2 Attaque Blackhole

Lors de cette attaque, l'attaquant prétend avoir trouvé le meilleur chemin pour atteindre la destination après avoir violemment modifié son rang. Il refuse de recevoir les paquets de routage de ses victimes et ne les distribue pas au point de destination précis.

Scenario 1:
Créer un nœud serveur, illustré en jaune dans Figure IV.5, ainsi que 5 nœuds clients, illustrés en vert, ainsi que 2 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.5.
Les conséquences de cette attaque seront analysées et interprétées après une simulation de 8 minutes.

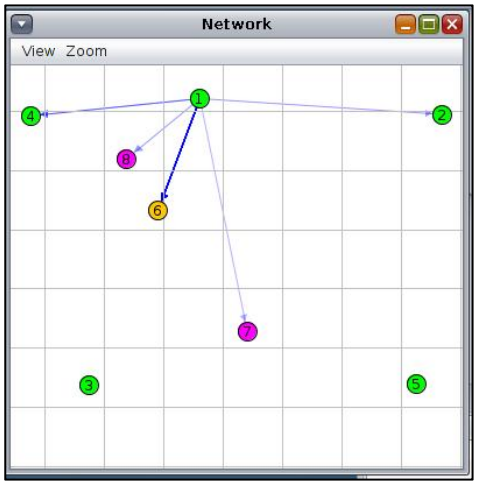

Figure IV.5 : Topologie de la simulation de Blackhole en Scenario 1.

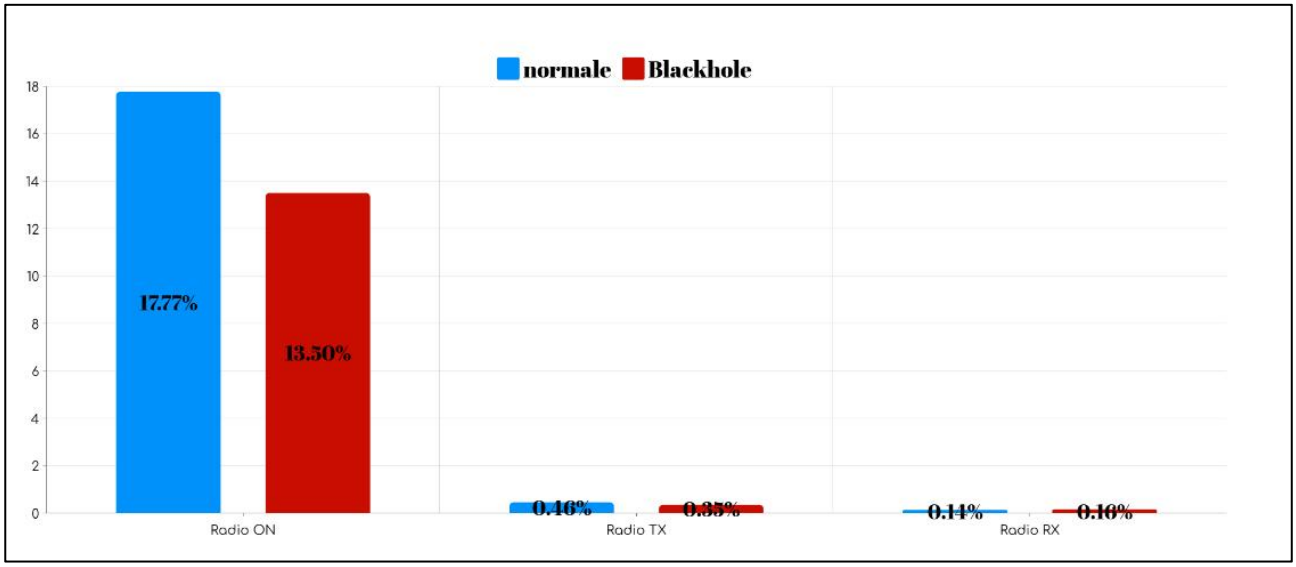

Figure IV.6 : Diagrammes à barres comparant la consommation d'énergie en Scenario 1.

Scenario 2:

Créer un nœud serveur, illustré en jaune dans Figure IV.7, ainsi que 15 nœuds clients, illustrés en vert, ainsi que 4 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.7.

Les conséquences de cette attaque seront analysées et interprétées après une simulation de 8 minutes.

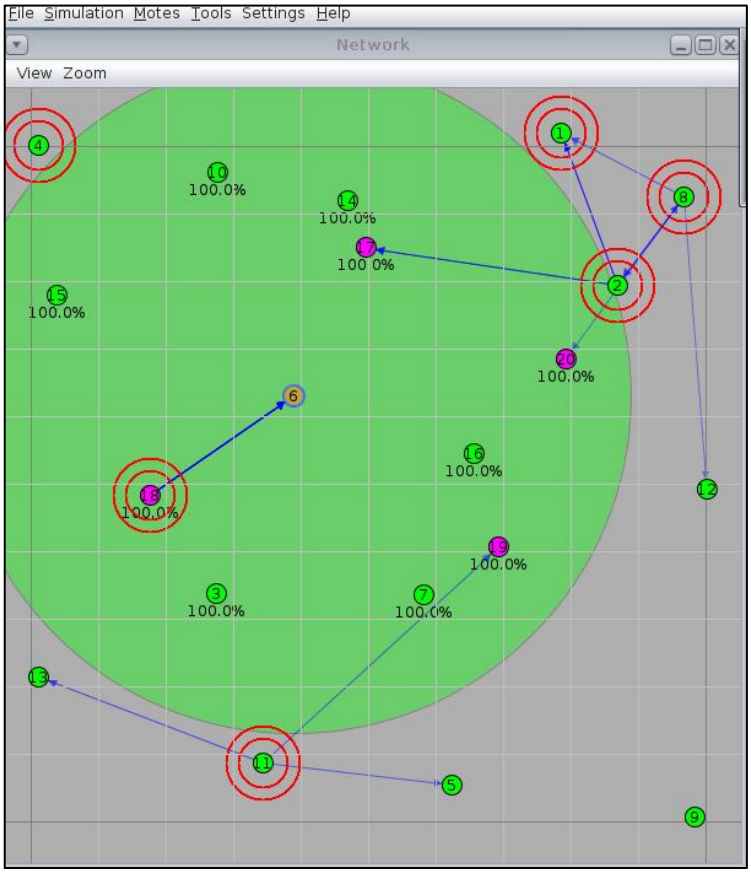

Figure IV.7 : Topologie de la simulation de Blackhole en Scenario 2.

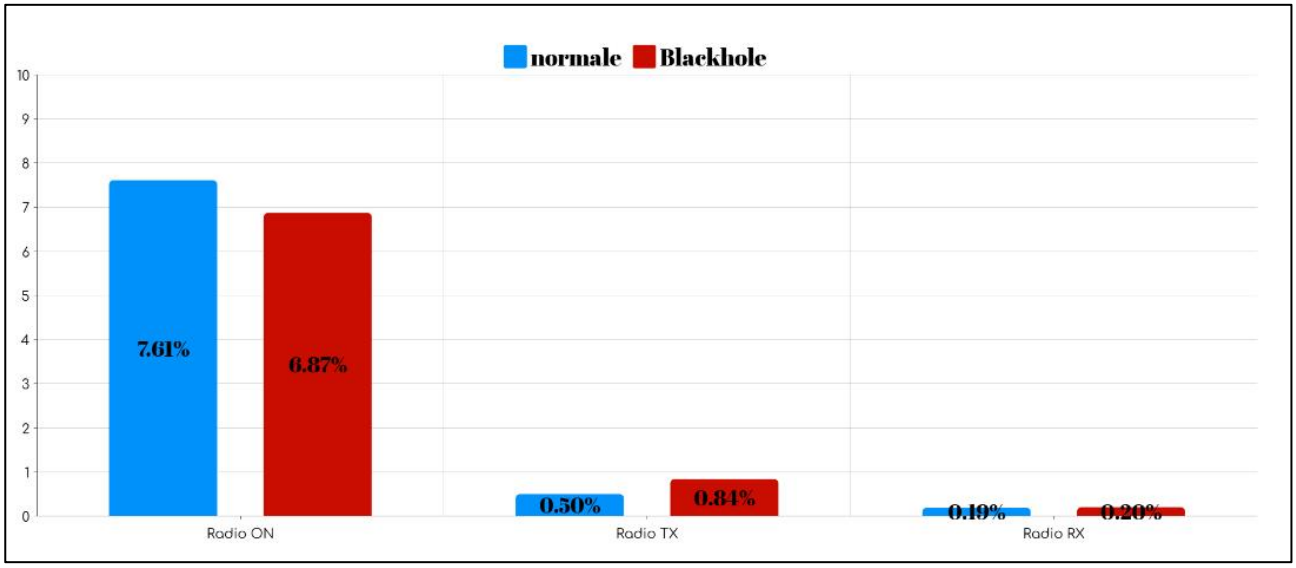

Figure IV.8 : Diagrammes à barres comparant la consommation d'énergie Scenario 2.

Scenario 3:

Créer un nœud serveur, illustré en jaune dans Figure IV.9, ainsi que 25 nœuds clients, illustrés en vert, ainsi que 3 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.9.

Les conséquences de cette attaque seront analysées et interprétées après une simulation de 8 minutes.

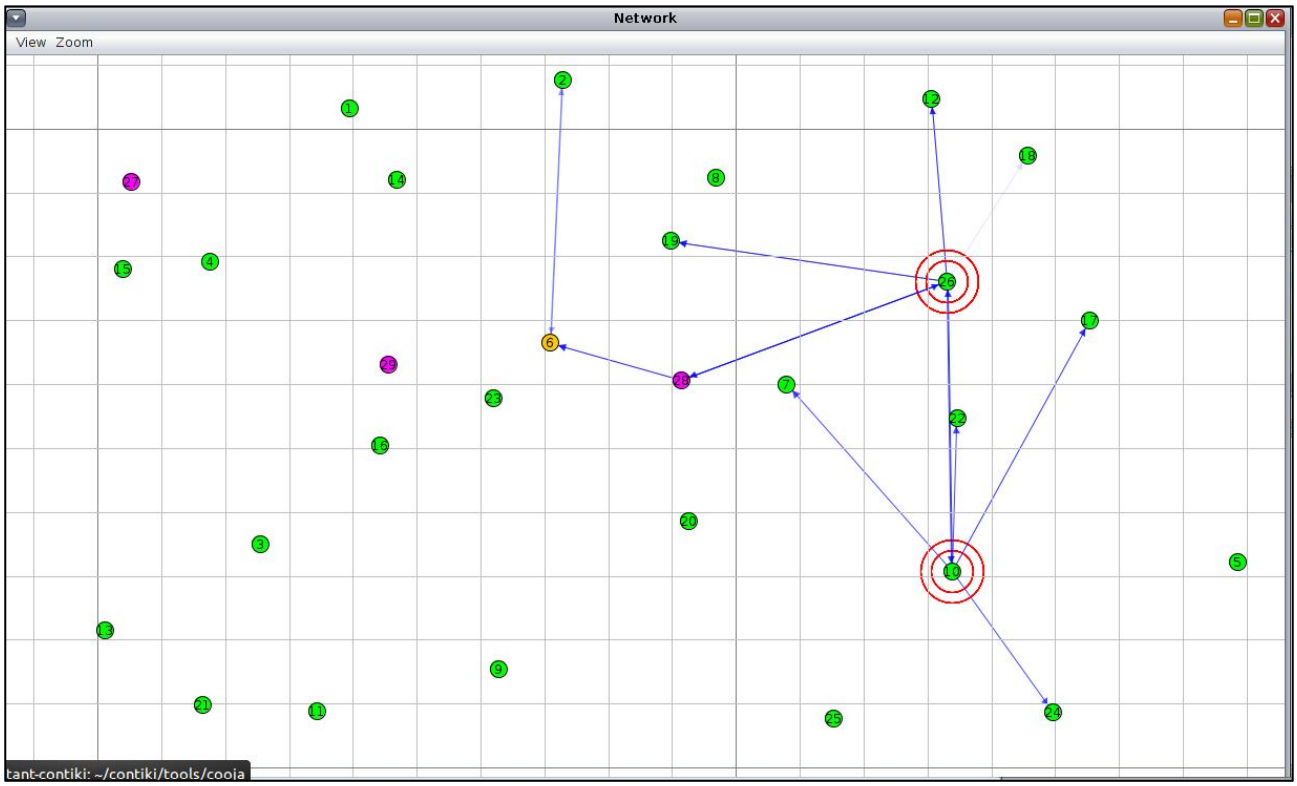

Figure IV.9 : Topologie de la simulation de Blackhole en Scenario 3.

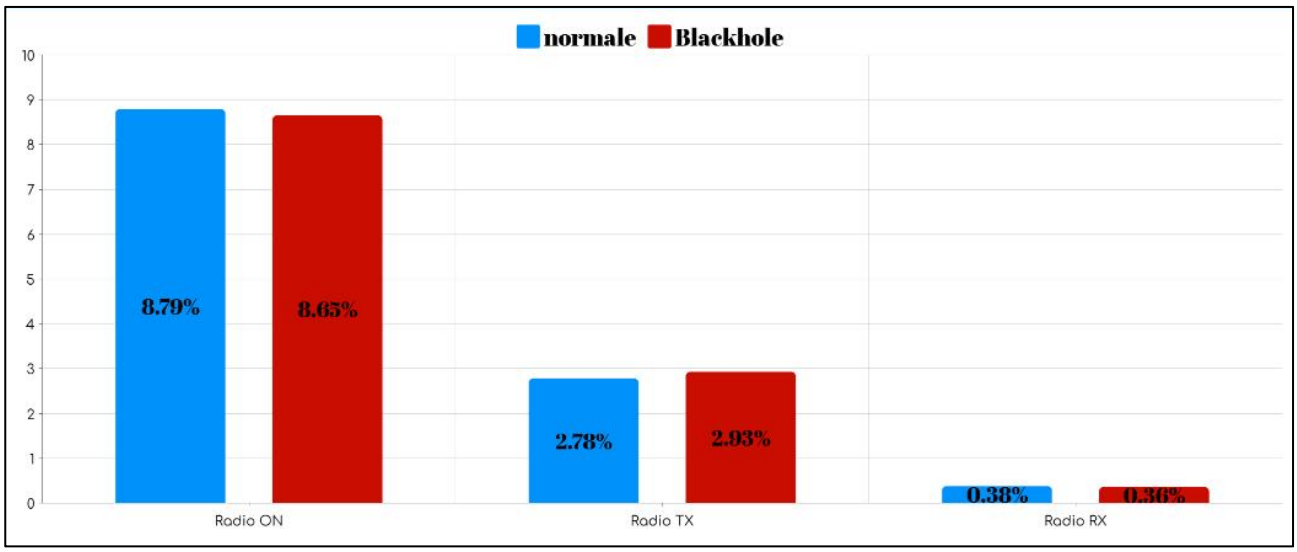

Figure IV.10 : Diagrammes à barres comparant la consommation d'énergie Scenario 3.

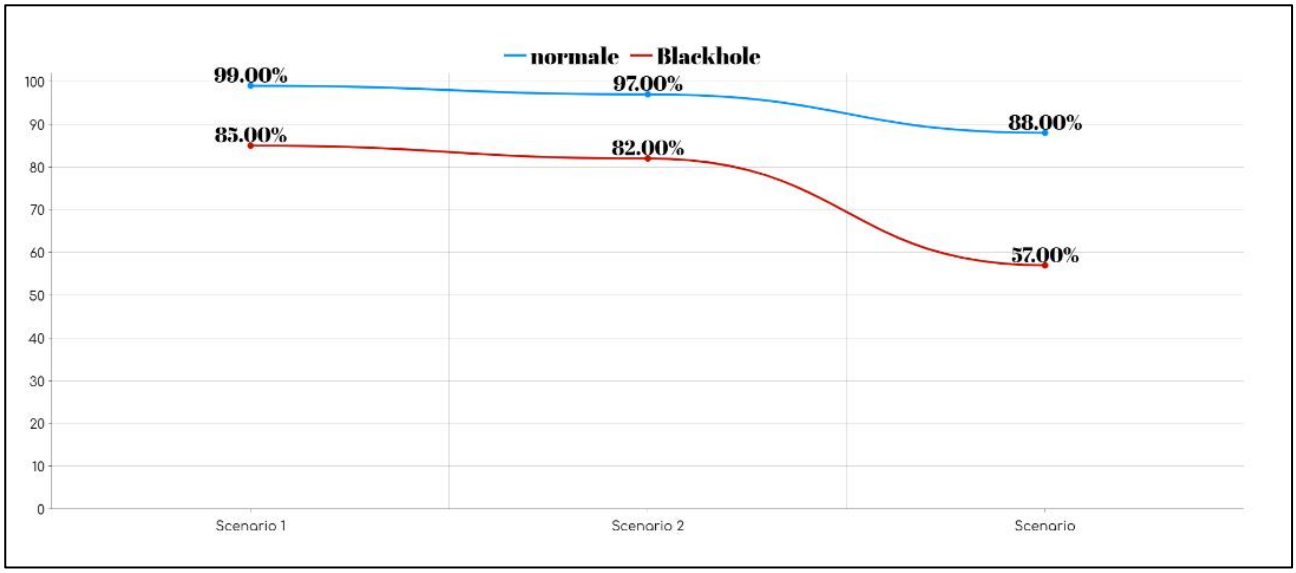

Figure IV.11: Courbe graphique comparant la valeur de PDR en les 3 Scenarios.

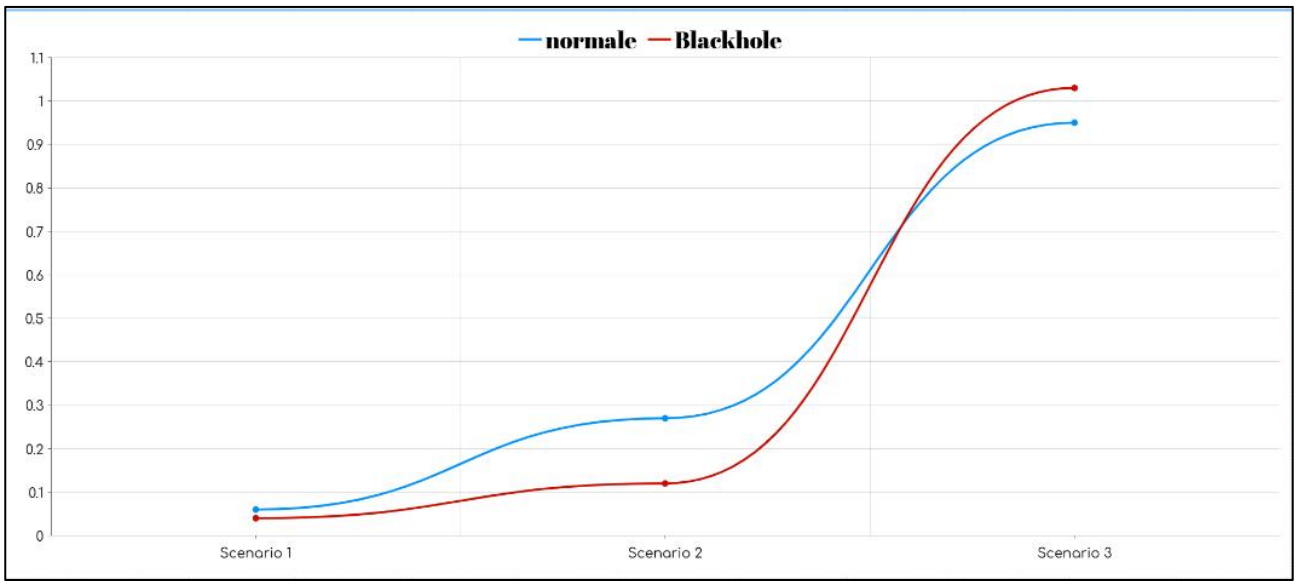

Figure IV.12: Courbe graphique de délai de bout en bout en les 3 Scenarios.

IV.4.3 Attaque Sinkhole

Ce type d'attaque consiste à attirer le trafic réseau en se faisant passer pour un nœud légitime dans le processus de routage. La station de base est entravée dans l'accès aux informations légitimes, crée une menace et ouvre la voie à d'autres attaques également. Le compromis tente d'éliminer les paquets.

Scenario 1:

Créer un nœud serveur, illustré en jaune dans Figure IV.13, ainsi que 5 nœuds clients, illustrés en vert, ainsi que 2 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.13.
Les conséquences de cette attaque seront analysées et interprétées après une simulation de 6 minutes.

Figure IV.13 : Topologie de la simulation de Sinkhole en Scenario 1.

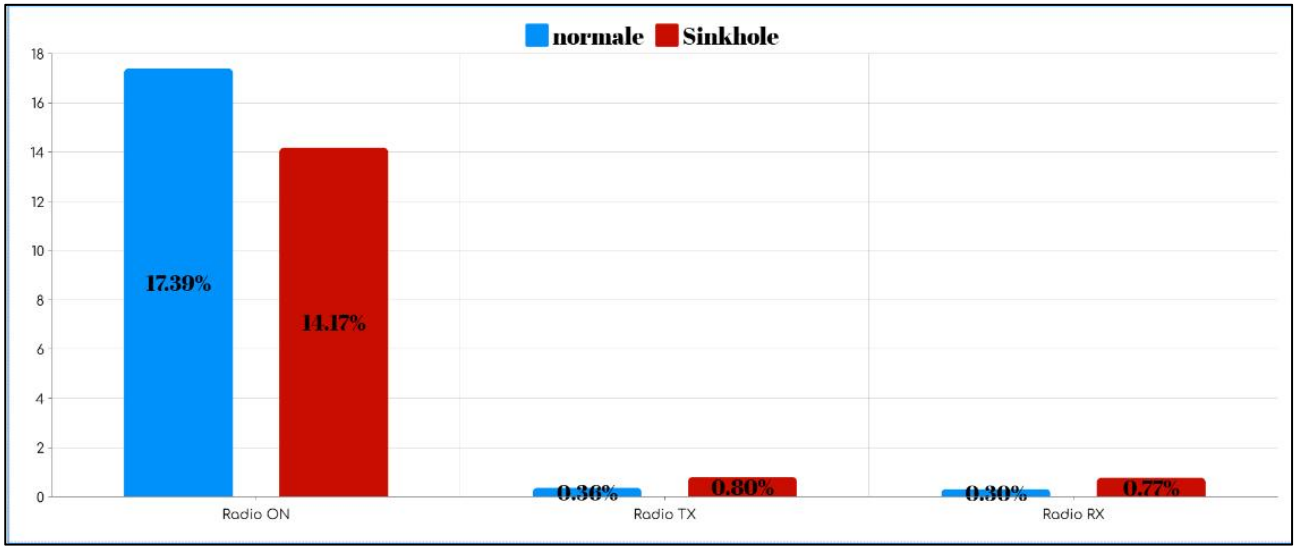

Figure IV.14 : Diagrammes à barres comparant la consommation d'énergie Scenario 1.

Scenario 2:

créer un nœud serveur, illustré en jaune dans Figure IV.15, ainsi que 15 nœuds clients, illustrés en vert, ainsi que 4 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.15.

Les conséquences de cette attaque seront analysées et interprétées après une simulation de 6 minutes.

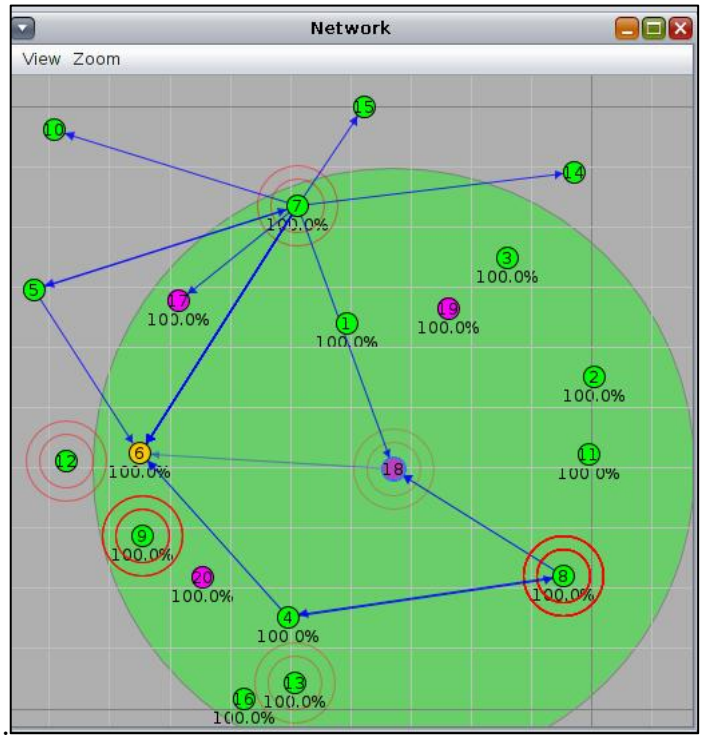

Figure IV.15 : Topologie de la simulation de Sinkhole en Scenario 2.

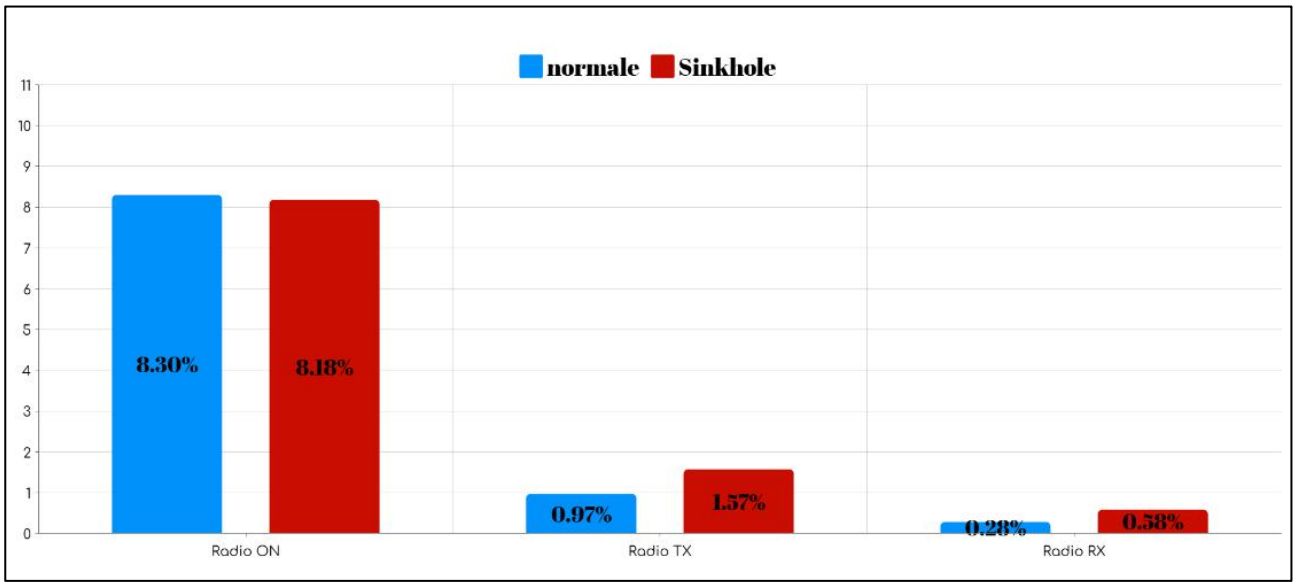

Figure IV.16 : Diagrammes à barres comparant la consommation d'énergie Scenario 2.

Scenario 3:

créer un nœud serveur, illustré en jaune dans Figure IV.17, ainsi que 25 nœuds clients, illustrés en vert, ainsi que 3 nœud malveillant (Violette) que l'on peut observer dans la Figure IV.17.

Les conséquences de cette attaque seront analysées et interprétées après une simulation de 6 minutes.

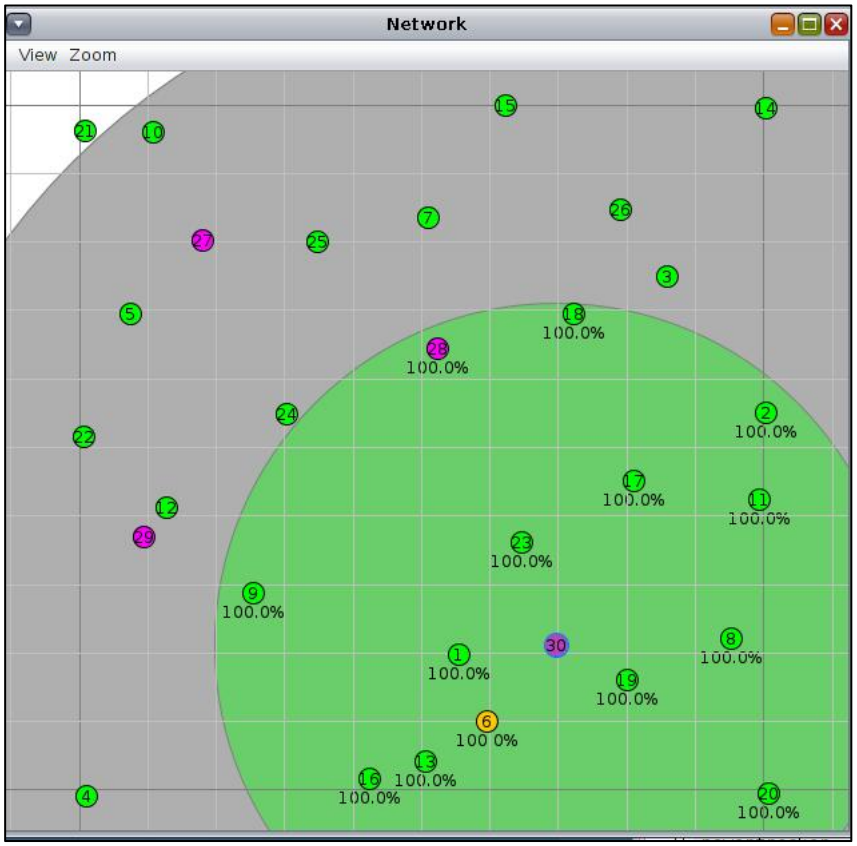

Figure IV.17 : Topologie de la simulation de Sinkhole en Scenario 3.

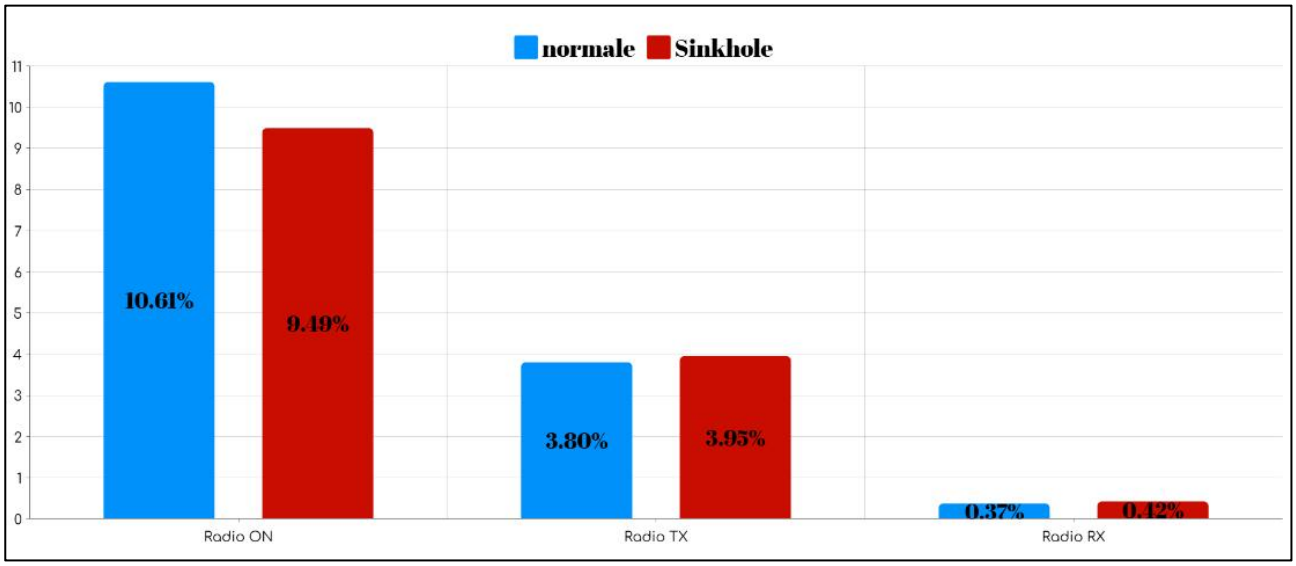

Figure IV.18: Diagrammes à barres comparant la consommation d'énergie Scenario 3.

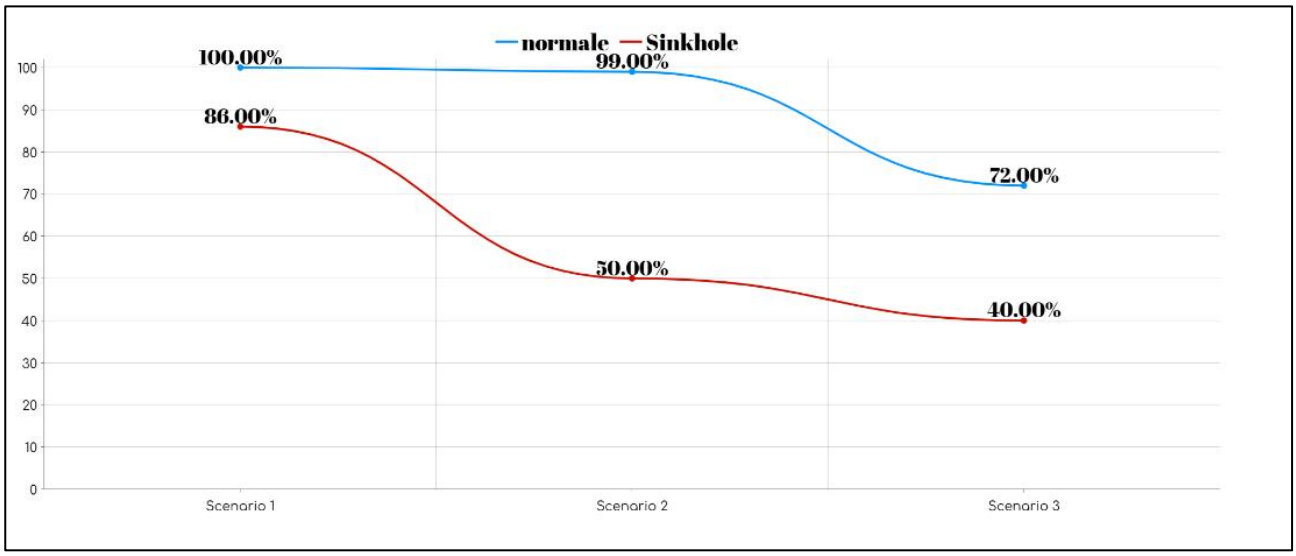

Figure IV.19:Courbe graphique comparant la valeur de PDR en les 3 Scenarios.

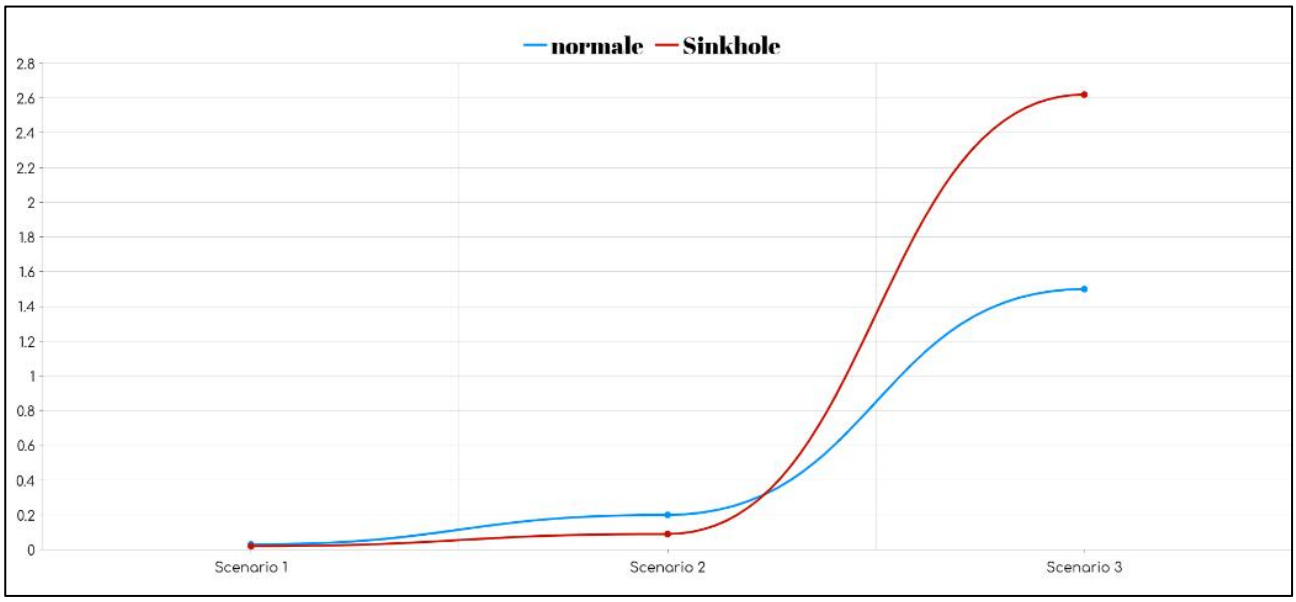

Figure IV.20: Courbe graphique de Délai de bout en bout en les 3 Scenarios.

IV.5 La discussion

cas normale :

Dans la figure IV.11, on peut observer que la valeur de PDR dans les trois scénarios a été la suivante :

- **Scenario1**
  D'après les conditions normales et la topologie mentionnée dans la figure IV.2, une valeur de PDR = 0,99 a été obtenue, ce qui signifie que le trafic des paquets dans le réseau a été effectué à 99%.
- **Scenario 2**
  D'après les conditions normales et la topologie mentionnée dans la figure IV.3, une valeur de PDR = 0.97 a été obtenue, ce qui signifie que le trafic des paquets dans le réseau a été effectué à 97%.
- **Scenario 3**
  D'après les conditions normales et la topologie mentionnée dans la figure IV.4, une valeur de PDR = 0.88 a été obtenue, ce qui signifie que le trafic des paquets dans le réseau a été de 88%.

Blackhole :

Dans la figure IV.11, on peut observer que la valeur de PDR dans les trois scénarios a été la suivante :

- Dans le scénario 1, on a atteint une valeur de PDR de 85%, ce qui entraîne une perte de 15% des messages envoyés par les nœuds du DODAG vers le puits.

- Dans le scénario 2, on a atteint une valeur de PDR de 82%, ce qui signifie qu'il y a une diminution de 18% des messages envoyés par les nœuds du DODAG vers le puits.

- Dans le scénario 3, on a atteint une valeur de PDR de 57%, ce qui entraîne une diminution de 43% des messages envoyés par les nœuds du DODAG vers le puits.

Sinkhole :

Dans la figure IV.19, on peut observer que la valeur de PDR dans les trois scénarios a été la suivante :

- Dans le scénario 1, on a atteint une valeur de PDR de 86%, ce qui entraîne une perte de 14% des messages envoyés par les nœuds du DODAG vers le puits.

- Dans le scénario 2, on a atteint une valeur de PDR de 50%, ce qui signifie qu'il y a une diminution de 50% des messages envoyés par les nœuds du DODAG vers le puits.

- Dans le scénario 3, on a atteint une valeur de PDR de 40%, ce qui entraîne une diminution de 60% des messages envoyés par les nœuds du DODAG vers le puits.

- Le PDR est donc fortement influencé par la taille et la complexité du réseau. En règle générale, le PDR des réseaux plus grands et plus complexes est inférieur à celui des réseaux plus petits et plus simples. Les nœuds malveillants affectent également la transmission des paquets sur le réseau et la perte partielle de paquets indique que les attaques par blackhole ont un impact sur une partie du réseau, tandis qu'une perte de paquets plus grande indique que les attaques par

sinkhole ont un impact presque total sur le réseau et causent plus de dommages.

Les valeurs de la consommation d'énergie dans les trois scénarios ont été représentées par les figures 6,8,10,14,16,18 :

- Une fois les attaques appliquées dans les trois scénario, on voir que les trois valeurs de Radio (On, Tx, Rx) diminer a comparant l'autre dans le cas normal

Dans les deux figures 12,20, on peut observer les valeurs de ED2ED dans les trois scénarios de la manière suivante :
Si les conditions normales sont respectées, tous les nœuds du réseau échangent des paquets, ce qui entraîne une congestion qui contribue à augmenter le ED2ED.

- Alors, Le délai E2E est fortement influencé par la taille et la complexité du réseau. Le délai E2E des réseaux plus grands et plus complexes, avec de nombreux sauts entre les nœuds, sera généralement plus long que celui des réseaux plus petits et plus simples.

- Une fois les attaques appliquées le délai bout à bout (E2E) dans les réseaux RPL peut être considérablement affecté par les attaques, ce qui entraîne une augmentation du temps de réponse et une détérioration de la qualité de service.

IV.6 Conclusion

Au cours de ce chapitre, nous avons simulé deux attaques et examiné trois indicateurs, à savoir le PDR, la consommation d'énergie et délai de bout en bout. De ces deux attaques, le Blackhole et le Sinkhole, nous avons conclu que sont de nature topologique en raison de leur impact sur le PDR, la consommation d'énergie et délai de bout en bout.

Conclusion générale

L'IdO est un réseau composé d'une variété d'appareils, tels que les capteurs, les appareils mobiles, etc.., qui peuvent être connectés à Internet. Les réseaux LLN, également connus sous le nom de réseaux à faible puissance et à perte, sont un autre type de réseaux sans fils et filaires où les objets sont généralement soumis à des contraintes de puissance de traitement, de cache et de batterie. En effet, RPL a été développé dans le but de servir de protocole de routage efficace et évolutif pour les LLN. Effectivement, le fait que ces types de réseaux manquent de ressources les rend particulièrement exposés aux menaces de sécurité, qu'elles soient externes ou internes, qui mettent en péril le réseau. C'est pourquoi il existe des mécanismes de sécurité tels que les IDS pour prévenir ces menaces. Néanmoins, malgré tous les dispositifs mis en œuvre pour prévenir ces menaces, il existe toujours des nœuds internes susceptibles d'être compromis et d'agir de manière spécifique sur le réseau pour le perturber.

Ainsi, dans ce mémoire, nous exposons quelques catégories d'attaques, parmi une quinzaine d'attaques décrites, qui affectent le réseau RPL, telles que le Blackhole et le SinkHole. Nous avons examiné l'effet de ces deux attaques sur trois indicateurs du réseau RPL, à savoir le PDR, délai de bout en bout et la consommation d'énergie. Nous avons remarqué que chaque attaque perturbait le routage en affectant les ressources, notamment PDR, et en changemant également la topologie. Afin de mettre en place ces dernières, nous avons utilisé le simulateur COOJA sous Contiki OS. Nous avons effectué des simulations pour chaque attaque, ainsi que d'autres sans les attaques, afin d'analyser et de déduire leur impact sur les ressources d'un réseau RPL.

Grâce à ce travail, nous avons pu explorer le domaine de l'internet des objets et développer une expertise approfondie non seulement sur les réseaux à faible puissance et à perte, mais aussi sur le protocole de routage des LLN. De plus, nous avons acquis des compétences en programmation dans l'environnement de Contiki et en simulation sur les réseaux LLN à l'aide du simulateur Cooja. Nous esperons de pouvoir travailler ultérieurement sur la recherche de méthodes plus avancées pour protéger les réseaux à faible puissance et avec des pertes contre les attaques externes et internes.

Références bibliographiques

[1] NhaKhanh Nguyen, Renaud Lifchitz, Julia Juvigny, Thomas Gayet, Damien Cauqui, et Christophe Baland, « la sécurité de l'Internet des Objet, livre blanc ».

[2] Cluster of European Research Projects on the Internet of Things, « Vision and Challenges for Realising the Internet of Things ». mars 2010.

[3] Taleb Omar et Mankouri Abdelkrim, « Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp », Mémoire de master, Université de Tlemcen, Algérie, 2016.

[4] Dave Evans, *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*, Cisco internet business solutions group (IBSG). Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[5] Bensadi S et Atoumi M Y, « Approche évolutionnaire pour la composition de services sensible à la QoS dans l'Internet des Objets à large échelle. », Université de Bejaia.

[6] « Comment se compose un système IoT ? », *Connectwave*, 2022, Consulté le: 21 avril 2024. [En ligne]. Disponible sur: https://www.connectwave.fr/techno-appli-iot/iot/reseaux-et-infrastructures-iot/

[7] Yick J, Mukherjee B, et Ghosal D, « Wireless sensor network survey - ScienceDirect », *Computer Networks*, p. 2292-2330.

[8] Haenggi M et Puccinelli D, « Wireless sensor networks: Applications and challenges of ubiquitous sensing », *IEEE Circuits and Systems Magazine*, p. 19-31.

[9] « DSpace at Kasdi Merbah University Ouargla: Etude comparative de protocoles de communication dans l'IOT ». Consulté le: 21 avril 2024. [En ligne]. Disponible sur: https://dspace.univ-ouargla.dz/jspui/handle/123456789/30911

[10] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of things: Energy oriented path and message scheduling approach," Sustain. Cities Soc., vol. 38, pp. 195-204, 2018,

[11] Qu'est-ce qu'une attaque par force brute ? | Définition, types & Fonctionnement (fortinet.com).

[12] Les 10 types de cyberattaques les plus courants (netwrix.fr).

[13] Attaques par déni de service (DoS) : Risques et précautions | Microsoft Experiences.

[14] MITM : En quoi consiste une attaque par l'homme du milieu ? (c-risk.com).

[15] Qu'est-ce qu'une attaque de logiciel malveillant ? - Définition (cyberark.com).

[16] Hanane Azzaoui, « The CIA Triad », Cours de 2 master, Université de Ouargla, Algérie, 2024.

[17] Muhammad Burhan et al. “IoT Elements, Layered Architectures and Security Issues : A Comprehensive Survey”. In : *Sensors* 18 (2018).

[18] Younes Abbassi et Habib Benlahmer. “Un aperçu sur la sécurité de l’internet des objets (IOT)”. In : Colloque sur les Objets et systèmes Connectés-COC’2021.

[19] Thubert, Pascal & Winter, Tim & Brandt, Anders & Hui, Jonathan & Kelsey, Richard & Levis, Phil & Pister, Kristofer & Struik, Rene & Vasseur, Jp & Alexander, Roger. (2012). RPL: IPv6 Routing Protocol for Low power and Lossy Networks. IETF. RFC 6550.

[20] Abdoulaye Ali et Mahamat-Saleh, « Estimation de la Qualité de Lien dans RPL », Mémoire de master, Université ABDELHAMID IBN BADIS, MONTAGANEM.

[21] H. Kharrufa, H. A. A. Al-Kashoash and A. H. Kemp, "RPL-Based Routing Protocols in IoT Applications: A Review," in IEEE Sensors Journal, vol. 19, no. 15, pp. 5952-5967, 1 Aug.1, 2019

[22] Ikram Boursas et Ihsane Djabrouhou, « Mitigation de l’attaque de numéro de version contre les réseaux IoT basés sur le protocole de routage RPL », mémoire de master, Université Saad Dahlab Blida 1, Algérie.

[23] Isabelle Chrismen, Rémi Badonnel, et Anthéa Mayzaud, « A Taxonomy of Attacks in RPL-based Internet of Things », *International journal of network security*, p. 459- 473, mai 2016.

[24] Aishwarya Parasuram, David Culler Ed, Randy Katz Ed, "An Analysis of the RPL Routing Standard for Low Power and Lossy Networks" University of California at Berkeley, May 14, 2016.

[25] RFC 6206: The Trickle Algorithm (rfc-editor.org)

[26] Sedrati Maamar, Azeddine Bilami, Guettala Leila, et Aouragh Lamia, (2007). « Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc ». Consulté le: 3 avril 2024.

[27] Olfa Gaddour et Anis Koubâa. “RPL in a nutshell : A survey”. In : Computer Networks 56.14 (2012), p. 3163-3178.

[28] Tanguy Ropitault «Protocole de routage RPL» , mai 2016.

[29] https://www.cloudflare.com/fr-fr/learning/ddos/syn-flood-ddos-attack/

[30] Bang, A.O., Rao, U.P. EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based internet of things. Peer-to-Peer Netw. Appl. 15, 642–665 (2022).

[31] Ghaleb Baraq,Al-Dubai Ahmed, Hussain A, Ahmad Jawad, Romdhani Imed, Jaroucheh Zakwan. « Resolving the Decreased Rank Attack in RPL's IoT Networks». 17 mai 2023.

[32] Mayzaud, Anthéa & Sehgal, Anuj & Badonnel, Rémi & Chrisment, I.. (2014). «Gestion de risques appliquée aux réseaux RPL».

[33] A. Dvir, T. Holczer, and L. Buttyan, “VeRA–version number and rank authentication in RPL,” in Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst., Oct. 2011, pp. 709–714.

[34] Karlof C., Wagner D. «Secure routing in wireless sensor networks: attacks and countermeasures Ad Hoc Networks» 2003.

[35] Linus Wallgren, Shahid Raza , and Thiemo Voigt. «Routing Attacks and Countermeasures in the RPL-Based Internet of Things».

[36] A Krari, A Hajami et E Jarmouni. “Study and Analysis of RPL Performance Routing Protocol Under Various Attacks”. In : International Journal on “Technical and Physical Problems of Engineering”(IJTPE) 13.49 (2021), p. 152-161.

[37] Rajasekar Ramalingam et Rajkumar Soundrapandiyan. “Analysis of Blackhole Attack in RPL-based 6LoWPAN Network : A Case Study”. In : nov. 2021, p. 1-6.

[38] BOUKERTOUTA Mohammed Amin, « Detection des intrusions basée sur l’apprentissage automatique dans les systèmes IdO (Internet des Objets) », Mémoire de master, Université de 8 Mai 1945 – Guelma -.

[39] Cong Pu. “Sybil Attack in RPL-Based Internet of Things : Analysis and Defenses”.In : IEEE Internet of Things Journal 7.6 (2020), p. 4937-4949.

[40] A. Dhingra and V. Sindhu, "A Study of RPL Attacks and Defense Mechanisms in the Internet of Things Network," 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), Kochi, India, 2022, pp. 1-6.

[41] S. Mangelkar, S. N. Dhage and A. V. Nimkar, "A comparative study on RPL attacks and security solutions," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017, pp. 1-6.

[42] A.Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," in IEEE Sensors Journal, vol. 20, no. 11, pp. 5666-5690, 1 June1, 2020.

[43] Windows VM | Workstation Pro | VMware.