République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Kadsi Merbah -Ouargla-
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et Technologie d'Information

Mémoire de MASTER professionnel

Domaine : Informatique et technologies de l'information
Branche : Informatique
Spécialité : Administration et Sécurité des Réseaux

Réalisé Par : Berdji Zouheyr

Thème

Proposer une solution d'atténuation des attaques du rang dans les réseaux RPL.

Soutenu devant le jury compose de :

- Dr. Boukhamla Akram — **Encadreur**
- Dr.Khlili.F — **Examinateur**
- Dr.Zgha.A — **Président de jury**

Année Université: 2021/2022

Remiercements :

Nous remercions ALLAH de nous avoir donné la santé et le courage afin de pouvoir réussir ce travail.Cetravail est l'aboutissement d'un long cheminement au cours duquel nous avons bénéficié de l'encadrement, de l'encouragement et du soutien de plusieurs personnes, à quinous tenons à dire profondément et sincèrement merci. J'exprime ma grande gratitude à mon Docteur

encadrant « Mr Boukhemla Akram», d'avoir accepté de suivre notre travail et pour ses précieux conseils et ses orientations.Nous avons eu le privilège de travailler parmi votre équipe , d'apprécier vos qualités , votre sérieux et votre compétence.Un grand merci aux membres de jury d'avoir accepté de juger notre travail,je remercie toutes les personnes qui m'ont apporté leur amitié, leur attention, leurs encouragements, leur appui et leur assistance pour que je puisse mener

à terme ce travail. Mesremerciements vont également à mes parents qui m'ont encouragé, qui m ont appris à travailler honnêtement et qui m'ont toujours supporté pendant toutes mes longues années d'études.

Dédicace

Je dédie ce travail, fruit de plusieurs années d'apprentissage, à tous ceux qui ont aimé de m'aider du proche ou du loin. Mon père qui m'a prêté attention et qui a fait de moi ce que je suis maintenant.

Ma très chère mère qui m'a offert depuis toujours le plus beau cadeau de l'univers, le cœur d'une mère et à qui je serais éternellement reconnaissant pour son soutien affectif.A mes frères à qui je souhaite beaucoup de joie et de bonheur dans leur vie.A tous les membres de ma famille, petits et grands, mes oncles, mes tantes, mes cousins et mes cousines. A tous mes amies et mes camarades ... Merci à tout le monde pour les moments qu'on a vécus ensemble. Enfin, tous simplement, je vous dis« J'aime Beaucoup » Zouheyr Berdji.

Résumé

Le monde, de jour en jour, demande fortement l'IOT dans certains domaines sensibles, mais l'IOT doit être améliorée en y combattant certains défis. Ces défis comportent le trafic des données dans les réseaux IOT. Le protocole du routage pour faible consommation et avec perte. RPL et classé comme protocole de routage proactif multi-saut qui fournit une connectivité IPv6 pour des dispositifs à faible puissance.RPL utilise une fonction objective qui sélectionne le meilleur trafic de données en respectant des contraintes présentes dans la topologie du réseau.

Ce choix du meilleur trafic va être exposé à des attaques(de ressources, de topologie)qui profitent des identificateurs,comme le rang. Pour cela, on vise à atteindre une solution sécuritaire légère, différente à la sécurité classique après la réalisation du point de vue des attaques du rang. On propose une solution pour contrôler les faux rangs des parents de chaque nœud appartenant a un intervalle suspect.

Pour évaluer cette solution, on a employé les métriques (PDR, ED2ED et la consommation d'énergie) qui ont abouti a des résultats satisfaisants.

Mot-clés : IOT, RPL, IPv6, La fonction objective, Le rang, PDR, ED2ED.

Abstract

The world, day by day, is strongly demanding IOT in some sensitive areas, but IOT needs to be improved by fighting some challenges in it. These challenges include data traffic in IOT networks. The low power and lossy routing protocol RPL is classified as a multi-hop proactive routing protocol that provides IPv6 connectivity for low power devices. RPL uses an objective function that selects the best data traffic within the constraints of the network topology.

This selection of the best traffic will be exposed to attacks (on resources, on topology) that take advantage of identifiers, such as rank. For that, we aim at reaching a light security solution, different to the classical security after the realization of the rank attacks. We propose a solution to control the false ranks of the parents of each node belonging to a suspect interval.

To evaluate this solution, we used the metrics (PDR, ED2ED and energy consumption) which led to satisfactory results.

Keywords: IOT, RPL, IPv6, Objective function, Rank, PDR, ED2ED.

الملخص

يطالب العالم ، يومًا بعد يوم ، بقوة إنترنت الأشياء في بعض المناطق الحساسة ، ولكن يحتاج إنترنت الأشياء إلى التحسين من خلال مواجهة بعض التحديات فيه. تشمل هذه التحديات حركة البيانات في شبكات إنترنت الأشياء. بروتوكول التوجيه منخفض الطاقة وفقدان البيانات RPL .والمصنف على أنه بروتوكول توجيه استباقي متعدد القفزات يوفر اتصال IPv6 للأجهزة منخفضة الطاقة. يستخدم RPL وظيفة موضوعية تحدد أفضل قيود تحترم حركة البيانات الموجودة في هيكل الشبكة.

سيتعرض هذا الاختيار لأفضل حركة مرور للهجمات (الموارد والطوبولوجيا) التي تستفيد من المعرفات ، مثل الرتبة. لهذا ، نهدف إلى تحقيق حل أمني خفيف ، يختلف عن الأمان التقليدي بعد الإدراك من وجهة نظر هجمات الرتب. نقترح حلاً للتحكم في الرتب الخاطئة لوالدي كل عقدة تنتمي إلى فترة مشبوهة.

لتقييم هذا الحل ، استخدمنا المقاييس PDR) ، ED2EDواستهلاك الطاقة (مما أدى إلى نتائج مرضية.

Table des matières

Liste des figures :

Liste des tableaux

Liste des abreviations:

IoT	Internet Of Things
RFID	Radio-frequency identification
CoAP	Constrained application protocol
RFC	Request For Comments
IETF	Internet engineering task force
http	Hypertext Transfer Protocol
MQTT	Message Queuing Telemetry Transport
TCP	Transmission contol protocol
IP	Internet Protocol
UDP	User datagram protocolc
LLN	Low-Power and Lossy Network
RPL	Routing Protocol for Low-power and lossy netwOrks
6LoWPAN	ipv6 Low power Wireless Personal Area Networks
IPv6	Internet Protocol Version 6
DODAG	Destination-Oriented Directed Acyclic Graph
DAG	Directed Acyclic Graph
ND	Neighbor Descovery
DIO	DODAG Information Object
ICMPv6	Internet Control Message Protocol for IPv6
DIS	DODAG Information Solicitation

MRHOF	Rang minimum avec fonction d'objectif d'hystérésis
ETX	Expected Transmission Count
DAO	Destination Advertisement Object
P2P	Point à point
ROLL	Routing Over Low-power and Lossy
Cooja	Java Contiki OS
E2E	End To End

Introduction générale

L’internet des objets(IoT) représente un domaine de la technologie dans lequel il est possible d'imaginer un réseau mondial qui rend les objets connectés. Internet des objets a tellement modifié notre vie à travers son impact sur l'enseignement, la communication, les entreprises, la science et les organismes publics.Cette invention est l'avenir du net car elle permet d'une part, de rendre tout objet physique intelligent, et d'autre part d'améliorer nos capacités à collecter, à analyser et à restituer les données. De nombreuses obstacles entravent l'évolution de l’IoT telles que la transition vers le protocole IPv6 et la mise en place de normes communes. Mais, malgré ces entraves les chercheurs veillent sur la bonneperformance et la progression de laIoT.Comme sa réussite dépend du bon fonctionnement du protocole de communication, la IoT doit être à l’abri de toutes menaces.

Le protocole RPL est vulnérable à un certain nombre d'attaques de sécurité. Ces attaques sont classées comme suit : attaques de nomination des sources du réseau, attaques de révision de la topologie du réseau et attaques liées au trafic du réseau.

La transmission sélective, la fabrication de la table de routage, l'attaque des voisins, l'attaque par trou de ver, l'attaque par puits, l'attaque par rejeu, etc. Ce sont des attaques de sous-optimisation, tandis que l'attaque par trou noir et l'attaque par incohérence DOA sont des attaques basées sur l'isolation dans la catégorie des attaques topologiques. Les attaques basées sur l'identité et la diminution du rang sont des attaques de détournement classées dans la catégorie des attaques basées sur le trafic.Les attaques par le numéro de version, l'attaque par le rang, etc. Ce sont classées dans la catégorie des attaques sur les ressources.

Dans l'attaque du rang, le nœud malveillant introduit le faux rangpar le biais de DIO sur le nœud voisin qui en résulte convergévers lui, et sélectionné comme parent préféré par DAO.

Les performances du réseau peuvent être affectées lorsque le nœud malveillant devient le nœud parent préféré (PPN) dans l'attaque. Le nœud malveillant devient le nœud parent préféré (PPN) dans la région attaquée. Afin de lancer une attaque de rang dans un réseau RPL,un nœud malveillant est introduit par l'attaquant, après que latopologie mise en place. Tous les nœuds, selon les règles définies par OF, obéissent aux règles de rang.

Les règles de rang définissant tous les nœuds fils RPL sélectionnent le PPN avec le rang le plus bas dans RPL.

Conformément aux règles RPL standard, plusieurs chemins sontétablis dans le réseau.

En réponse a notre problématique, on pourrait proposer les hypothèses suivantes :

- Il faut contrôler les activités des parents préférés pour chaque nœud.
- Il faut contrôler les rangs des membres de la liste des parents pour chaque nœud.
- Il faut contrôler les rangs de chaque nœud dans la topologie.

Nous avons choisi de configurer et de vérifier le protocole RPL en utilisant des outils performants.La sécurité des réseaux des protocoles du routage (RPL par exemple) dans les réseaux IOT se caractérise des autres réseaux par son empêchement d'appliquer la sécurité classique, qui protège contre les menaces.

On propose la solution suivante :

S’il y a diminution anormale de PDR, consommation abusive d'énergie et existence des nœuds ayant des faux rangs appartenant à un intervalle suspect plus grand du rang de route et moins que le rang du nœud légitime le plus proche du nœud puits,nous pourrons considérer ces nœuds comme des attaquants.

Chapitre I:
Généralités sur l'IoT.

I. 1 Introduction:

L'Internet des objets (IOT) est un nouvelle technologie qui occupe une grande importance dans les réseaux sans fil modernes des télécommunications.

L'idée de base de ce concept est la présence omniprésente autour de nous d'une variété de choses ou objets - tels que l'identification par radiofréquence (RFID) capteurs, actionneurs, téléphones portables… – qui, grâce à des schémas d'adressage uniques, sont capables d'interagir les uns avec les autres et coopérer avec leurs voisins pour atteindre des objectifs communs[1].

Incontestablement, la principale force de l'idée de l'IoT est l'impact important sur plusieurs aspects de la vie quotidienne et le comportement des utilisateurs potentiels. [2]

I. 2 Définition d'un objet connecté:

Un objet connecté est un appareil électronique sans fil communicant. Il récolte et stocke des informations, en émet, interagit avec d'autres appareils (smartphone, ordinateur, autre objet connecté, serveur, etc.). Il peut recevoir et transmettre des instructions.

Pour ce faire, il est équipé de capteurs (vidéo par exemple) connectés à Internet par des réseaux longues portées (Lora ou Sigfox), moyennes portées (wi-fi) ou courtes portées (Bluetooth, Zigbee). Toutes les informations qu'il va collecter sont transmises à une plateforme de traitement des données (data centers). Elles vont pouvoir être analysées et exploitées en temps réel et sans discontinuité. [3]

Figure 1:objets-connectés [6].

On distingue communément deux grands groupes d'objets connectés :

- Les objets destinés à la collecte et l'analyse de données, dont la mission

principale est de collecter et transmettre des informations.

- Les objets qui répondent à une logique de contrôle-commande et permettent de déclencher une action à distance. [4]

Ces derniers sont plus ou moins intelligents, selon qu'ils intègrent ou non eux-mêmes des algorithmes d'analyse de données et qu'ils s'auto-adaptent à leur environnement. [5]

I. 3 Les fonctions de l'objet connecté :

On distingue communément deux grands groupes d'objets connectés :

- les objets destinés à la collecte et l'analyse de données, dont la mission principale est de collecter et transmettre des informations.
- les objets qui répondent à une logique de contrôle-commande et permettent de déclencher une action à distance. [4]

Ces derniers sont plus ou moins intelligents, selon qu'ils intègrent ou non eux-mêmes des algorithmes d'analyse de données et qu'ils s'auto-adaptent à leur environnement. [5]

I. 4 Utilités de l'objet connecté:

Il permet de collecter et de traiter des données de capteurs, et de les communiquer à l'aide d'une fonction de connectivité et de recevoir des instructions pour exécuter une action. Ses

fonctions nécessitent une source d'énergie, pour que les données soient traitées directement en lui [7].

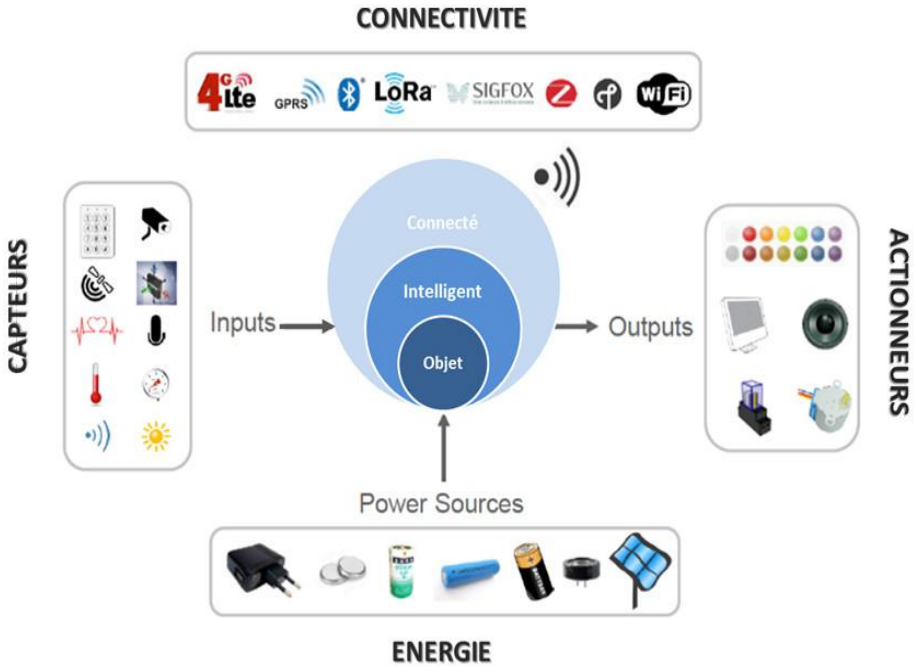

Figure 2:fonctions d'objet connecté[7].

I. 4. 1Les capteurs :

Pour transformer une grandeur physique, par exemple, température, luminosité, mouvement en une grandeur digitale utilisable par des logiciels, on doit utiliser des dispositif dits capteurs.

I. 4. 2Les sources d'énergie :

Elles peuvent être :

- Alimentation filaire (les objets ayant accès à une prise de courant).
- Piles ou batteries (les objets qui n'y ont pas accès).
- Capteurs d'énergie ou « energy harvesting » (photovoltaïque, piezoélectrique, Thermoélectrique, cinétique…) pour rallonger la durée de vie des objets à très faible consommation.
- Les objets passifs (sans piles qui sont alimentés par les ondes électromagnétiques des lecteurs : RFID, NFC…).

I. 4. 3Les actionneurs :

Ce sont en l'inverse du capteur : ils sont des dispositifs qui transforment une donnée digitale en phénomène physique afin de créer une action, Exemple d'actionneurs : Afficheurs, Alarmes, Caméras, Haut-parleurs, Interrupteurs, Lampes, Moteurs, Pompes, Serrures, Vannes, Ventilateur, Vérins, ….

I. 4. 4La connectivité

En vue de permettre la communication de l'objet vers un réseau il faut se rassurer de sa connectivité par une antenne Radio Fréquence. Les objets peuvent émettre des informations telles que leur identité, leur état, une alerte ou les données de capteurs, et d'autre part recevoir des informations telles que des commandes d'action et des données. Selon son module,la connectivité permet de gérer le « cycle de vie de l'objet », c'est-à-dire, l'authentification et l'enregistrement dans le réseau, la mise en service, la mise à jour et la suppression de l'objet du réseau.

I. 5 Les Composants du système Internet des objets :

Pour construire Un système IoT , il nécessaire de mettre en relation de divers composants technologiques : [7]

- Objets connectés
- Réseaux de communication sans fil .
- Plateformes de collecte.
- Hébergement.
- Traitement des données.
- Applications/services pour les utilisateurs finaux .
- Une supervision/sécurisation de toute la chaîne.

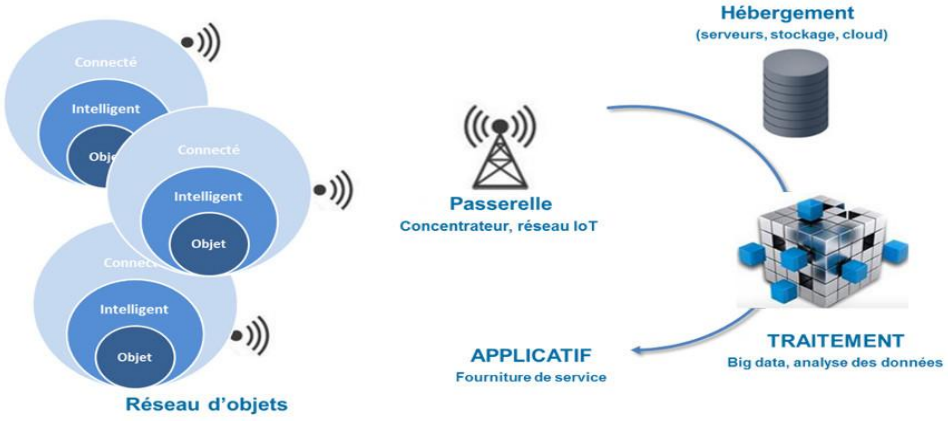

Figure 3:lescomposants du système IoT[7].

I. 6 Architecture de l'Internet des objets (IoT) :

Ses domaines d'application sont très variés, tels que l'automobile, les télécommunications, les technologies médicales ...etc. De ce fait les applications varient et se développent plus rapidement. L'IoT est dépourvu d'architecture du travail précise par la norme universelle ; il fonctionne selon ce qu' on a conçu / développé.

Pourtant, il existe un flux de processus de base sur lequel l'IoT est construit.

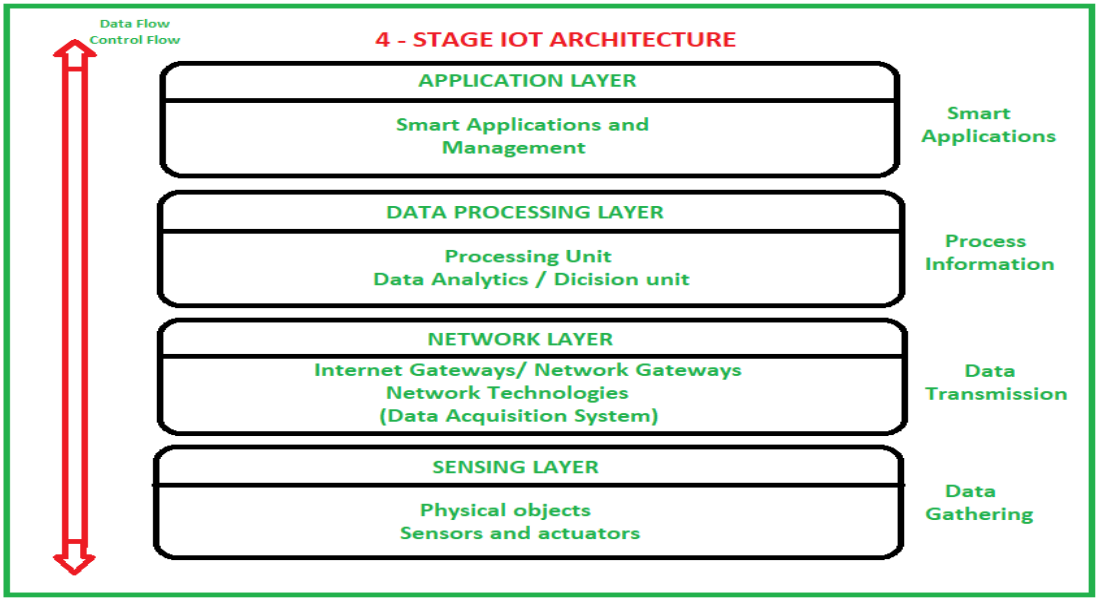

Figure 4: Architecture de l'Internet des objets[8].

La figure 4 montre que l' IoT se compose de 4 couches divisées comme suit:

couche de détection, couche réseau, couche de traitement de données et couche d'application.

Celles-ci sont expliquées comme suit ci-dessous.

I. 6. 1Couche de détection :

Elle traite les données et les émet sur le réseau en utilisant des capteurs, des actionneurs et des dispositifs. Ces derniers acceptent les données (paramètres physiques/environnementaux).

I. 6. 2Couche réseau :

Les passerelles Internet/réseau et le système d'acquisition de données (DAS) sont présents dans cette couche. Les passerelles avancées qui ouvrent principalement la connexion entre les réseaux de capteurs et Internet exécutent également de nombreuses fonctionnalités de passerelle de base telles que la protection contre les logiciels malveillants, et le filtrage également parfois la prise de décision basée sur les données saisies et les services de gestion des données, etc.

I. 6. 3Couche de traitement des données :

Il s'agit de l'unité de traitement de l'écosystème IoT. Ici, les données sont analysées et prétraitées avant de les envoyer au centre de données à partir duquel les données sont accessibles par des applications logicielles souvent appelées applications métier où les données sont surveillées et gérées et d'autres actions sont également préparées.

I. 6. 4Couche d'application :

Dans cette couche se trouvent les centres de données ou le cloud qui font la gestion et l'utilisation des données par les applications des utilisateurs finaux telles que l'agriculture, les soins de santé, l'aérospatiale, la défense, etc.[8]

I. 7 Les protocoles d'IoT :

Selon l architecture expliquée auparavanl, les appareils IoT communiquent à l'aide des protocoles IoT illustrés dans la figure : [9]

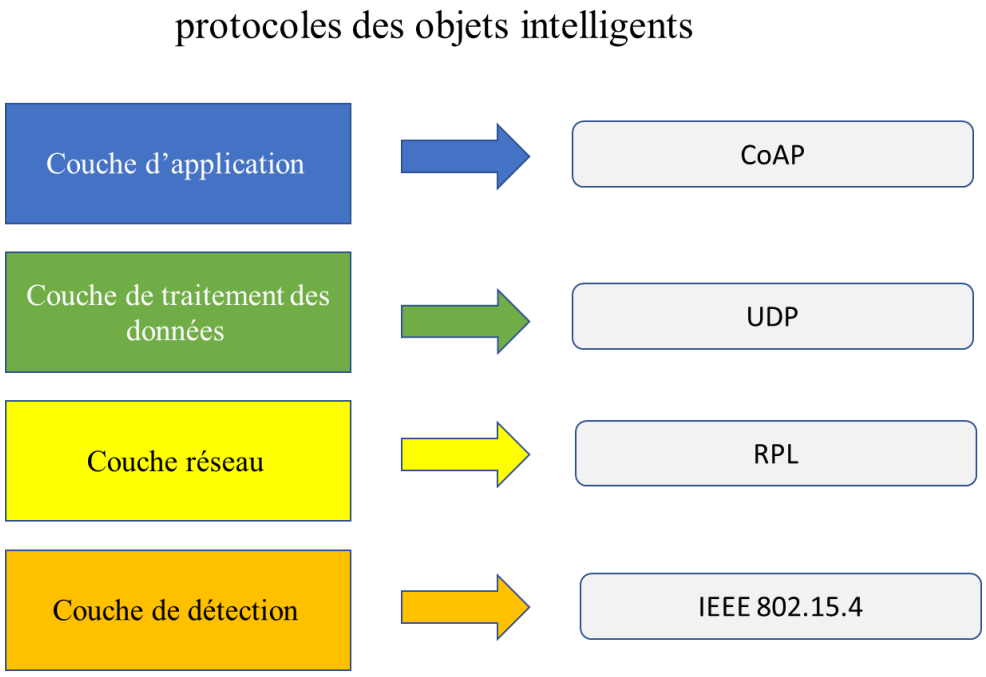

Figure 5: Protocoles des objets intelligents[41].

I. 7. 1Le protocole CoAP :

Est un protocole qui s'intéresse à la manière (le comment) des appareils à faible consommation d'énergie peuvent fonctionner dans l'Internet des objets (IoT). Conçu par l'Internet Engineering Task Force (ITEF), CoAP est spécifié dans IETF RFC 7252.

CoAP est conçu pour permettre aux appareils simples et contraints de rejoindre l'IoT même via des réseaux contraints avec une faible bande passante et une faible disponibilité. Le protocole est généralement utilisé pour la communication de machine à machine (M2M).

CoAP fonctionne comme une sorte de HTTP pour les appareils contraints, permettant à des équipements au niveau des composants tels que des capteurs ou des actionneurs de communiquer sur l'IoT, d'être contrôlés et de transmettre leurs données dans le cadre d'un système.

Le protocole est conçu pour la fiabilité dans une faible bande passante et une congestion élevée grâce à sa faible consommation d'énergie et à sa faible surcharge réseau. Selon Jullian Vermillard, ingénieur logiciel principal de Sierra Wireless, dans un réseau avec une connectivité limitée ou beaucoup de congestion CoAP peut continuer à fonctionner là où les protocoles basés sur TCP tels que MQTT ne parviennent pas à compléter une poignée de main.

Les caractéristiques efficaces et conservatrices du CoAP peuvent permettre à des appareils fonctionnant dans une qualité de signal médiocre d'envoyer leurs données de manière fiable ou permettre à un satellite en orbite de maintenir avec succès sa communication à distance. Malgré la capacité de CoAp à fonctionner sur de petits appareils, il prend en charge les réseaux avec des milliards de nœuds. Pour des raisons de sécurité, les paramètres DTLS choisis par défaut sont équivalents aux clés RSA 3072 bits. [10]

I. 7. 2Le protocole UDP :

Est un protocole de couche de transport. UDP fait partie de la suite de protocoles Internet, appelée suite UDP/IP. Contrairement à TCP, il s'agit d'un protocole peu fiable et sans connexion. Il n'est donc pas nécessaire d'établir une connexion avant le transfert de données.

Bien que le protocole TCP (Transmission Control Protocol) soit le protocole de couche de transport dominant utilisé avec la plupart des services Internet ; fournit une livraison assurée, une fiabilité et bien plus encore, mais tous ces services nous coûtent des frais généraux et une latence supplémentaire. Ici, UDP entre en scène. Pour les services en temps réel tels que les jeux informatiques, la communication vocale ou vidéo, les conférences en direct ; nous avons besoin d'UDP. Étant donné que des performances élevées sont nécessaires, UDP permet de supprimer les paquets au lieu de traiter les paquets retardés. Il n'y a pas de vérification des erreurs dans UDP, ce qui permet également d'économiser de la bande passante.

Le protocole UDP (User Datagram Protocol) est plus efficace en termes de latence et de bande passante.

L'en-tête UDP est un en-tête fixe et simple de 8 octets, tandis que pour TCP, il peut varier de 20 octets à 60 octets. Les 8 premiers octets contiennent toutes les informations d'en-tête nécessaires et la partie restante est constituée de données. Les champs de numéro de port UDP ont chacun une longueur de 16 bits, par conséquent, la plage pour les numéros de port est définie de 0 à 65535 ; le numéro de port 0 est réservé. Les numéros de port aident à distinguer les différentes demandes ou processus des utilisateurs.[11]

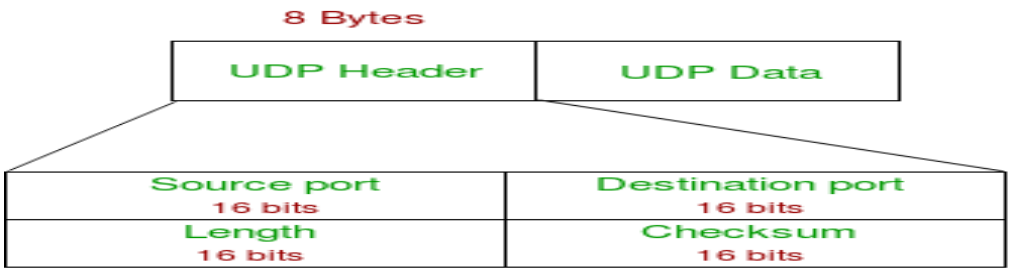

Figure 6: L'en-tête UDP[11].

I. 7. 2. 1UDP dans l'IoT :

Dans l'IoT (et la transmission de données en général), le protocole de datagramme utilisateur est moins courant que TCP. Mais UDP séduit souvent les fabricants d'IoT car il utilise moins de ressources réseau pour transmettre et n'a pas besoin de maintenir une connexion constante entre les deux points de terminaison. En d'autres termes, il utilise moins de données et consomme moins d'énergie.

Périphériques à ressources limitées :

Les appareils IoT fonctionnent souvent dans des réseaux avec perte (LLN) à faible consommation d'énergie. Les LLN sont optimisés pour l'efficacité énergétique, ils ont donc très peu de ressources. Le protocole CoAP (Constrained Application Protocol) a été spécialement développé pour aider ces périphériques à communiquer, et il s'exécute sur les périphériques qui utilisent UDP.

Transmissions de liaison descendante faibles :

UDP n'envoie aucun accusé de réception d'une transmission. L'expéditeur ne sait pas si les paquets de données sont arrivés, mais l'échange nécessite moins de budget de liaison descendante. Pour les transmissions avec de faibles allocations de liaison descendante, UDP peut être un protocole de communication précieux.

Applications basse consommation :

Dans l'IoT, ce n'est souvent pas un problème de perdre un seul point de données car l'appareil l'envoie périodiquement. Essayer de renvoyer les données épuise plus la batterie ; chaque fois qu'un point de données est perdu ou il y a eu une erreur. Et comme UDP n'envoie pas d'accusé de réception, l'appareil peut s'éteindre plus rapidement après l'envoi ou la réception d'une transmission. Cela rend UDP attrayant pour les développeurs qui souhaitent maximiser l'efficacité énergétique.[12]

I. 7. 3Le Protocole RPL :

Les réseaux à faible puissance et avec perte (LLN) sont une classe de réseau dans laquelle les routeurs et leur interconnexion sont limités : les routeurs LLN fonctionnent généralement avec des contraintes sur (tout sous-ensemble) la puissance de traitement, la mémoire et l'énergie (batterie), et leurs interconnexions sont caractérisées par (tout sous-ensemble) taux de perte élevés, faibles débits de données et instabilité. [13]

Le protocole RPL est un protocole de routage à vecteur de distance utilisant IPv6,spécialement conçu par l'IETF pour répondre aux besoins des réseaux LLN, ce protocole et ses règles sont détailles dans le deuxième chapitre.[14]

I. 7. 4Le ProtocoleIEEE 802.15.4 :

IEEE 802.15.4™ est une norme mondiale pour les développeurs d'applications de ville intelligente et d'Internet des objets (IoT). Dans le passé, les développeurs, les fournisseurs de services et les utilisateurs finaux étaient confrontés au dilemme de l'interopérabilité pour la mise en œuvre de la couche de communication. Pour résoudre ce problème et tirer parti de la norme IEEE 802.15.4, ils disposent désormais d'une option acceptée à l'échelle mondiale.

IEEE 802.15.4 a été développé pour permettre des applications à faible débit de données qui nécessitent des années d'autonomie de la batterie, des architectures de faible complexité pour minimiser les coûts et la capacité de fonctionner dans un spectre sans licence. Les exemples incluent les réseaux de services publics intelligents, la gestion de l'éclairage public, l'automatisation des bâtiments, le contrôle de la maison et la sécurité résidentielle.

I. 8 Les avantages de l'IoT :

Il y a de nombreux avantages d'incorporer l'IoT dans notre vie quotidienne, elle peut aider les individus, les institutions, les entreprises et la société au quotidien. Les entreprises peuvent également tirer de nombreux avantages de

L'IoT, notamment le suivi des biens et le contrôle des stocks, la sécurité et la

capacité de suivre les consommateurs individuels (ex : électricité, gaz, eau) et

de cibler ces consommateurs sur la base des informations fournies par les

dispositifs intelligents déployés (ex : compteurs intelligents).

Les avantages de l'IoT s'étendent à tous les domaines de la vie. En voici certains :

Amélioration de la collecte des données :la collecte des données modernes souffre de ses limites et de sa conception pour une utilisation passive. Avec l'IoT, c'est tout l'environnement qui nous entoure peut être intégrer au monde numérique. Grâce à l'utilisation des capteurs et des actionneurs

elle peut interagir avec l'environnement et le monde physique (collecte de données/informations, et agir sur l'environnement, etc.).

l'IoT nous permet d'avoir une image précise et à granularité fine sur le monde réel.

Etendre la connectivité d'Internet et ses applications à notre environnement physique et aux objets du quotidien (électroménager, voitures, domotique, industrie, etc.). Ceci permet d'améliorer sensiblement les services fournis au quotidien ainsi que l'apparition de nouveaux services innovants. [15]

I. 9 Inconvénients de l'IoT :

- Sécurité : l'IoT crée un écosystème de périphériques constamment connectés qui communiquent sur des réseaux. Le système offre peu de contrôle malgré toutes les mesures de sécurité. Cela laisse les utilisateurs exposés à divers types d'attaquants et risques sécuritaire.

- Complexité : Certains trouvent les systèmes l'IoT complexes en termes de conception, de déploiement et de maintenance, étant donné qu'ils utilisent de multiples technologies et un grand nombre de nouvelles technologies hétérogènes.
- La flexibilité : Beaucoup s'inquiètent de la flexibilité d'un système l'IoT pour s'intégrer facilement à un autre. Ils s'inquiètent de se retrouver avec plusieurs systèmes conflictuels ou verrouillés. [15]

I. 10 Conclusion

L'Internet des objets est une nouvelle révolution de l'internet qui peut représenter le prochain grand bond en avant dans le secteur des technologies de l'information et de la communication (TIC).

La possibilité de fusionner le monde réel et le monde virtuel, grâce au déploiement massif d'appareils embarqués, ouvre de nouvelles voies intéressantes pour la recherche et les affaires.[15]

Chapitre II:

Le Protocole du routage RPL.

II. 1 Introduction

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance [16],Routing Protocol for Low power and Lossy network (RPL) est un protocole développé spécifiquement pourle réseau 6LoWPANafin de concrétiser le concept d'Internet des objets (IoT).

RPL offre de nombreux avantages tels que l'efficacité énergétique, un routage optimal et un sur coût minimal, ce qui le rend plus performant que les autres protocoles de routage précédents [17].

II. 2 Définition du Protocole RPL :

Le protocole de routage proactif nommé RPL est le protocole standard proposé pour les LLN par l'IETF et a été récemment mis à jour dans Mars 2012 comme [13].

RPL fournit une connectivité Internet IPv6 et en outre, en utilisant RPL, le coût pour atteindre la racine (base station) à partir de n'importe quel nœud du LLN est également réduite [13].

II. 3 La topologie RPL :

RPL construit une topologie du routage appelée graphe acyclique orientée vers la destination (DODAG) enracinée au niveau de la passerelle. [18]

RPL organise la topologie du réseau dans une approche orientée destinationGraph (DAG), composée d'un ou de plusieurs graphes acycliques orientés vers la destination (DODAG).

Chaque DODAG représente un arbre de routage créé par un nœud racine, également appelé nœud puits. [19]

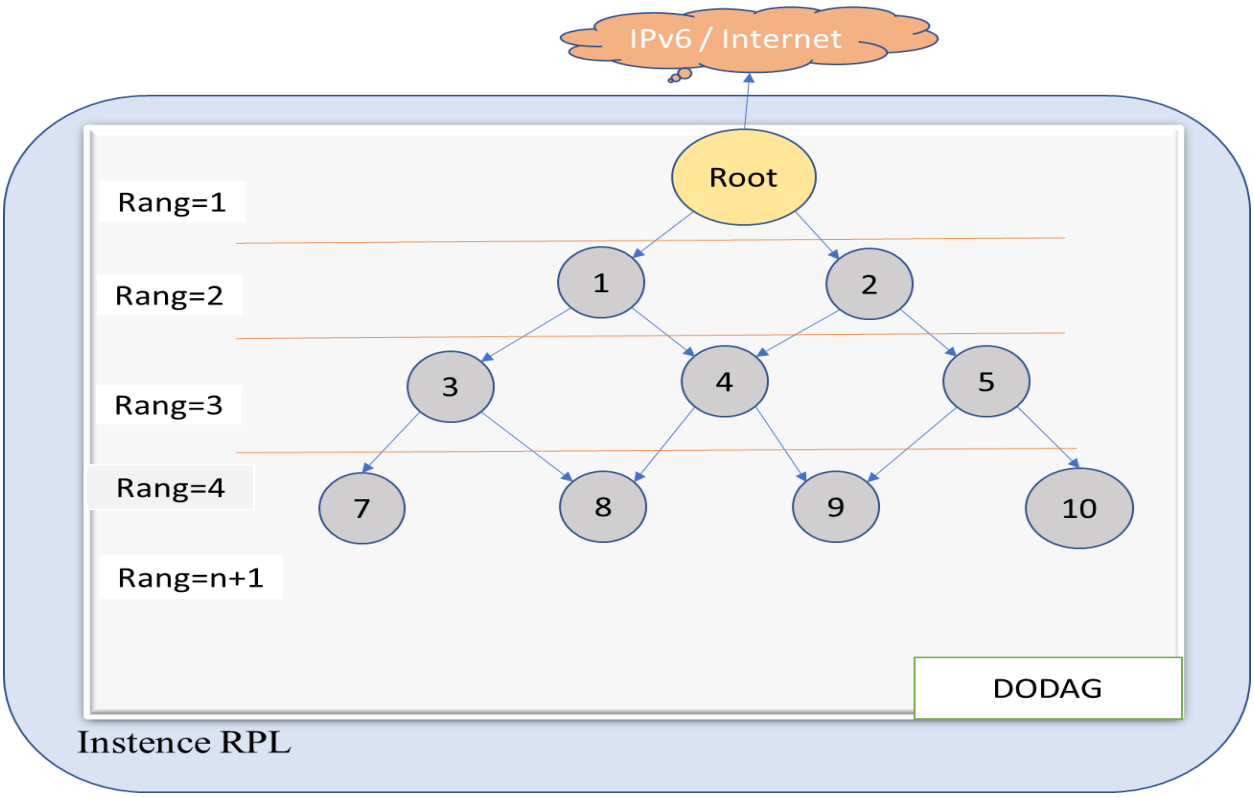

Figure 7: Partition de topologie RPL.

II. 3. 1 Identifiant RPL :

II. 3. 1. 1 DODAGID :

C'est l'identificateur de la racine DODAG. DODAGID possède des propriétés uniques dans une gamme d'instances RPL au sein de LLN. Le tuple (RPLInstanceID, DODAGID et DODAG VersionNumber) identifie et définit de manière unique les informations de version DODAG. [13]

II. 3. 1. 2 Version DODAG :

C'est une itération spécifique ("version") d'un DODAG avec un DODAGID donné.

II. 3. 1. 3 DODAG VersionNumber

C'est un compteur qui est compté séquentiellement.Il incrémente à partir de la racine, capable de former une toute nouvelle version du DODAG. La version DODAG est identifiée de manière unique par RPLInstanceID, DODAGID, DODAG VersionNumber.[13]

II. 3. 1. 4 Le rang (rank)

C'est l'attribut du nœud dans le système DODAG, indiquant l'emplacement du nœud par rapport à la racine de ce système. Le rang ne peut être utilisé que dans une version du DODAG et non dans différentes versions. Dans le sens de s'éloigner de la racine DODAG, le rang augmente progressivement vers les noeuds feuilles et diminue progressivement vers la racine pour éviter les boucles de routage. Cette valeur calculée par la fonction d'objectif OF et doit toujours être supérieure au rang de ses parents afin de garantir l'aspect cyclique dugraphe.[13]

II. 3. 2 La construction DODAG

Le processus de découverte des voisins (Neighbor Descovery (ND)) détermine la construction du DODAG. Ce processus s'opère comme suit :

1. L'orientation descendante, dans laquelle le processus commence du nœud racine par la diffusion d'un message de contrôle DIO à ses voisins, ayant pour but d'annoncer ses informations (DODAGID, le rang et l'OF).

Dans le cas présent, il y a deux possibilités :

- Message DIO reçu ultérieurement :

Le nœud se rejoint au DODAG, il exploite les informations fournies dans le message DIO en ajoutant l'adresse de l' émetteur du message DIO à sa liste de parents candidats.

Puis, la fonction OF calcule le rang du nœud. et enfin il transmet le message DIO mis à jour. Après avoir calculé son propre rang en fonction de l'OF, il sélectionne l'un des parents depuis la liste des parents comme parent préféré.

Ensuite, le nœud transmet le message DIO avec les informations mises à jour à ses voisins et répète le même processus jusqu'à ce que tous les nœuds possèdent une route ascendante pour transmettre le trafic vers la racine.

- Message DIO n'est pas reçu ultérieurement :

le nœud a le choix de rejeter le message DIO ou de l' analyser en conservant son rang dans le DODAG ou d'optimiser son rang par un niveau inférieur.

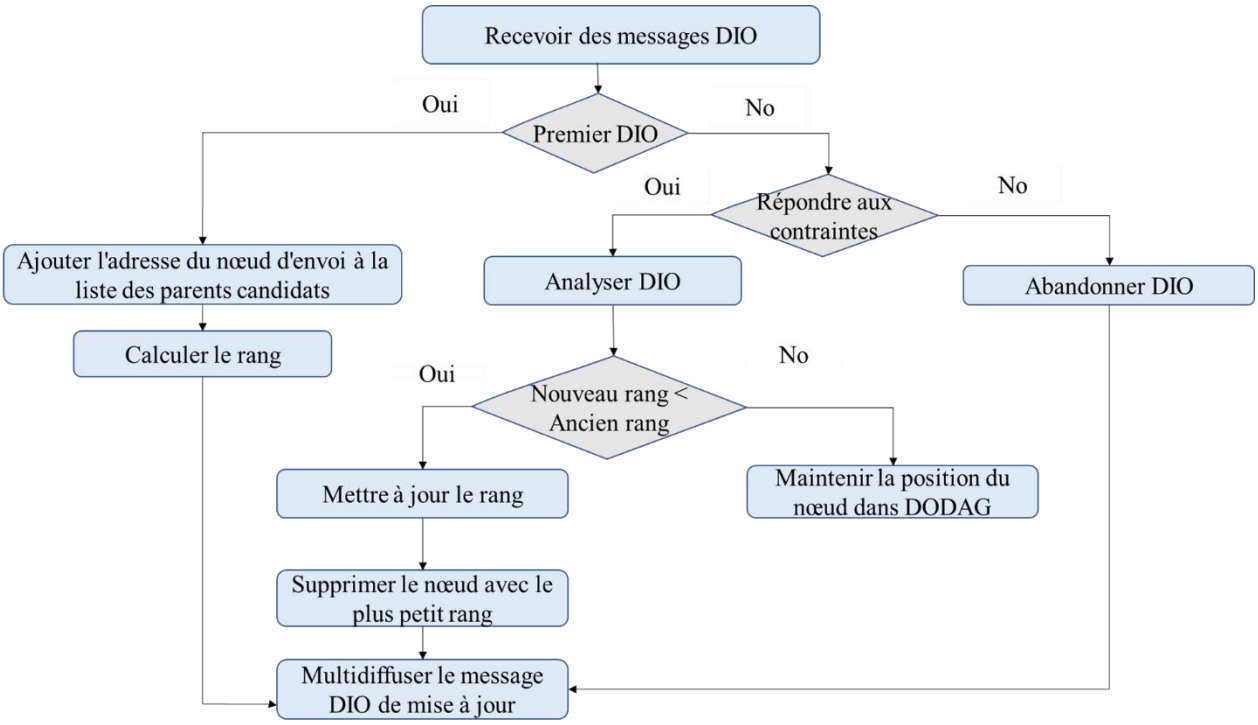

Figure 8: Processus de calcul le rang.

2. La deuxième étape dans la construction de la direction ascendante consiste à propager les messages DAO des nœuds feuilles vers la racine du DODAG.

D'une autre manière, RPL spécifie un mécanisme pour les applications nécessitant un trafic descendant depuis la passerelle (racine) vers un nœud, dans lequel un nœud envoie un message de contrôle de type DAO en unicast dans le but de créer une Information du chemin inverse.

En plus, un autre type de message de contrôle ICMPv6 appelé DIS qui est fourni par le nœud qui ne reçoit pas de message DIO en sollicitant les voisins d'un message DIO.

Chaque nœud rejoignant le DODAG possède une route vers la racine.

Les nœuds qui rejoignent le DODAG agissent l'une des deux manières suivantes : si le nœud agit comme un routeur, il diffuse les informations du graphe à ses voisins, sinon le nœud agit comme un nœud feuille et n'envoie pas les messages DIO.

Tous les nœuds voisins répètent tout ce processus et construisent les bords du DODAG (feuilles).

La construction du DODAG est basée sur la fonction d'objectif OF qui déploie un ensemble de métriques de routage pour construire le DODAG sur la base d'algorithmes ou d'une formule de calcul.[20]

II. 3. 3La Fonction Objectif :

Pour obtenir un large éventail de domaines d'application LLN, RPL sépare le traitement et le transfert des paquets de l'objectif d'optimisation du routage. Des exemples de tels objectifs incluent la minimisation de l'énergie, la minimisation de la latence ou la satisfaction des contraintes .l'OF est identifiée par un point de code objectif (OCP) dans le message de contrôleDIO. Elle définit aussi les routes optimales pour les nœuds RPL au sein d'une instance RPL.

L'OF utilise un ensemble des métriques de routage[qui viennent après] pour les besoins suivants :

1. La sélection de DODAG pour rejoindre ;
2. Le rang de chaque nœud au sein du DODAG ;
3. le nombre de pairs dans ce DODAG en tant que parents et le calcul d'une liste ordonnée de parentS ;
4. Le résultat du processus utilisé par un nœud RPL pour sélectionner et optimiser les itinéraires dans une instance RPL basée sur les objets d'information disponibles.

A la date de rédaction de ce document, le ROLL WG a défini deux fonctionsà la fonction objective:

• la fonction objective zéro (OF0) [23] : ou la métrique de routage retenue représente le nombre de sauts. OF0 est conçu pour être l'OF commun qui permettra l'interopérabilité entre les différentes implémentations de RPL[21].

• MRHOF : Rang minimum avec fonction d'objectif d'hystérésis [22]MRHOF sélectionne des itinéraires qui minimisent une métrique, tout en utilisant l'hystérésis pour réduire le taux de désabonnement en réponse à de petits changements de métrique. MRHOF fonctionne avec des métriques qui se combinent le long d'un itinéraire.

Il s'agit de la métrique traditionnelle ETX (Expected Transmission Count).

L'ETX d'une liaison sans fil est le nombre moyen estimé de transmissions de trames de données et de trames ACK nécessaires à la réussite de la transmission d'un paquet [24].La séparation des OF de la spécification du cœur du protocole vise à permettre l'adaptation de RPL pour répondre aux différents critères d'optimisation requis par le large éventail de déploiements, des applications et des conceptions de réseaux [23].

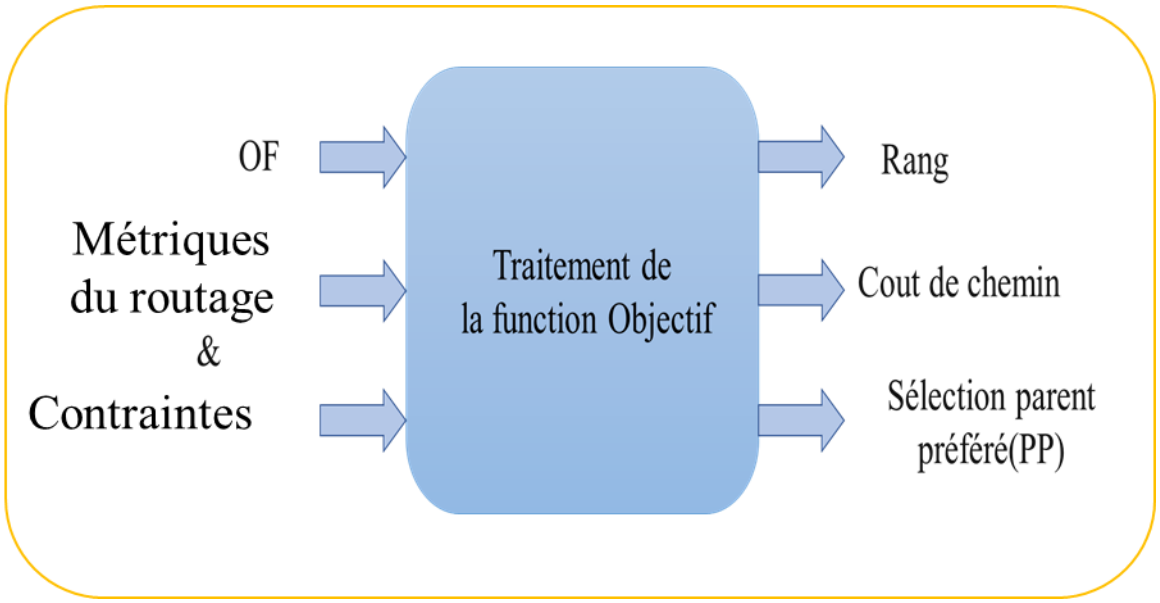

Figure 9: Un schéma illustrer le principe de l'utilisation de la fonction objectif.

II. 4 les messages de contrôle :

La spécification RPL définit les quatre types de contrôle messages sous forme de messages d'information ICMPv6[25].

Pour découvrir les chemins de transfert de données,utiliser les messages de contrôle :

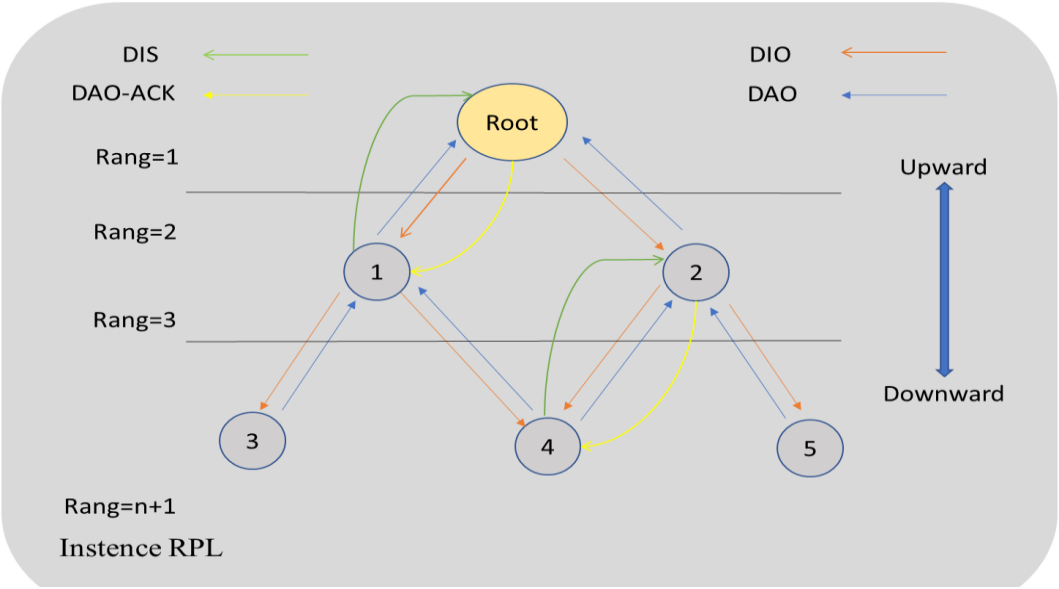

Figure 10: Un schéma illustrer les messages de contrôle de la topologie RPL.

II. 4. 1Destination Advertisement Object (DAO) :

les messages DAO sont utilisés par les nœudsRPL pour propager les informations de routage afin de permettre tracer P2MP. Le deuxième est appelé un objet de publicité de destination (DAO). Il permet le support de down trac et est utilisé pour propager informations de destination vers le haut le long du DODAG. [25]

1 byte	1	1	6 bits	1 byte	1 byte
RPL Instance ID	K	D	Flags	Reserved	DAO Sequence
DODAGID (128 bits)					
Sub-option(s)					

Figure 11: Structure du message de contrôle DAO[18].

II. 4. 2DAO-ACK :

Un DAO-ACK est envoyé par un destinataire DAO en réponse à un message DAO.

II. 4. 3Objet d'information DODAG (DIO) :

Un DIO permetà un nœud de découvrir l'instance RPL et enstocker ID instance dans le premier champ de données.

Le deuxième et le troisième champ incluent la version DODAG et le rang de l'expéditeur du message. [25]

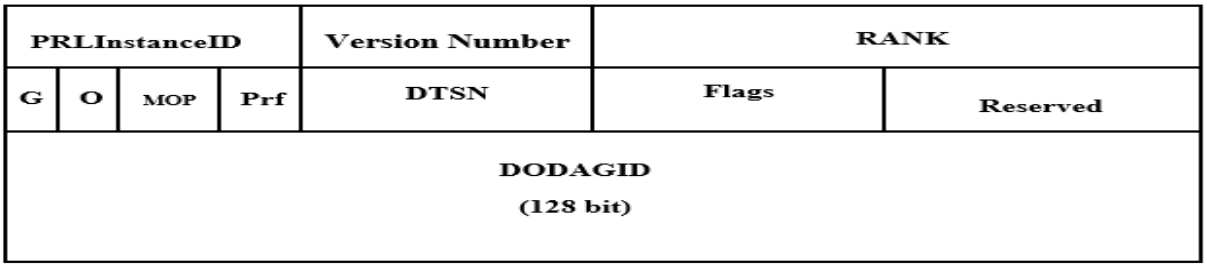

Figure 12: Structure du message de contrôle DIO[18].

II. 4. 4DODAG Information Sollicitation (DIS) :

Permet à un nœud d'exiger des messages DIO d'un voisin joignable. [25]

II. 5 Les fonctionnements RPL :

Pour la prise en charge des communications RPL supporte deux modes de fonctionnement :

II. 5. 1Le mode sans stockage (non-storing Mode) :

Entièrement avec état MOP 1 le nœud envoie des données jusqu'à la racine du DODAG en transmettant récursivement les messages aux parents DIO.À la racine du DODAG, le paquet est acheminé à la source vers la destination requise.[26]

II. 5. 2Le mode avec stockage (Storing mode) :

Entièrement avec état MOP 0, le paquet est transmis aux parents DIO jusqu'à ce qu'il atteigne un ancêtre qui peut diriger le paquet vers la destination requise.

Ces deux modes de fonctionnement sont incompatibles. Ils nécessitent l'utilisation de messages DAO et l'utilisation facultative de messages DAO-ACK.[26]

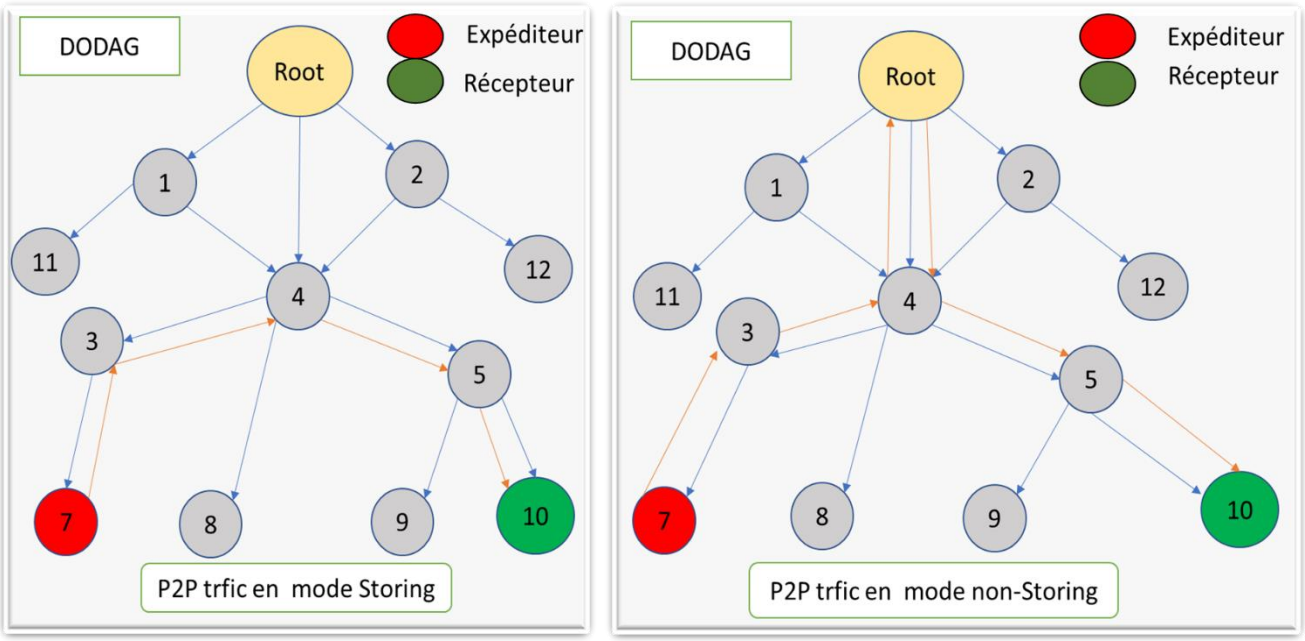

Figure 13: Mode non-storing et Mode storing.

II. 6 Les paradigmes de communication :

II. 6. 1Du multipoint au point (MP2P) :

La fonction essentielle de RPL est l'optimisation du type de flux de trafic MP2P, les nœuds clients, dans certains cas, envoient un DAO vers la racine DODAG via des routes ascendantes grâce à la communication MP2P. mais à condition d'être connecté à un réseau.

II. 6. 2Point 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 (préfixes, adresses ou groupes de multidiffusion) . Par exemple les messages DIO, P2PM est le modèle de trafic requis par plusieurs applications LLN.

Les messages DIO, P2PM sont le modèle de trafic requis par plusieurs applications LLN qui supportent le trafic P2MP. [27][13]Ce dernier offre un service de publicité qui prévoit des itinéraires descendants de la racine vers des destinations (une seule adresse ou multidiffusion) [27].

II. 6. 3Point à point (P2P) :

le trafic P2P se base sur le mode de fonctionnement du protocole RPL.

Pour le mode Storing mode, le paquet sera envoyé à la destination en passant par un ancêtre. Dans d'autres cas, il peut s'agir d'un nœud plus proche de la source ou de la destination.

Pour le mode Non-Storing mode le paquet se dirige vers une racine(Root), ensuite la racine effectuera le routage vers la destination. [13] [28]

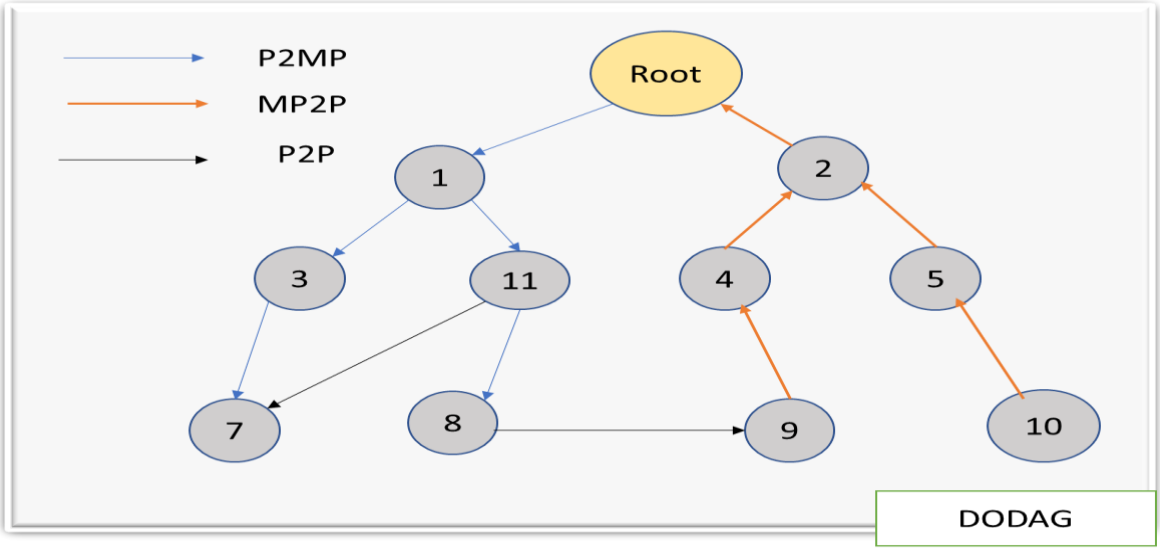

Figure 14: Les paradigmes de communication en RPL.

II. 7 Maintenance de la topologie :

En cas de rupture d'un lien, le DODAG peut être réparé de deux façons :

II. 7. 1Réparation globale :

Elles est couteuse en trafic ; la reconstruction complète du DODAG est initiée par la racine au moyen des messages DIO. Pour différencier les DODAG anciens et nouveaux, on utilise les numéros de séquence. [29]

II. 7. 2Réparation locale :

Le nœud atteint se fouille pour trouver une nouvelle origine dans ses voisins. Avoir une nouvelle optimisation, se réalise par réparation globale seulement. [29]

II. 8 La sécurité du réseau RPL :

Les applications IoT sont sécurisées par RPL. elles devraient avoir l'intégrité, la confidentialité, la disponibilité, la confidentialité, l'authentification et la confiance.

La simplicité matérielle IOT n'assure pas la sécurité suffisante aux nœuds :

- Blocage leur services du nœuds ;
- Exploitation de leurs données.

Au niveau du routage, le principal problème de la sécurité se trouve lors de l'évaluation des performances du réseau [30]. En fonction de la norme RPL identifiée dans [13], trois modes de sécurité apparaissent :

- Non sécurisé : Sans considération de la sécurité, Les messages de contrôle sont envoyés.
- Préinstallé : Dans le but de rejoindre un réseau, une clé préinstallée est utilisée par les nœuds.
- Authentifié : Pour que les nœuds feuille fonctionnent comme un routeur, Ils demandent un message d'authentification. Tout en passant préalablement par le mode préinstallé.

II. 9 Classification des attaques RPL :

Le ROLL permet une compréhension complète des caractéristiques de sécuritédu RLP. Les attaques de sécurité sont classées en fonction du modèle de sécurité, qui comprend les principes fondamentaux de sécurité (C.I.A.A). Cependant, les mécanismes conventionnels disponibles pour la sécurité câblée tels que le pare-feu ne sont pas applicablespour la sécurité des RPL en raison de leur comportement dynamique et, par conséquent, leurs nœudsn'ont pas de frontières bien définies.

De plus, lesmécanismes de cryptographie ne peuvent pas être utilisés pour défendre la sécuritédu routage RPL en raison de l'absence d'administration centralisée et de coopération entre les nœuds.

De surplus, comme les dispositifs des nœudsne sont pas inviolables, il devient plus facile d'exposer les nœuds et de violer leur cryptographie. Par conséquent, les nœuds compromis peuvent dégrader les performances du réseau RPL en raison de la manipulation du code source de l'application[31]. De plus,La figure 14 présente une taxonomie des attaques contre les réseaux RPL [32].

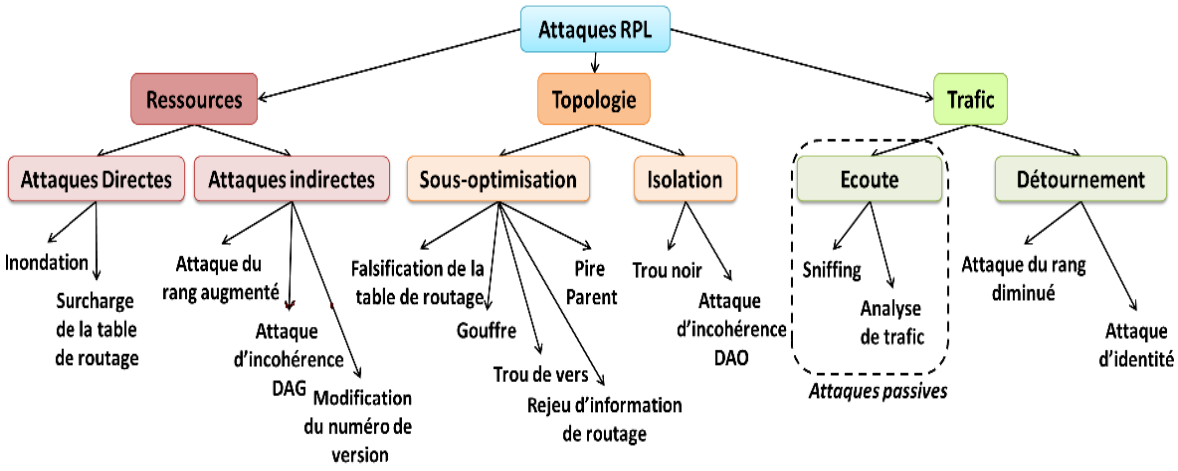

Figure 15: Une taxonomie des attaques réseau RPL[32].

Les attaques de sécurité contre les protocoles de routage RPL sont classées en trois catégories :[32,33]

II. 9. 1Les attaques contre les ressources :

font généralement des nœuds des tâches dispensables pour drainer leurs ressources. Ces attaques consomment les ressources des nœuds telles que le stockage, l'énergie et le traitement.

Par conséquent, la disponibilité du réseau est affectée en rendant les liens disponibles encombrés et affecte alors la durée de vie du réseau,qui peut être réduite de manière significative. Ce type d'attaque est classé en deux sous-catégories :

II. 9. 1. 1 Les attaques directes :

Le nœud malveillant peut dégrader le réseau en générant directement une surcharge.

II. 9. 1. 2 Les attaques indirectes :

Dans lesquelles d'autres nœuds malveillants qui génèrent un grand nombre de surcharge de traficpeuvent créer une boucle.

II. 9. 2Attaques sur la topologie :

Qui porte atteinte à la topologie du réseau etest classée en deux sous-catégories qui sont :

II. 9. 2. 1Les attaques de sous-optimisation :

Dans lesquelles les attaquants dégradent laperformance du réseau en diminuant ses chemins optimaux.

II. 9. 2. 2Les attaques par isolement :

Dans lesquelles les attaquants isolent les nœudsdu réseau RPL, ce qui les rend incapables de communiqueravec le nœud parent.

II. 9. 3Attaques sur le trafic :

il s'agit d'avoir un impact sur le trafic du réseau, classée en deux sous-catégories qui sont :

II. 9. 3. 1 Les attaques passives :

Dans lesquelles les attaquants produisent des activités d'écoute telles que l'analyse du trafic du réseau.

II. 9. 3. 2 Attaques par tromperie/désappropriation :

Dans lesquelles l'identité dunœud autorisé est saisie et ses performances sont surestimées et revendiquées. Ces attaques sont utilisées comme première étape pour d'autres attaques.

Selon la figure 15de la classification des attaques de la sécurité RPL, l'attaque du rang est l'une des attaques indirectes de la catégorie des ressources du réseau.

Selon la base du calcul du rang, les nœuds enfants de latopologie du réseau doivent avoir les rangs les plus élevés. L'attaque du rang avec les chemins réguliers du réseau peut entraîner une perte de paquets qui est directement proportionnelle à l'attaque.

Le nœud parent attire toujours le nœud enfant,en tenant compte de l'emplacement du rang dunœud voisin.

Cela signifie qu'un nœud parent est choisi pour un nœud enfant particulier pour gérer la qualité de ses services et envoyer ses paquets de données en se basant sur le nœud qui a le rang le plus bas [34]. L'attaque de rang est l'attaque la plus destructrice parmi les autres pour le protocole RPL car elle produit d'autres attaques telles que le trou noir, le sinkhole, etc.

Un nœud malveillant peut manipuler le rang pour dégrader intentionnellement les performances. [35]

II. 10 Conclusion :

Nous avons tenté, le plus possible, de mettre en évidence le protocole RPL, qui satisfait aux exigences des réseaux LLN telles que la consommation d'énergie et la perte des paquets. Ce protocole permet également l'optimisation des réseauxde différents scénarios d'application et de déploiements. Et ce, avec des défenses sécuritaires susceptibles d'être pénétrées par des attaques du RPL.

Chapitre III:

Evaluation des performances.

III. 1 Introduction:

Cette étude s'intéresse à l'implémentation du protocole de l'extension RPL. Elle emploie des outils (VMware Workstation Player,Le simulateur cooja et ContikiOS) pour évaluer notre constat qui vise la détection des attaques du rang sur le protocole RPL.

III. 2 Les outils de la simulation :

III. 2. 1VMware Workstation Player:

VMware Workstation Player est un outil permettant de créer des machines virtuelles pour y'installer un système d'exploitation qui se diffère de celui de la machine hôte. Il prend en charge des systèmes d'exploitation (Linux et Windows).

Nous allons utiliser la solution VMware WorkstationPlayer pour exécuter une machine virtuelle sur Windows 10nommé Instant ContikiOS[36].

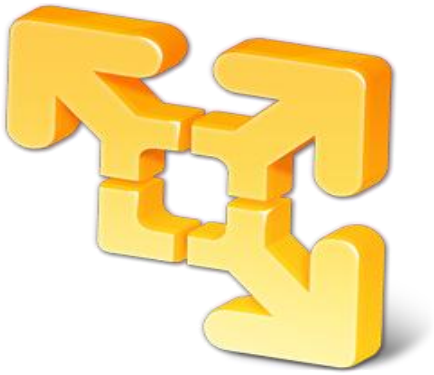

Figure 16: VMware Workstation Player[36].

III. 2. 2Contiki OS:

Les chercheurs dans l'IOTutilisent des systèmes d'exploitationlégers. Ces derniers ont été développé en faveur des systèmes à ressourceslimitées - les réseaux capteurs, par exemple - pour faciliter le développement des applicationsdédiées à ces systèmes, tels-que ContikiOS,TinyOS, Mantis, LiteOS et autre, chacun offre ses propres fonctionnalités.

Le système d'exploitation léger, flexible et open sourcea été développé par une équipe de recherche du centre suédois SICS. Nommé par Contiki créé par Adam Dunkels écrit en langage Cen 2002.[37][38]

Il propose les principales caractéristiques et fonctionnalités d'un système d'exploitation tout en favorisant une consommation énergétique et une utilisation de minimale mémoire.

Ses principes sont le support des protocoles IPv6 et 6LoWPAN, la flexibilité et la portabilité.

Il est disponible gratuitement sous licence BSD et il peut être utilisé et modifié, même à des fins commerciales.

Figure 17: Le logo de Contiki OS[42].

III. 2. 2. 1Architecture:

Le système d'exploitation Contiki est basé sur une architecture modulaire contrairement à un système d'exploitation monolithique.

Il se constitue tel qu' il montré dans la figure 18 :

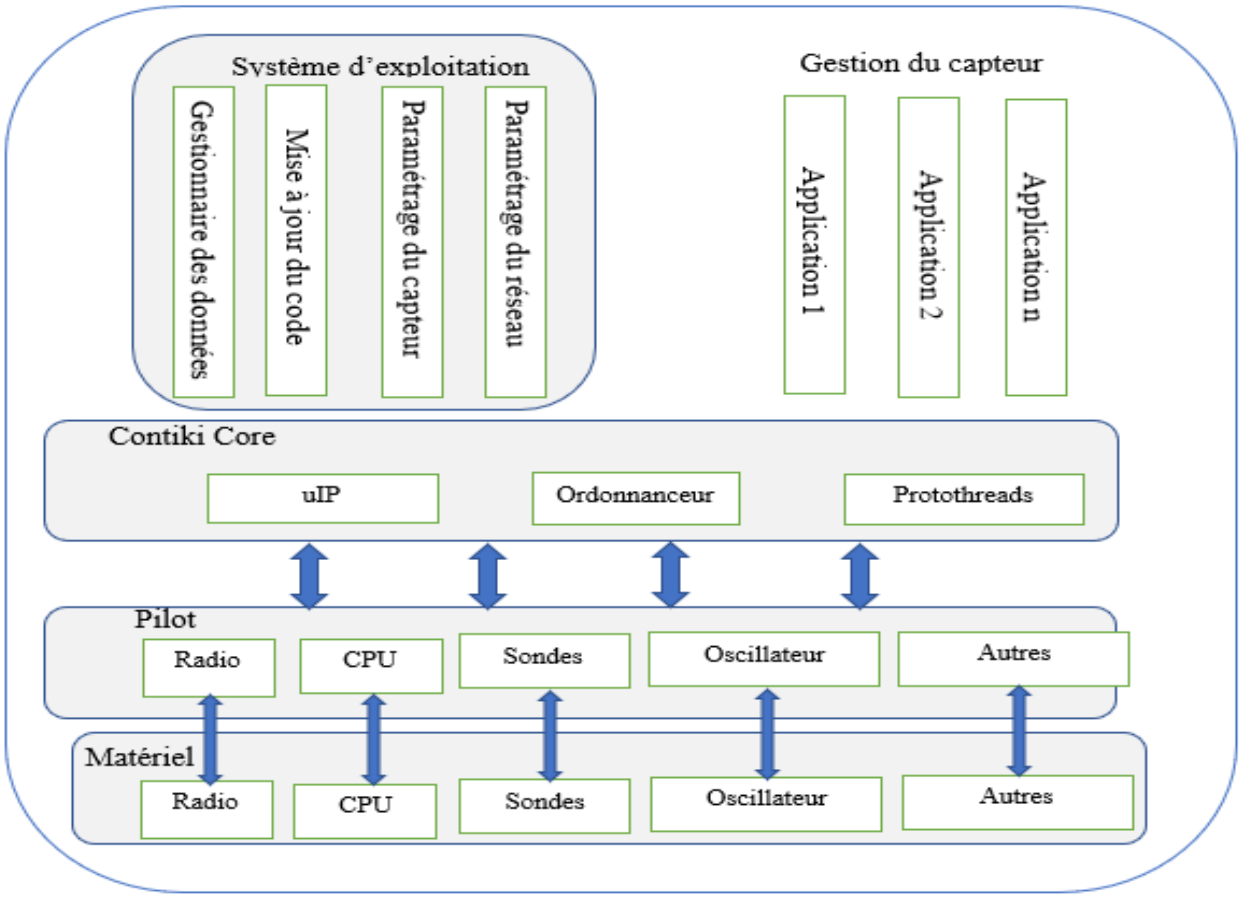

Figure 18: Architecteur contiki[43].

Contiki est un système événementiel dans lequel les processus sont implémentés comme des gestionnaires d'événements qui s'exécutent jusqu'à la fin.

système Contiki est divisé en deux parties : le noyau et les programmes chargés. Le noyau est constitué du noyau Contiki, le chargeur de programmes, le langage d'exécution et une pile de communication avec des pilotes de périphériques pour le matériel de communication[39].

III. 2. 3Le simulateur cooja :

Parmi les simulateurs de réseau des capteurs,Cooja(Java Contiki OS)qui en est une forme

Abrégée conçue pour:

- Simuler des réseaux de capteurs utilisant le système d'exploitation Contiki;
- Simuler simultanément les différentes couches du réseau;
- Émuler des objets connectés réelles tels que Skymote,Z1mote, MicaZ ...etc.

III. 3 L'installation :

Avec une manière simple, celle d'installer et d'utiliser ContikiOS,il vous suffit de télécharger Instant Contiki.zip, qui est une machine virtuelle créée avec toutes les chaînes d'outils et les logiciels nécessaires au développement de ContikiOS[40]. Mais, avant ce-ci, il faut télécharger et installer VMware Workstation Player sur la machine locale.

Apres avoir ouvert la fenêtre de lecture VMware, clique sur « Open a virtuale machine » où on cherche le fichier VMX.

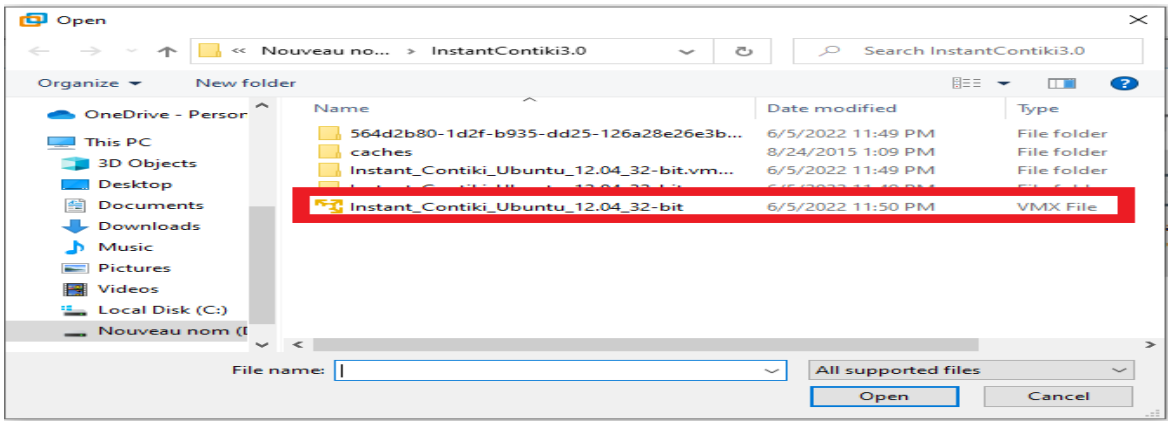

Figure 19: le fichier VMX.

- Configurer la machine avec ses caractéristiques.

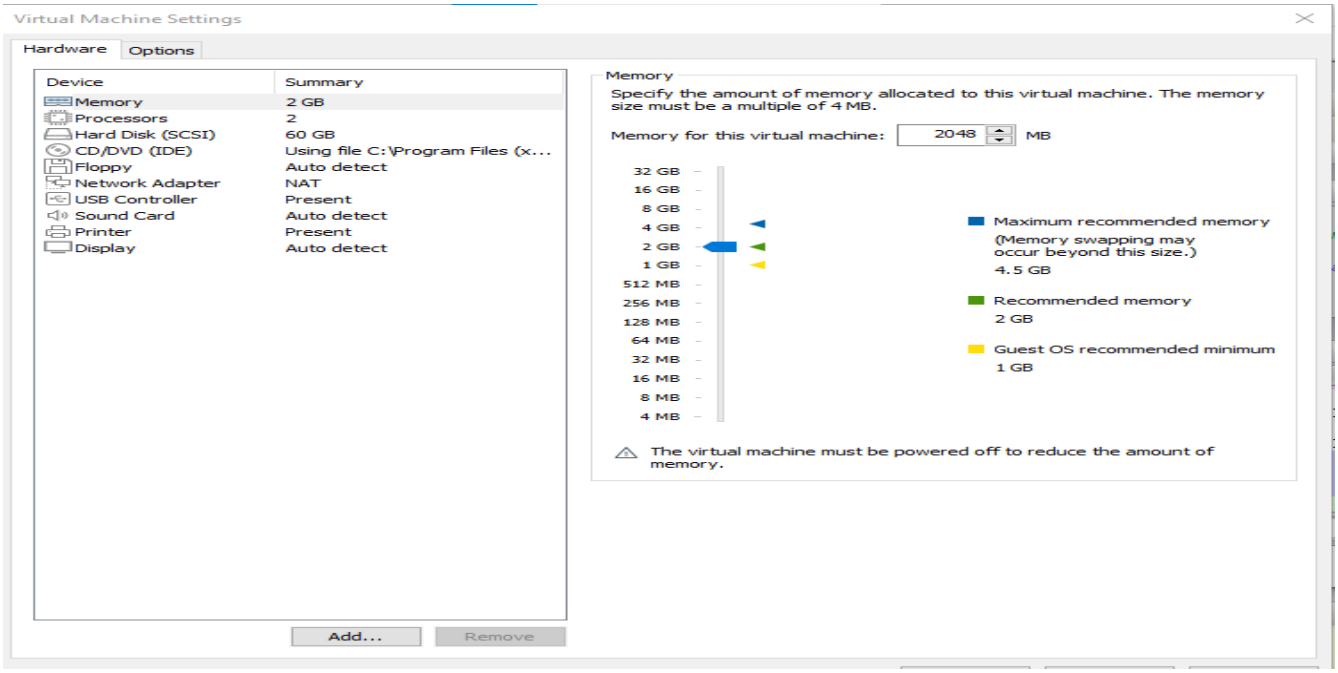

Figure 20: Caractéristiques de la machine virtuelle utilisée pour les simulations.

- Lancer la machine virtuelle.
- Taper le mot de passe par défaut : « user ».
- Appuyer sur le « terminal » où on tape les commandes suivantes :

A. « sudo apt-get update »
B. « sudo apt-get upgrade »
C. « sudo apt update »
D. « sudo apt upgrade »

- Ouvrir le simulateur Cooja en tapant sur le « terminal » les commandes « cd contiki\tools\cooja »puis « ant run ».

III. 4 Métriques de la simulation :

Dans le but de mesurer les performances de protocole de routage RPL avec ou sans des attaques, on emploie les métriques suivantes :

III. 4. 1Energie :

Elle montre l'énergie consommée par les nœuds du réseau.

III. 4. 2Délai de bout en bout :

Divergence entre le moment où l'expéditeur a généré le paquet et celui où le récepteur a reçu le paquet. Le retard E2E est également connu sous le nom de délai unidirectionnel qui se réfère à la période nécessaire au paquet pour être transmis à travers le réseau de l'expéditeur au récepteur.

Formule :

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

III. 4. 3Taux de réussite (PDR) :

Elle montre le rapport entre le nombre de paquets de donnéeslivrées à la racine et le nombre de paquets envoyés par les différents nœuds du DODAG :

$$PDR = \frac{\sum Messages reçus par la racine}{\sum Messages envoyés par les noeuds du DODAG}$$

III. 5 Le déroulement de la simulation:

On crée une simulation nommée « My simulation » munie de :

III. 5. 1Configuration :

- Créer un nœud serveur parcourir «/home/user/contiki/examples/ipv6/rpl-udp/udp-server.c» ;
- Créer un nœud client parcourir «/home/user/contiki/examples/ipv6/rpl-udp/udp-client.c».

III. 5. 2Paramètres :

Tableau 1: Les paramétres de la simulation.

Paramètres	Valeurs
Simulateur	Cooja
Nombre de nœuds	15 nœuds client légitime avec une couleur jaune
Nombre de nœuds racines	1 nœud serveur avec une couleur verte
Nombre de nœuds malveillants	8 nœuds malveillants avec une couleur violet
Durée de la simulation(s)	3600
Identité du nœud racine	1
Surface (mètres)	300 X 300
La fonction objective	MRHOF
Mote startup delay (ms)	1,000
Topologie	Random
Mote types	Z1
Radio Environment	UDGM(Distance Loss)

III. 5. 3Scenario 1:

Il s'applique dans des conditions stables. C'est une simulation avec les paramètres de la table 1 mais sans le paramétré des nœuds malveillants.Puis on vérifie les métriques de performance.

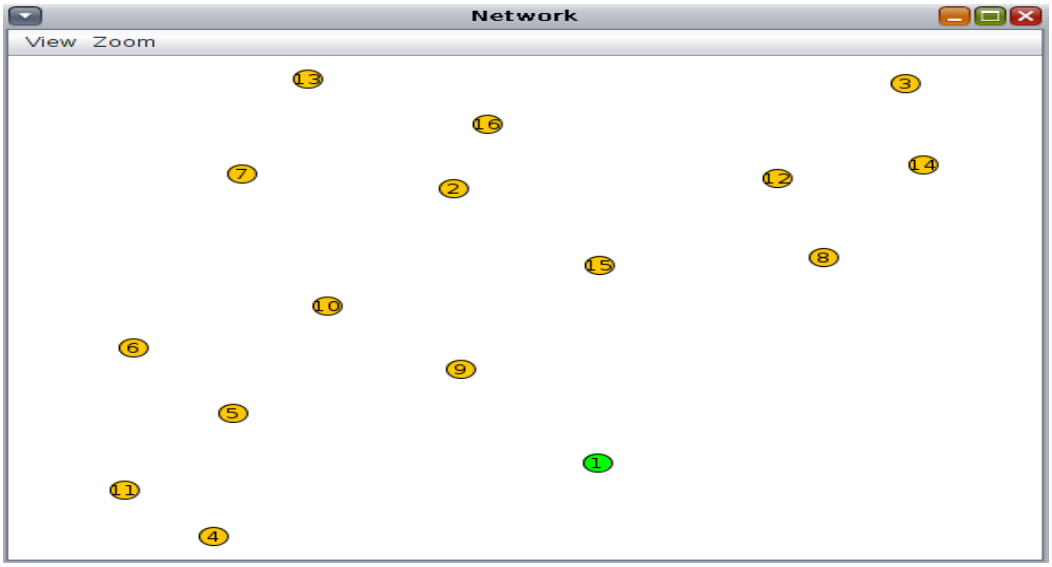

Figure 21: la topologie du réseau dans le scénario 1.

III. 5. 4Scénario 2 :

Il s'effectue en ajoutant au scénario 1 le paramètre des nœuds malveillants qui appliquent les attaques de transmission sélective.

III. 5. 4. 1 Les attaques de transmission sélective (selective forwarding) :

Dans l'attaque par transfert sélectif, un attaquant ne transfère que des paquets sélectionnés.Par exemple, un attaquant peut transmettre uniquement les messages de routage et laisser tomber tous les autres paquets pour perturber la partie du réseau.

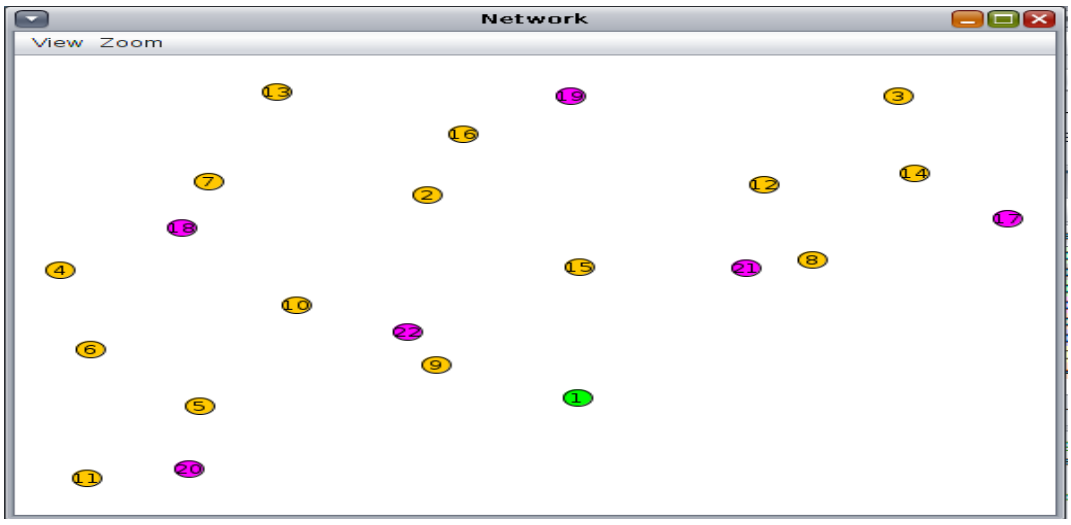

Figure 22: la topologie du réseau dans le scénario 2.

III. 5. 5Scénario 3 :

C'est le scénario 2mais les nœuds malveillants appliquent les attaques par trou noir (black hole).

III. 5. 5. 1 L'attaque trou noir (black hole) :

Dans l'attaque Blackhole, un intrus malveillant laisse tomber tous les paquets qu'il est censé transmettre. Cette attaque peut être très préjudiciable lorsqu'elle est combinée à une attaque de type "sinkhole", entraînant la perte d'une grande partie du trafic.

III. 6 La représentation des résultats de la simulation :

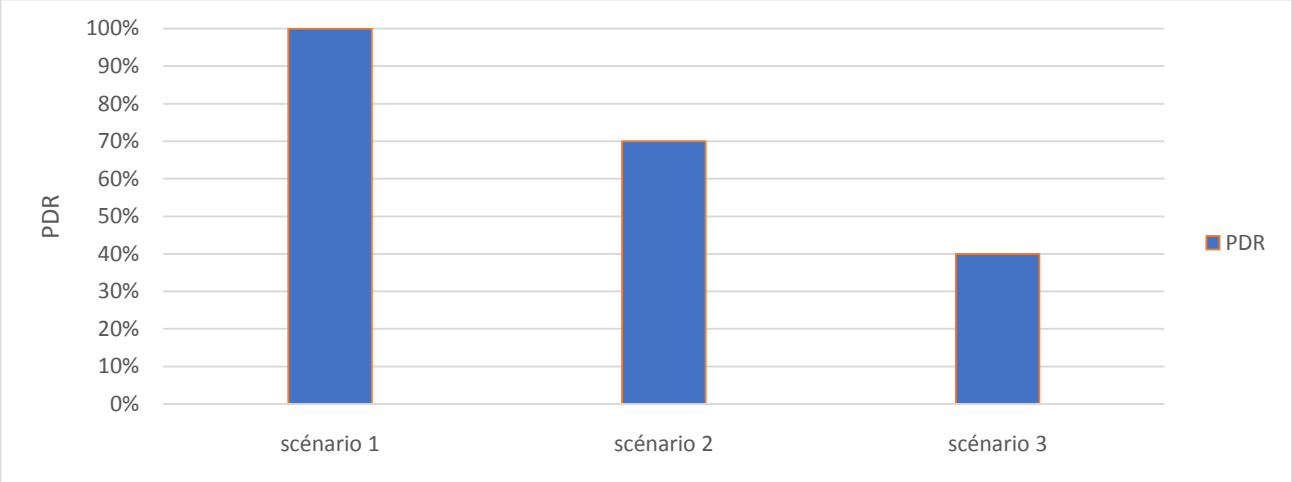

Figure 23: La valeur du PDR dans les 3 scénario.

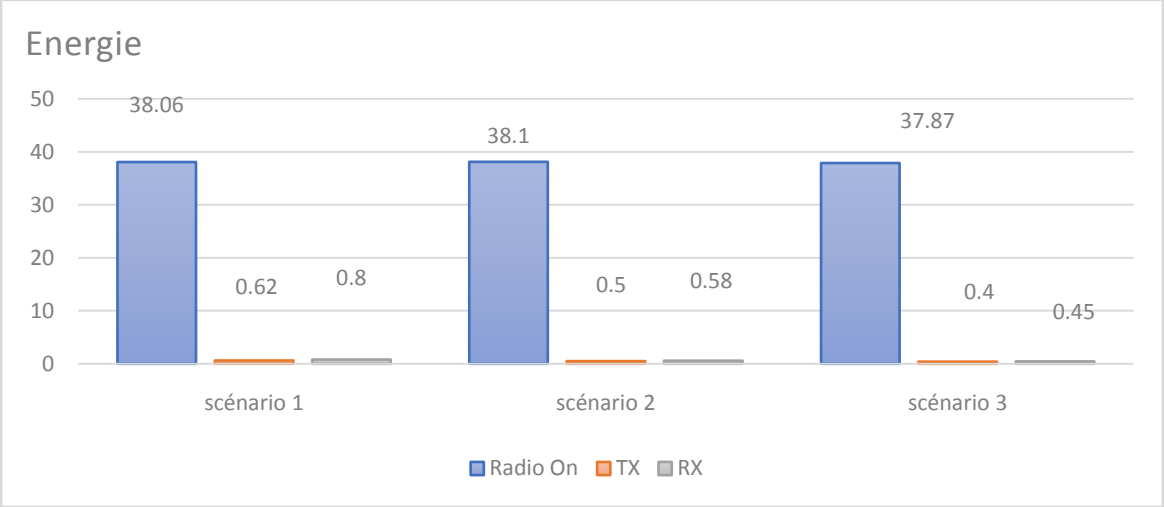

Figure 24:la consommation d'énergie dans les 3 scénario.

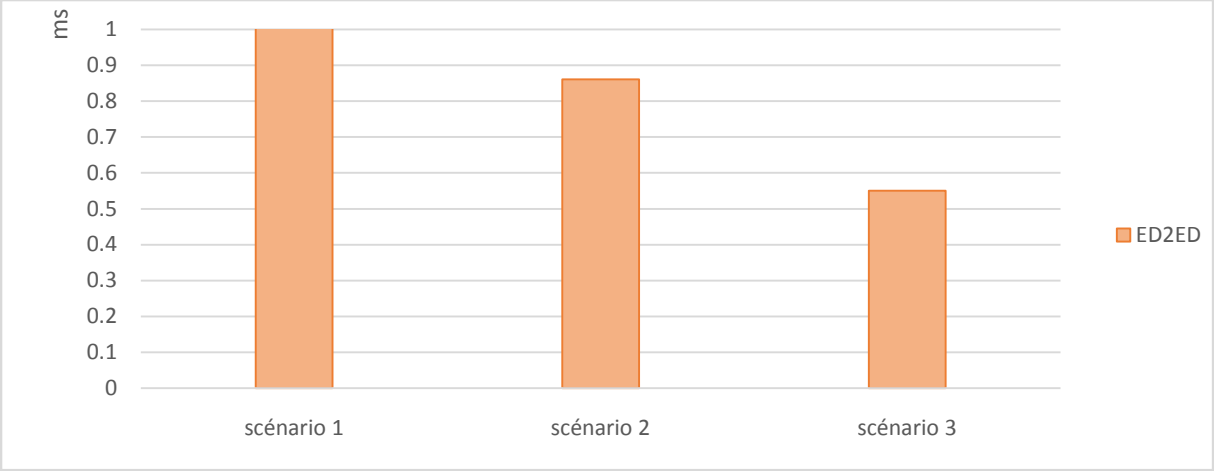

Figure 25: Retard E2E dans les 3 scénario.

III. 7 La discussion:

A travers la figure 22, la valeur de PDR dans les trois scénarios a été comme suit :

- Premier scénario :

Selon les conditions normales et la topologie évoquée dans la figure 21, on a obtenu une valeur de PDR=1

C'est à dire le trafic des paquets dans le réseau s'est effectué 100%.

-Deuxième scénario :

Dans les paramètres de scénario 2, on est arrivé à une valeur de PDR= 70% ; une perte de 30% des messages envoyés par les nœuds du DODAG vers le puits.

-Troisième scénario :

On a remarqué une perte aigue des paquets qui s'approche de 60% autrement dit la valeur de PDR=40%.

Au cours de la détection des nœuds malveillants qui influencent sur la transmission des paquets sur le réseau - mesurée par la métrique PDR-, la perte des paquets a été partielle (30%),chose qui montre que les attaques exécutées dans le scénario 2 influencent sur une partie du réseau.

Mais, en comparaissant avec le PDR de scénario 3 (60%), on a su que les attaques du trous noirs détruisent plus de paquets.

Le principal résultat de ce travail qu'on est arrivéà saisir les défis et les études actuelles pour la détection des attaques du rang dans le protocole de routage RPL.

À travers les messages de contrôle DIO échangés entre les nœuds du réseau, on a remarqué qu'ils choisissent leurs rangs d'une manière trompeuse. Ces faux rangs choisis appartiennent à un intervalle suspect, supérieur au rang dunœud puits (root) et inférieur au rang dunœud (client) le plus proche du root.Si la valeur du rang de l'attaquant appartient à cet intervalle, le nœud malveillant peut être un parent préféré ou un membre de la liste des parents de chaque nœud.

On a tenté de dresser certaines instructions pour vérifier les rangs des membres de la liste des parents de chaque nœud. Si un membre a un rang qui appartient a cet intervalle suspect, ce nœud(membre) sera un nœud malveillant.

A travers la figure 23, les valeurs de la consommation d'énergie dans les trois scénarios a été comme suit :

- Premier scénario :

Selon les conditions normales et la topologie évoquée descénario 1 , on a obtenu une valeur de Radio On =38,06 ; Tx=0,62 ; Rx= 0,8.

Après l'application des attaques dans le deuxième et le troisième scénario on a obtenu les valeur suivant:

-Deuxième scénario : Radio On =38 ,1 ; Tx= 0,5 ; Rx=0,58 .

-Troisième scénario : Radio On = 37,78 ; Tx=0,4 , Rx=0,45 .

La solution que nous avons choisie ne consommait pas beaucoup d'énergie.

A travers la figure 24, les valeurs de ED2ED dans les trois scénarios a été comme suit :

Scénario 1 : selon les conditions normales tous les nœuds du réseau échangent des paquets, Alors il y a un congestion qui contribue a élever le ED2ED.

Dans le deuxième scénariol'échange des paquets diminue partiellement par les attaques de transmission sélective, Alors la congestion diminue et le ED2ED aussi.

Dans le troisième scénario l'échange des paquets diminue pluspar les attaques du trou noir, Alors la congestion le ED2ED diminuent.

III. 8 Conclusion:

En conclusion de ce troisième chapitre, on peut dire que l'emploi du coojacomme un environnement de simulation pour le protocole RPL, nous a tellement aidé à réaliser l'idée de défense contre les attaques RPL.Sa réalisation nous a permis d'être sûr que l'attaque du trou noir perd les paquets d'une manière totale tandis que l'attaque de transmission sélective perd partiellement les paquets.

Ces deux attaques se croisent au fauxrang appartenant à l'intervalle suspect.

Conclusion générale :

Dans cette étude nous avons abordé la sécurité d'Internet des objets du côté du routage dans le réseau 6LAWPAN.

Dans le premier chapitre, on a présenté une vue générale sur l'écosystème de lIoT (architecture, notions de base, infrastructure, domaine d'application…….).

Ainsi, nous avons traité les protocoles employés dans les différentes couches de ces écosystèmes, et compris les protocoles principaux du routage dans la couche réseau.

Ces derniers protocoles nous ont passé au deuxième chapitre dans lequel le protocole RPL a été notre objet d'étude.On est arrivé à affirmer que RPL répond aux besoins des ressources limitées des LLN.

Conçu par IETF comme protocole du routage proactif multi-saut , RPL se base sur une topologie de variables sensibles, le rang par exemple, qui décrit les positions des composants de la topologie, se compte par la fonction objective MRHOF en se référant aux métriques du routage.Sa sensibilité est réduite par RPL à travers des mécanismes sécuritaires .RPL est fondé sur des mécanismes sécuritaires par défaut qui vivent en pleine optimisation, et ce, montre leur faiblesse.

Enfin, et en réponse à l'amélioration de sécurité, on a utilisé dans le chapitre 3 des outils pour simplifier la modélisation de l'étude -comme le simulateur cooja- via des scénarios qui représentent des attaques durang de point de vue comme le trou noir et la transmission sélective.Ces scénarios ont été évalués par des métriques (PDR, consommation d'énergie et le délai de bout en bout) .

Si on constate :

- diminution anormal de PDR ;
- consommation abusive d'énergie ;

- existence des nœuds ayant des faux rangs appartenant à un intervalle suspect plus grand durang de route et moins que le rang du nœud légitime le plus proche dunœudpuits , on pourra considérer ces nœuds comme des attaquants.

Les résultats obtenus dans ce travail nous ouvrent un large horizon de recherche, Autrement dit, y -aura-t-il des méthodes ou des solutions plus efficaces et plus légères pour plus de sécurité dans le domaine de l' IoT ?

Bibliographie

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.

[2] Atzori, L., Lera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805.

[3] https://www.ideematic.com/actualites/2018/12/les-objets-connectes-quelles-opportunites-et-interets-pour-les-entreprises/(consulté le 15 Mars 2022).

[4]https://www.smartgrids-cre.fr/encyclopedie/linternet-des-objets-au-coeur-des-smart-grids/definitions-autour-des-objets-connectes(consulté le 15 Mars 2022).

[5] https://pastebin.com/kW4fpPEd(consulté le 15 Mars 2022).

[6] http://www.automation-sense.com/medias/images/objets-connectes.jpg(consulté le 15 Mars 2022).

[7] https://www.connectwave.fr/techno-appli-IoT/IoT/reseaux-et-infrastructures-IoT/(consulté le 20 Mars 2022).

[8] https://www.geeksforgeeks.org/architecture-of-internet-of-things-IoT/(consulté le 22 Mars 2022).

[9] https://azure.microsoft.com/fr-fr/overview/internet-of-things-IoT/IoT-technology-protocols/(consulté le 28 Mars 2022).

[10] https://whatis.techtarget.com/definition/Constrained-Application-Protocol(consulté le 28 Mars 2022).

[11] https://www.geeksforgeeks.org/user-datagram-protocol-udp/(consulté le 29 Mars 2022).

[12]https://www.emnify.com/IoT-glossary/udp#:~:text=UDP%20in%20IoT%20In%20IoT%20%28and%20data%20transmission,it%20uses%20less%20data%20and%20consumes%20less%20power(consulté le 29 Mars 2022).

[13] Winter T, Thubert P (2010) RFC 6550: RPL: IPv6 routing protocol for Low-Power and Lossy Networks, Internet Engineering Task Force (IETF) Request For Comments, March 2022.

[14] https://sarssi14.liris.cnrs.fr/ressources/pdfs/sarssi2014_amayzaud.pdf(consulté le 5 Avril 2022).

[15] Etude-de-lauthentification-dune-source-de-diffusion-dans-le-contexte.pdf (univ-tlemcen.dz).(consulté le 6 Avril 2022).

[16] http://opera.inrialpes.fr/people/Tayeb.Lemlouma/Papers/AdHoc_Presentation.pdf(consulté le 8 Avril 2022).

[17] Sobral, J. V. V., Rodrigues, J. J. P. C., Rabêlo, R. A. L., Al-Muhtadi, J., & Korotaev, V. (2019). *Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications. Sensors, 19(9), 2144*.

[18] Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.; Alexander, R. RPL: IPv6 Rotuing Protocol for Low-Power and Lossy Networks. Available online: https://tools.ietf.org/html/rfc6550 (consulté le 11 avril 2022).

[19] Iova, O.; Theoleyre, F.; Noel, T. Using multiparent routing in RPL to increase the stability and the lifetime of the network. Ad Hoc Netw. 2015, 29, 45–62.

[20] O. Gaddour, A. Koubaa, S. Chaudhry, M. Tezeghdanti, R. Chaari, and M. Abid, "Simulation and performance evaluation of DAG construction with RPL," in Proceedings of the 3rd IEEE International Conference on Communications and Networking, pp. 1–8, 2012.

[21] Olfa Gaddour et al. "OF-FL: QoS-Aware Fuzzy Logic Objective Function for the RPL Routing Protocol". In: 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt) (2014).

[22] O. Gnawali. "The Minimum Rank with Hysteresis Objective Function". In: Internet Engineering Task Force (IETF) 6719 (2012).

[23] Ed P. Thubert. "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)". In: Internet Engineering Task Force (IETF) 6552 (2012).

[24] Wei Xiao et al. "An Optimization of the Object Function for Routing Protocol of Low-Power and Lossy Networks". In: 2nd International Conference on Systems and Informatics (ICSAI 2014) (2014).

[25] Internet Assigned Numbers Authority (IANA). Internet Control Message Protocol version 6 (ICMPv6) Parameters. http://www.iana.org/assignments/, 2011.

[26] http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-106.pdf(consulté le 26 Avril 2022).

[27] 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.

[28] Mr. Tall HAMADOUN, "Réseau maillé sans fil à basse consommation énergétique", Mémoire de Stage de fin d'études Master Informatique, institut de la Francophonie Lyon 1.

[29] 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.

[30] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A security threat analysis for the routing protocol for low-power and lossy networks (RPLs)," tech. rep., 2015.

[31] A. Kamble, V.S. Malemath, D. Patil, Security attacks and secure routing protocols in RPL-based internet of things : survey, in: Presented at the 2017 In ternational Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, 2017, pp. 3-5 .

[32] W. Mardini , M. Ebrahim , M. Al - Rudaini , Comprehensive performance analysis of RPL objective functions in loT networks , Int . J. Commun . Netw . Inf . Secur . (IJCNIS) 9 (3) (2017) 323-332 .

[33] A. Mayzaud , R. Badonnel , I. Chrisment , A taxonomy of attacks in RPL - based internet of thing , Int . J. Netw . Secur . 18 (3) (2016) 459-473 .

[34] - V.K. Karthik, M. Pushpalatha , Addressing attacks and security mechanism in the RPL based loT , Int . J. Comput. Sci. Eng. Commun . 5 (5) (2017) 1715-1721.

[35] - A. Althubaity , H. Ji , T. Gong , M. Nixon , R. Ammar , S. Han , ARM : a hybra specification - based intrusion detection system for rank attacks in 6TISC networks , in : Presented at the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) , Limassol , Cypru 2017 , pp . 12-15.

[36] https://www.blogdumoderateur.com/tools/vmware-workstation-player/. (consulté le 27 Mai 2022).

[37] The Contiki MAC Radio Duty Cycling Protocol Adam (slidetodoc.com) (consulté le 27 Mai 2022).

[38] Edosoft Factory, CONTIKI AND TINYOS, (consulté le 13Mai 2022).

[39][Enligne]https://www.google.com/url?sa=t&rct=j&q=&erc=s&source=web&cd=&cad=

rja&uact=8&ved=2ahUKEwjoyKig rxAhWlz4UKHctxBn8QFjAAegQIBBAD & url = http % 3A % 2F % 2Fwww.contiki os.org % 2F & usg = AOvVaw1kQf_ZYjADt420x - dTueF2 .(consulté le 15 Mai 2022).

[40] https://anrg.usc.edu/contiki/index.php/Installation(consulté le 16 Mai 2022).

[41] http://www.infiniteinformationtechnology.com/iot-connectivity-iot-protocol-layers(consulté le1Jui 2022).

[42]https://www.thewindowsclub.com/wp-content/uploads/2016/01/Contiki-OS-vs-Windows-10-for-Internet-of-Things.png?ezimgfmt=ng:webp/ngcb190(consulté le 1Jui 2022).

[43] Embedded Operating Systems for the IoT - (virginia.edu)(consulté le 1 Jui 2022).