UNIVERSITÉ KASDI MERBAH OUARGLA

Faculté des nouvelles technologies, de l'information et de la communication

Département d'informatique

Mémoire

Présenté pour l'obtention du diplôme de

MASTER ACADEMIQUE

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Administration – Sécurité - Réseaux

Présenté Par :

Ibrahim Katchalou Ahmed & Aboubacar Issa Mohamed

Thème :

ETUDE COMPARATIVE DES IMPACTS DES ATTAQUES IOT SUR LES RESSOURCES RPL

Soutenu publiquement le :
18/06/2022

Devant le jury composé de :

Pr Korichi Ahmed	President	UKM Ouargla
Amirate H	Examinateur	UKM Ouargla
Dr Akram Boukhamla	Superviseur	UKM Ouargla

Année Universitaire : 2021/2022

Remerciements

Nous tenons tout d'abord à remercier ALLAH le Tout-Puissant de nous avoir donné la santé, le courage et la volonté de réaliser ce mémoire.

Nous remercions et témoignons notre reconnaissance à notre encadreur Mr. Akram Boukhamla pour ses précieux conseils, ses soutiens constants et ses aides qui nous ont permis de mener à bien ce travail.

Nous tenons également à exprimer une reconnaissance aux membres du jury pour avoir accepté d'examiner et de porter leur jugement sur notre travail.

Nos vifs remerciements à nos familles pour nous avoir aidé à surmonter tous les obstacles et forger sur dent à travers les difficultés vécues tout au long de cette période de travail.

Nos vifs remerciements à nos proches amis qui nous ont vivement soutenus et encouragés au cours de la réalisation de ce modeste travail, et nos remerciements à toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce modeste travail :

A mes chers parents, pour tous leurs amours, leurs patiences, leurs grands

Sacrifices et leurs soutiens tout au long de mes études,

A mes chères frères et sœurs Djibril, Bachir et Farida pour leurs encouragements

Permanents et leur soutien moral,

A Kadidja, Mohamed et Aminou qui m'ont encouragé et à qui je

Souhaite énormément de succès,

A mes professeurs de mémoire, pour leurs suivis, leurs soutiens et leur conseil.

AHMED

Je dédie ce modeste travail tout d'abord :

A mes chers parents, pour tout leur amour, leur patience, leur sacrifice et surtout leur soutien tout au long de mes études,

A mes frères et sœurs pour leurs encouragements permanents et leur soutien moral,

A mon oncle qui se trouve à Alger qui m'a été d'une grande aide et qui m'a toujours encouragé,

A mes camarades de l'université qui ont toujours été là pour moi et à qui je souhaite le succès,

Et enfin à mes professeurs de mémoire, pour leurs suivis, leurs soutiens et leurs conseils.

Mohamed

Résumé

Le concept de l'Internet des objets implique le déploiement de réseaux à faible puissance et avec perte (LLNs), composé de milliers de nœuds contraints et de liaisons non fiables. Ces réseaux LLNs présentent de nouveaux défis surtout concernant le routage. L'IETF a conçu le protocole de routage pour les réseaux à faible puissance et avec perte (RPL) pour prendre en charge ces réseaux contraints. RPL organise des réseaux à faible puissance et avec perte sous la forme d'un ou de plusieurs graphes acycliques orientés dirigés vers une destination (DODAGs).

Chaque nœud possède plusieurs métriques ou propriétés telles que l'énergie, le PDR, etc qui permettent le bon fonctionnement de celui-ci.

Un nœud malveillant peut provoquer une surcharge au niveau du réseau RPL et agir sur les métriques des différents nœuds. Malheureusement, les services de sécurité actuellement disponibles dans RPL ne le protégeront pas contre un nœud interne compromis qui peut nuire au bon fonctionnement du réseau.

Dans ce mémoire, nous allons étudier et comparer les répercussions de quelques attaques IOTs sur les métriques des nœuds du réseau RPL

Mots-clés : Internet des Objets, Sécurité, LLN, RPL, Noeud.

Abstract

The concept of the Internet of Things involves the deployment of low-power, lossy networks (LLN), consisting of thousands of constrained nodes and unreliable links. These LLN present new challenges especially regarding routing. The IETF designed the Routing Protocol for Low Power and Lossy Networks (RPL) to support these constrained networks. RPL organizes low-power, lossy networks as one or more directed destination-directed acyclic graphs (DODAG).

Each node has several metrics or properties such as energy, PDR, etc. that allow it to function properly.

A malicious node can cause an overload at the level of the RPL network and act on the metrics of the different nodes. Unfortunately, the security services currently available in RPL will not protect it against a compromised internal node that can harm the proper functioning of the network.

In this thesis, we will study and compare the repercussions of some IOT attacks on the metrics of the nodes of the RPL network.

Keywords: Internet of Things, Security, LLN, RPL, Node.

ملخص

تتكون من آلاف العقد المقيدة والروابط غير ، (LLNs) يتضمن مفهوم إنترنت الأشياء نشر شبكات منخفضة الطاقة ومفقودة بروتوكول التوجيه للشبكات IETF هذه تحديات جديدة خاصة فيما يتعلق بالتوجيه .صممت LLN الموثوق بها .تمثل شبكات شبكات منخفضة الطاقة وفقدان كواحد أو أكثر من RPL لدعم هذه الشبكات المقيدة .ينظم (RPL) منخفضة الطاقة والمفقودة الرسوم البيانية الحلقية الموجهة نحو الوجهة (DODAGs).

وما إلى ذلك التي تسمح لها بالعمل بشكل PDR تحتوي كل عقدة على العديد من المقاييس أو الخصائص مثل الطاقة و صحيح.

، والعمل وفقًا لمقاييس العقد المختلفة .لسوء الحظ RPL يمكن أن تتسبب العقدة الخبيثة في زيادة الحمل على مستوى شبكة .لن تحميها من العقدة الداخلية المخترقة التي يمكن أن تضر بالأداء السليم للشبكة RPL فإن خدمات الأمن المتوفرة حاليًا في

على قياسات عقد شبكة IOT في هذه الرسالة ، سوف ندرس ونقارن تداعيات بعض هجمات RPL.

الكلمات الرئيسية :إنترنت الأشياء ، الأمن ، LLN ، RPL ، العقدة.

Liste des figures

Figure I.1 : Graphe du marché mondial de l'internet des objets de 2009 à 2019. [3] 16
Figure I.2 : Caractéristiques de l'internet des objets 19
Figure II.1 : Graphe du DAG et du DODAG. 22
Figure II.2 : Structure d'un message DIO [6] 22
Figure II.3 : Construction d'un DODAG. 26
Figure III.1 : Illustration de l'attaque Hello flooding [9] 33
Figure III.2: Illustration de l'attaque Increase Rank Attack [9] 33
Figure III.3 : Illustration de l'attaque Decrease Rank Attack [10] 34
Figure III.4 : Illustration de l'attaque SinkHole Attack [9] 35
Figure III.5 : Illustration de l'attaque WormHole Attack [9] 36
Figure III.6 : Illustration de l'attaque Worst Parent Attack [10] 36
Figure III.7 : Illustration de l'attaque DIO Suppression [11] 38
Figure III.8 : Illustration de l'attaque Black Hole [10] 38
Figure III.9 : Illustration de l'attaque DODAG Inconstancy [10] 39
Figure III.10 : Illustration de l'attaque Clone ID [9] 40
Figure III.11 : Repartition des differentes attaques sur le protocole RPL [12] 41
Figure IV.1 : Icone de l'application VMWare Player 44
Figure IV.2 : Interface de Simulation Cooja 45
Figure IV.2 : Construction de la simulation pour l'attaque DIS Flooding. 47
Figure IV.3 : Graphe de comparaison de la consommation d'énergie pendant le DIS Flooding 47
Figure IV.4 : Graphe de comparaison de la consommation d'énergie pendant le BlackHole . 48
Figure IV.5 : Graphe de comparaison de la consommation d'énergie pendant le GrayHole... 49
Figure IV.6 : Graphe de comparaison de la consommation d'énergie pendant le DIO Suppress 51
Figure IV.1 : Tableau récapitulatif des attaques 52

Liste des abréviations

6LoWPAN	IPv6 Low power Wireless Personal Area Network
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
IDS	Intrusion Detection System
IoT	Internet of Things (Internet des objets)
IEEE	Institute of Electrical and Electronics Engineers
IETF	International Engineering Task Force
IPv6	Internet Protocol Version 6
LLN	Low Power and Lossy Network
MP2P	Multi-Point to Point
P2MP	Point to Multi-Point
P2P	Point to Point
RoLL	Routing over Low-power and Lossy Network
RPL	IPv6 Routing Protocol for Low-power and Lossy Network

SOMMAIRE

Remerciements 1

Dédicaces 2

Résumé 4

Abstract 5

ملخص 6

Liste des figures 7

Liste des abréviations 8

SOMMAIRE 9

Introduction Générale 12

Chapitre I : Introduction à L'internet des Objets 14

I. Introduction 14

II. Internet des Objets 14

1. Historique 15

2. Définition 16

III. Pourquoi utiliser l'internet des objets ? 17

IV. Domaine d'application 17

V. Caractéristiques de l'iot 17

VI. Les réseaux à faibles consommation et avec perte 19

VII. Les protocoles de l'IoT 20

VIII. Conclusion 20

Chapitre 2 : Le Protocole de Routage RPL 21

INTRODUCTION 21

I. LE PROTOCOLE DE ROUTAGE RPL 21

II. FONCTIONNEMENT DU PROTOCOLE RPL 21

1. LES GRAPHES DAG ET DODAG 21
2. LES MESSAGES DE CONTROLE DANS RPL 22
3. LES TYPES DE NŒUDS DANS RPL 23
4. Identifiants RPL et procédure de construction 24
5. Maintenance de la topologie 26
6. Le fonctionnement de l'algorithme Trickle Timer 26
7. Les modes d'opération du protocole RPL 27
8. Les paradigmes de communication 27
9. Fonction objectif 28
III. Travaux d'optimisation de RPL 28
1. Choix des métriques : 29
2. Choix de la fonction objective 29
3. Optimisation de la topologie logique 30
4. Optimisation de Trickle Timer 30
Conclusion 30
CHAPITRE 3 : LES ATTAQUES CONTRE LE RESEAU RPL ET LES MECANISMES DE SECURITE 32
I. LES ATTAQUES CONTRE LE RESEAU RPL 32
Introduction 32
1. Les attaques basées sur les ressources 32
2. Les attaques basées sur la topologie 35
3. Les attaques basées sur le trafic 39
II. LES MECANISMES DE DEFENSE DU RESEAU RPL 41
Introduction 41
I. Solutions basées sur le protocole sécurisé 42
II. Les solutions basées sur le système de détection d'intrusion 42
CONCUSION 42

Chapitre 4 : Etudes des impacts de quelques attaques Iot sur le réseau RPL 44
Introduction 44
I. Outils d'implémentations 44
1. VMware Player : 44
2. Contiki OS : 45
3. Cooja : 45
II. Les différentes métriques d'un nœud en RPL 46
III. Implémentation et Etudes 46
1. DIS Flooding 46
2. BlackHole Attack 48
3. GrayHole Attack 49
4. DIO Suppress 50
Conclusion 52
Conclusion générale 53
Références bibliographiques 54

Introduction Générale

De nos jours la technologie a énormément évolué et ne cesse d'évoluée. Nous avons vu l'apparition de l'internet qui est une source immense de plusieurs types d'informations.

Ainsi la connexion de certains objets physiques à internet a donné jours à l'internet des objets (IoT) dont son intérêt et son déploiement en expansion sera ressenti dans divers domaines notamment les villes intelligentes, l'agriculture intelligente, la santé, le transport et l'éducation. Les principales exigences de réseau dans la plupart de ces déploiements reposent sur la mise en place d'infrastructures de réseau sous-jacentes de communications économes en énergie et à faible consommation. Ainsi, les réseaux à faible puissance et avec perte (LLN) répondent à un tel besoin avec des déploiements peu coûteux et moins complexes. Les LLN permettent une connectivité efficace entre de nombreux appareils IoT de petite taille et aux ressources limitées qui sont interconnectés sans fil. L'Internet des objets (IoT) est l'un des paradigmes de mise en réseau émergents les plus rapides permettant un grand nombre d'applications au profit de l'humanité. Les progrès de la technologie des systèmes embarqués et de l'IPv6 compressé ont permis la prise en charge de la pile IP dans les appareils intelligents hétérogènes à ressources limitées. Cependant, la connectivité mondiale et les ressources limitées des appareils intelligents les ont exposés à différentes attaques internes et externes, qui mettent en danger la sécurité et la confidentialité des utilisateurs. Divers risques associés à l'IoT ralentissent sa croissance et deviennent un obstacle à l'adoption mondiale de ses applications. Le protocole de routage IPv6 pour réseau à faible puissance et avec perte (RPL) est spécifié par le groupe de travail ROLL de l'IETF pour faciliter un routage efficace dans les réseaux IPv6 LoW Power wireless Area Networks (6LoWPAN), tout en tenant compte de ses limites. En raison de la nature limitée des ressources des nœuds dans l'IoT, RPL est vulnérable à de nombreuses attaques qui consomment les ressources du nœud et dégradent les performances du réseau.

L'Internet Engineering Task Force (IETF) fournit un protocole de routage LLN personnalisé et efficace. Il s'agit du protocole de routage IPv6 pour réseau à faible puissance et avec perte (RPL), qui active les réseaux IoT avec routage IPv6. RPL a été conçu pour fournir des topologies de réseau simples et structurées avec un routage sans boucle. Il facilite également la personnalisation flexible du routage pour répondre à certaines exigences de réseau pour les

différentes applications IoT. À cette fin, RPL fournit une solution de routage qui s'appuie sur une fonction d'objectif personnalisable tenant compte des différentes exigences des différentes applications IoT. Une telle propriété RPL dicte deux paramètres de routage principaux, le rang de nœud et la version de routage.

L'objectif visé dans ce mémoire est de faire une étude comparative des impacts de quelques attaques sur le réseau RPL, le fonctionnement de ces attaques et la façon dont les ressources de ce réseau sont consommées par ces attaques.

Notre travail porte essentiellement sur quatre chapitres dont le premier portera sur la présentation de l'internet des objets et de leur principaux caractéristiques , ensuite le second traitera sur le protocole RPL , ces principaux concepts , les différents protocoles et les différents domaines d'applications , puis le troisième sera basé sur les attaques IoT en générale ensuite un quatrième chapitre qui portera sur l'analyse des métriques dues à certaines attaques contre le réseau RPL et enfin une conclusion générale ainsi que quelques perspectives pour des travaux futurs.

Chapitre I : Introduction à L'internet des Objets

I. Introduction

L'internet des objets est la nouvelle ère de la mise en réseau et la communication intelligente qui est devenue un domaine attractif pour les chercheurs en raison de sa vaste collection d'application et de facilité de déploiement dans plusieurs domaines de la vie réelle.

Entre autres, il rend les objets qui nous entourent intelligents en leur offrant la faculté de communiquer entre eux pour atteindre des objectifs communs dans de nombreux domaines d'application.

Dans ce chapitre, nous présentons l'IoT, ses domaines d'application, ses caractéristiques et ses protocoles.

II. Internet des Objets

L'Internet des objets se compose d'appareils ordinaires qui peuvent se connecter à Internet et communiquer entre eux. Généralement, il est donc nécessaire d'ajouter des capteurs spéciaux à des objets ordinaires comme des machines à laver, des radiateurs, des montres, etc.

Certains appareils utilisent ces capteurs pour collecter et retransmettre des informations. Le tout premier dispositif connecté dont il est question, un distributeur automatique, utilisait des capteurs pour contrôler son inventaire et transmettre ces informations à son propriétaire.

D'autres appareils peuvent recevoir des informations, puis effectuer une action. Par exemple, les serrures de porte intelligentes reçoivent un signal indiquant que vous souhaitez les ouvrir, puis effectuent l'opération.

Les appareils connectés les plus sophistiqués (et généralement les plus utiles) peuvent faire les deux. Dans le cadre des objets connectés au milieu industriel, il peut s'agir par exemple du suivi des pièces des machines à la recherche d'éventuels dysfonctionnements, qui déclenche une alarme lorsqu'un problème est détecté. En milieu domestique, en revanche, il peut s'agir de votre thermostat intelligent, qui collecte des informations sur vos préférences et vos habitudes en termes de température, puis agit en conséquence pour chauffer ou refroidir votre domicile à la température souhaitée en fonction de l'heure de la journée.

En général, la technologie intelligente contribue à un meilleur fonctionnement des objets, gagnant en efficacité et en synchronisation.

La plupart des objets connectés en milieu domestiques se connectent à une maison intelligente, au sens large, via votre routeur, ce qui vous permet de contrôler de nombreuses fonctions de votre maison via des commandes vocales ou votre smartphone pour gagner du temps, de l'énergie voire les deux.

Sur le plan commercial, la technologie connectée aide les entreprises à surveiller et à gérer leurs usines, leurs chaînes d'approvisionnement, etc. Des capteurs peuvent également être ajoutés à certaines machines à grande échelle, comme les foreuses sur une plateforme pétrolière, pour en améliorer la production et la sécurité

.

1. Historique

Le terme Internet des Objets a été utilisé pour la première fois en 1999 par K. Ashton, co-fondateur d'Auto-ID Center au MIT dans l'une de ses présentations. [1]

Cependant déjà en 1989, Mark Weiser, professeur à Berkeley avait une vision d'un monde ou la technologie s'intègre dans les objets de la vie quotidienne. [2] Sa vision a pris forme grâce au développement de l'informatique et de l'électronique. Lors d'une de ses présentations K. Ashton décrit la façon dont les objets et les personnes du monde physique peuvent être recensés et gérer informatiquement grâce à la technologie RFID (Radio-Frequency Identification). Depuis lors, ce concept a beaucoup évolué grâce aux énormes progrès effectués dans divers domaines technologiques, allant de celui des microcontrôleurs, de la nanotechnologie, des capteurs et actionneurs à celui des technologies sans fils.

L'IoT a énormément évolué grâce aux progrès effectués dans les divers domaines technologiques. Il fait aujourd'hui référence à la possibilité de connecter tout objet du quotidien à L'Internet traditionnel. L'intérêt pour ces objets a énormément grandi au cours des dernières

années. En effet, comme le montre la Figure I.1, le marché de l'IoT continue de croître.

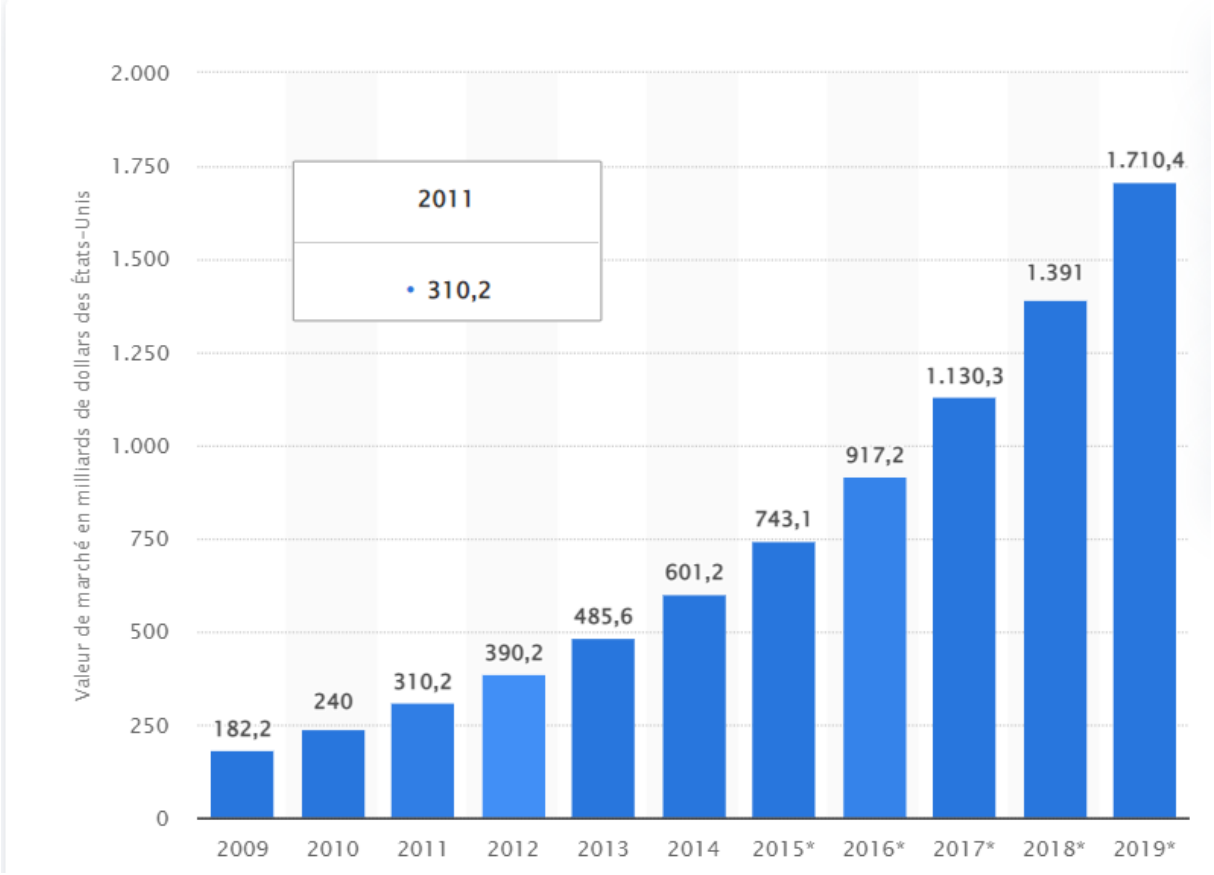


Figure I.1 : Graphe du marché mondial de l'internet des objets de 2009 à 2019. [3]

2. Définition

C'est une technologie qui permet de connecter n'importe quels ensembles d'objets du monde physique entre eux à travers l'Internet et /ou des réseaux locaux comme les réseaux des capteurs sans fil (WSN), pas seulement des dispositifs électroniques, mais consiste à intégrer et embarquer des capteurs et systèmes intelligents dans les divers produits, pour récupérer les informations et les données (sur leur identité, leurs caractéristiques et leur environnement, etc.).

L'Internet Des Objets attribue à chaque objet du monde réel une identification unique sous forme d'une étiquette lisible par des dispositifs mobiles sans fil et définit un monde dans lequel les objets peuvent communiquer automatiquement entre eux et avec des ordinateurs, prendre des décisions intelligemment et même offrir à un utilisateur distant le contrôle de ses objets afin de fournir des services pour divers secteurs (par exemple domotique, santé, industrie, etc.).

III. Pourquoi utiliser l'internet des objets ?

Tout d'abord l'IoT et sa technologie améliorent tous les aspects de notre quotidien. Par exemple, elle supprime une partie de notre effort manuel au niveau des machines en exécutant les taches à un temps donné ou selon une condition précise, réduit les couts et rend la vie plus confortable. On peut citer les machines à café automatiques, des voitures autonomes, des bracelets qui détectent et signalent les maladies parmi les applications possibles grâce à l'internet des objets.

IV. Domaine d'application

On peut citer plusieurs domaines d'application touchés par l'IoT, les principaux domaines sont :

- **Environnements intelligents** : prédictions des séismes, détection d'incendies, qualité de l'air, etc.
- **Sécurité et gestion des urgences** : radiations, attentats, explosions, etc.
- **Logistique** : facilite les décisions d'approvisionnement, suivre des éléments spécifiques dans le processus de la livraison, etc.
- **Contrôle industriel** : mesure, pronostic et prédiction des pannes, dépannage à distance.
- **Santé** : suivi des paramètres biologiques à distance.
- **Agriculture intelligente**, **domotiques, applications ludiques**, etc.

V. Caractéristiques de l'iot

L'internet des objets a pris une place très importante parmi les technologies du 21^{e} siècle attirant l'attention de nombreux experts, gouvernements et industries. L'importance de l'iot augmentant de jour en jour, différentes caractéristiques doivent être prises en considération comme illustrés dans la Figure ci-dessous.

- **La mobilité**

La mobilité est un grand défi pour les implémentations iot, ou la plupart des appareils tels que les smartphones ont un degré élevé de mobilité. En effet, la mobilité est une caractéristique très demandée et importante dans le monde de l'IoT, mais elle rend également l'iot vulnérable à de nombreux risques en termes de sécurité.

- **Limitations des ressources**

Les objets IoT sont généralement différents, donc différents aussi en matière de capacités énergétiques, de stockage et de calcul. En fait la majorité des objets IoT sont réputés pour leurs contraintes de ressources limitées. Par conséquent le développement des plateformes iot doit optimiser et minimiser le plus l'utilisation de l'énergie, du stockage et du calcul des objets.

- **Interopérabilité**

Elle est très importante pour l'internet des objets car celui-ci se compose de beaucoup d'appareils hétérogène appartenant à des plateformes différentes qui communiquent avec d'autres appareils, échangent et analysent également les données entre plusieurs systèmes sur différents réseaux. Due à cela, l'internet des objets doit gérer un degré élevé d'interopérabilité.

- **Connectivité et ubiquité**

Permettre la communication et la connexion entre tous les objets est très important pour l'internet des objets. Aussi, cette connectivité pourra avoir lieu n'importe quand et n'importe où, et permet également la compatibilité d'accès au réseau et d'échanger les données.

- **L'évolutivité**

L'évolutivité, qui par définition signifie la capacité d'ajouter de nouveaux services et fonctions sans affecter négativement ceux qui sont déjà présent nécessite une mise en place de cadre de sécurité flexible et innovants qui permet de réduire le risque de sécurité.

- **Sécurité**

Caractéristique très importante au niveau de l'IoT du au nombre croissant d'appareils intelligents qui nous entourent en plus de leur hétérogénéité et leurs ressources limitées. De plus pendant la création des protocoles et des applications iot il faut bien prendre en compte la sécurité.

- **Auto-organisation et autoréparation**

Les objets IoT intelligents peuvent réagir de manière autonome et s'autoorganiser en réseaux ad hoc transitoires selon les situations, états et contexte grâce à une intelligence embarqués dont ils sont équipés, cela est dû au fait que le nombre d'objets iot et leurs états de connexion et d'emplacement changent de manière dynamique.

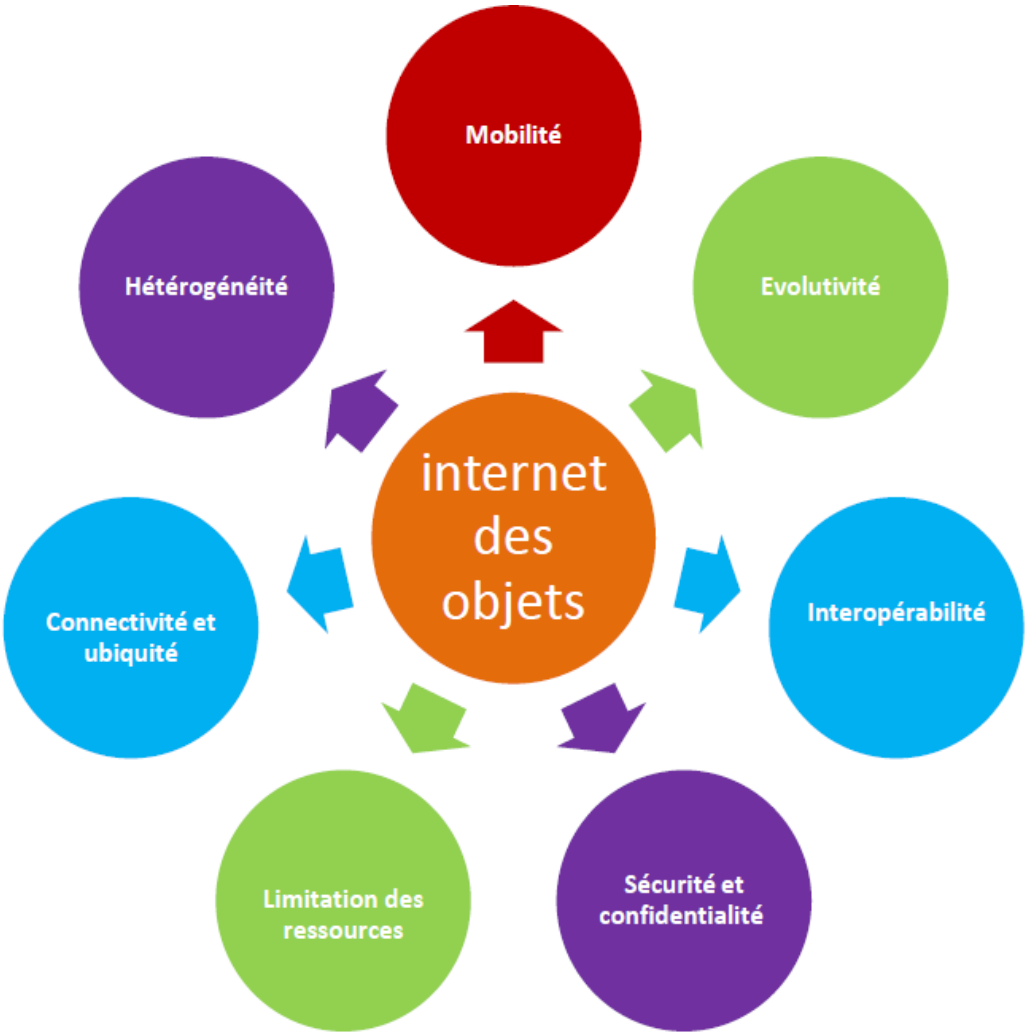


Figure I.2 : Caractéristiques de l'internet des objets

VI. Les réseaux à faibles consommation et avec perte

Nous avons évoqué ci-dessus les limitations de l'internet des objets, pour mettre en œuvre l'iot plusieurs technologies ont été impliquées en les prenant en compte nous nous concentrerons sur les réseaux à faibles consommation et avec perte (connus en anglais sous le nom « Low Power and Lossy Networks » ou « LLN ») car ils représentent un composant nécessaire pour l'iot.

Les LLNs peuvent être définis comme des réseaux de capteurs dans lesquels les routeurs et les nœuds sont fortement limités en termes de ressources en termes de capacité de traitement, de batterie et de taille de mémoire, et leurs liens d'interconnexion sont instables avec un taux de perte élevé, de faibles débits de donnés et de faibles taux de livraison de paquets.

Avec l'apparition de l'IoT et son évolution, le routage dans les LLNs est devenu l'un des principaux défis. On doit prendre en compte les limitations et les contraintes des LLNs pour

concevoir et mettre en œuvre n'importe quel protocole de routage. Un protocole de routage du nom de RPL a été spécialement conçu par l'IETF pour répondre aux contraintes spécifiques qu'impose ce type de réseaux.

VII. Les protocoles de l'IoT

Communiquer étant le seul moyen pour les objets iot intelligents d'échanger des données entre eux, l'IEEE et l'IETF travaillent continuellement à la formation et au développement de protocoles standardisés. On peut citer les plus courants dans le domaine de l'iot comme :

- **L'IEEE 802.15.4**
- **6LowPAN**
- **Le protocole de routage RPL**
- **Le protocole d'application contraint (CoAP)**

VIII. Conclusion

L'internet des objets est devenu l'une des technologies les plus importante de ce siècle et s'est développé rapidement dans le contexte des réseaux et services. Nous avons présenté dans ce chapitre tout ce qui englobe l'iot en général tel que sa définition, l'historique de l'iot, ses domaines d'applications, ses caractéristiques et les différents protocoles.

Dans le chapitre qui suit quant à lui, nous allons présenter plus en profondeur le protocole de routage RPL qui nous intéresse.

Chapitre 2 : Le Protocole de Routage RPL

INTRODUCTION

Le protocole RPL est un protocole de routage IPv6 (Internet Protocol version6) proactif a vecteur de distance. Il a été conçu par le groupe de travail ROLL de l'IETF en 2012 pour les LLN. Le fonctionnement de ce protocole est garanti par la construction d'un graphe appelé DODAG (Destination Oriented Directed Acyclic Graph) [4]. Dans ce chapitre, nous allons aborder le fonctionnement du protocole RPL en citant la procédure de construction de la topologie RPL avec leur concept clés et en citant les deux modes d'opération « Non-Storing mode » et « Storing mode », les paradigmes de la communication, suivies de la classification des travaux antérieurs sur les améliorations de RPL.

I. LE PROTOCOLE DE ROUTAGE RPL

RPL est sans doute l'un des protocoles de routage IPv6 les plus connus pour les réseaux à faible consommation et à perte (LLN) développé par ROLL dans la RFC 6550 pour répondre aux limites des réseaux LLN telles que la faible puissance de traitement, de batterie et de mémoire. RPL vise principalement les réseaux de collecte, où les nœuds envoient périodiquement des mesures à un point de collecte. Le protocole a été conçu pour être très adapté aux conditions du réseau et pour fournir des itinéraires de rechange, chaque fois que les itinéraires par défaut sont inaccessibles. RPL fournit un mécanisme pour diffuser l'information sur la nouvelle topologie de réseau formée dynamiquement.

II. FONCTIONNEMENT DU PROTOCOLE RPL

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. [5]

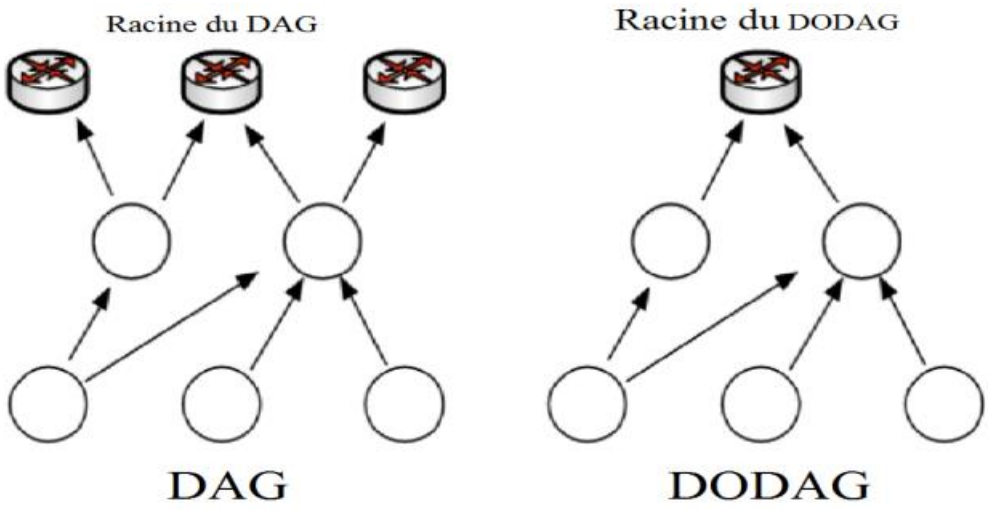


Figure II.1 : Graphe du DAG et du DODAG.

2. LES MESSAGES DE CONTROLE DANS RPL

Pour mettre en place et maintenir la topologie de routage, quatre messages ICMPv6 ont été définit pour le protocole RPL, comme illustre figure :

1. DIO (Objet d'Information DODAG) : contient des informations permettant à un nœud de découvrir une instance RPL apprendre ses paramètres de configuration de calculé son rang et de choisir des parents qui minimisent le coût sur la route vers la racine du DODAG.

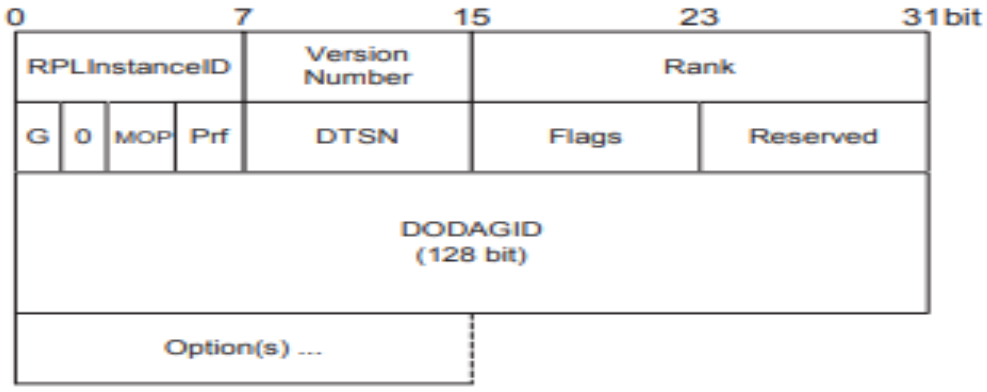


Figure II.2 : Structure d'un message DIO [6]

DIO transporte des informations qui permettent à un nœud de découvrir un parent préféré, connaître ses paramètres de configuration, sélectionner un ensemble de parents DODAG et gérer le DODAG. Il est émis par la racine DODAG pour construire un nouveau DAG, puis envoyé en multidiffusion via la structure DODAG. Le message DIO transporte des informations réseau pertinentes qui permettent à un nœud de découvrir une instance RPL, d'apprendre ses

paramètres de configuration, de sélectionner un ensemble parent DODAG et de gérer le DODAG.

2. DIS (Sollicitation Information DODAG) : pour solliciter un DIO de leurs voisins. Elle est utilisée par un nœud qui souhaite rejoindre la topologie (envoi en multidiffusion) ou réclamant des informations de configuration plus récentes (envoi en monodiffusion). Dans tous les cas, un nœud recevant un DIS répond à l'initiateur par une monodiffusion de paquet DIO. [7]

3. DAO (Destination Annonce Objet) : pour propager les informations de destination en remontant le DODAG le message DAO est unicast de l'enfant au parent. Les messages DAO sont envoyés par chaque nœud, autre que la racine DODAG, pour remplir les tables de routage avec les préfixes de leurs enfants et pour publier leurs adresses et préfixes à leurs parents. Après avoir transmis ce message DAO via le chemin d'un noeud particulier à la racine DODAG via les routes DAG par défaut, un chemin complet entre la racine DODAG et le noeud est établi. Les principaux champs de message DAO sont :

– RPLInstanceID qui est l'ID de l'instance RPL

– Indicateur K

– DAO Sequence qui est un numéro de séquence incrémenté à chaque message DAO

– DODAGID qui identifie un DODAG. [5]

4. DAO-ACK : Le message DAO- ACK est envoyé en tant que paquet unicast par un destinataire DAO en réponse à un message DAO unicast. Il est utilisé par la destination en réponse à un message DAO reçu pour acquitter ce dernier. En cas de non réception du DAO Ack par la source, celle-ci peut réémettre le DAO initial. [7]

3. LES TYPES DE NŒUDS DANS RPL

RPL définit trois types de nœuds :

LOW POWER AND LOSSY BORDER ROUTERS (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. [8]

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. [8]

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. [8]

4. Identifiants RPL et procédure de construction

Un réseau RPL est identifié par quatre champs :

Fonction Objectif (OF) : définit comment les nœuds RPL sélectionnent et optimisent les itinéraires au sein d'une instance RPL.

Rank : c'est le rang d'un nœud définit la position individuelle du nœud à d'autres nœuds à l'égard d'une racine DODAG. Classement strictement augmente dans la direction vers le bas et diminue strictement vers le haut. La façon exacte de calculer le rang se dépend de la fonction objectif (OF). Le rang peut suivre de façon analogue une distance topologique simple, peut être calculée comme une fonction de métriques de lien, et peut considérer d'autres propriétés telles que contraintes.

RPLInstanceID : Les DODAG ayant le même RPL Instance ID partagent la même fonction Objectif.

Instance RPL : Une instance RPL est un ensemble d'un ou plusieurs DODAG qui partagent un RPL Instance ID.

La construction DODAG est basée sur le processus de découverte de voisin, qui consiste en deux opérations principales : la diffusion de la transmission des messages de contrôle DIO émis par la racine DODAG pour construire des routes dans le sens descendant de la racine vers les nœuds clients, la monodiffusion des messages de contrôle DAO émis par les nœuds clients et envoyés à la racine DODAG pour construire des routes dans les directions ascendantes. Afin de construire un nouveau DODAG, la racine DODAG diffuse un message DIO pour annoncer son DODAGID, ses informations de rang pour permettre aux nœuds de déterminer leurs positions dans le DODAG et la fonction d'objectif identifiée par le point de code objectif (OCP)

dans le Champs d'options de configuration du DIO. Ce message sera reçu par un nœud client qui peut être soit un nœud prêt à rejoindre, soit un nœud déjà joint. Lorsqu'un nœud souhaitant rejoindre le DODAG reçoit le message DIO :

– il ajoute l'adresse de l'expéditeur DIO à sa liste des parents

– calcule son rang à l'aide de la fonction d'objectif spécifiée dans le fichier OCP, de sorte que le rang du nœud soit supérieur à celui de ses parents

– transmet le message DIO avec les informations de classement mises à jour Le parent le plus préféré (rang le plus petit) parmi la liste des parents du nœud client sera choisi comme un nœud par défaut par lequel le trafic entrant est acheminé. Lorsqu'un nœud déjà associé à DODAG reçoit un autre message DIO, il peut procéder de trois manières différentes :

– rejeter le message DIO selon certains critères spécifiés par RPL

– traiter le message DIO pour maintenir son emplacement dans un DODAG existant – améliorer sa localisation en obtenant un rang inférieur dans le DODAG sur la base du calcul du coût de chemin spécifié par la fonction Objective Chaque fois qu'un nœud change de rang, il doit ignorer tous les nœuds de la liste des parents dont les rangs sont supérieurs au rang du nouveau nœud calculé pour éviter les boucles de routage. Si l'indicateur de mode de fonctionnement dans l'objet de base DIO est différent de zéro, les routes descendantes de la racine aux nœuds sont prises en charge et doivent être maintenues. Dans ce cas, chaque poste client doit envoyer un message de contrôle DAO mono diffusion pour déterminer les informations de route inverse. Lors du retour à la racine DODAG, les nœuds visités sont enregistrés dans le paquet le long de la route ascendante, et la route complète est alors établie entre la racine DODAG et le nœud client. Enregistrés dans le paquet le long de la route ascendante, et la route complète est alors établie entre la racine DODAG et le nœud client. [5]

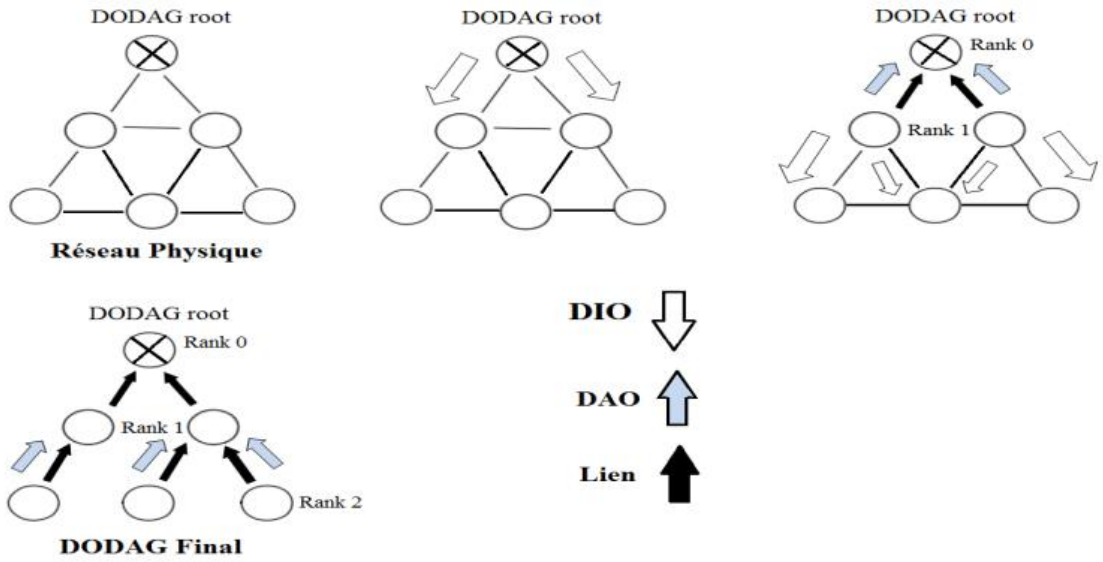


Figure II.3 : Construction d'un DODAG.

5. Maintenance de la topologie

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

Réparation globale : La racine initie une reconstruction complète du DODAG avec des messages DIO, des numéros de séquence sont utilisés pour différentier les DODAG ancien et nouveau, réparation couteuse en trafic.

Réparation locale : Recherche d'un nouveau parent par le nœud affecté, le DOGAG n'est plus optimal, seule une réparation globale permettra une nouvelle optimisation [17].

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.

7. Les modes d'opération du protocole RPL

En fonction de la capacité des nœuds en termes de mémoire et de la taille éventuelle du réseau, le protocole RPL offre deux modes de fonctionnement, le fonctionnement en « storing mode » et celui en « Non-Storing mode ».

Le fonctionnement en « Non-Storing mode » Dans ce mode, seul la racine est en mesure de stocker des informations de routage. Les autres nœuds du réseau conservent uniquement les adresses de leur parent direct. Toutes les informations sur la structuration du DODAG sont transmises à la racine dans les messages DAO. En cas de besoin de router des données vers une destination quelconque, les nœuds transmettent ces données à la racine en passant par leur parent. La racine effectuera un routage à la source vers la bonne destination.

Le fonctionnement en « Storing mode » Dans ce mode, les nœuds intermédiaires sont en mesure de garder en mémoire des informations de routage puis de rediriger les données reçues vers la bonne destination en consultant les informations du routage. Contrairement au « NonStoring mode », dans le fonctionnement en « Storing mode », les messages DAO ne sont pas tous transmis à la racine. Chaque nœud transmet son message à son parent direct (parent à un saut) qui maintient une table de routage à son niveau.

8. Les paradigmes de communication

RPL prend en charge trois paradigmes de communication (MP2P), (P2MP) et (P2P). Dans ce qui suit, nous détaillons le fonctionnement de ces modèles de communication.

Multipoint à point (MP2P) : RPL a été conçu principalement pour optimiser le type de flux de trafic multipoint à point (MP2P), cette communication MP2P a été fourni par la constructions des routes à partir de chaque nœud vers la racine DODAG à l'aide de DIO du parent préféré d'un nœud il s'agit de « Routes ascendantes » (Upward Routes) 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.

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 (préfixes, adresses ou groupes de multidiffusion). Par exemple les messages DIO, P2PM est le modèle de trafic requis par plusieurs applications LLN ([RFC5867], [RFC5826], [RFC5673] et [RFC5548]).

Point à point (P2P) : Pour le trafic P2P, la construction des routes ça dépend de mode de fonctionnement du protocole RPL. Si le cas de mode Non-Storing mode le paquet dirige vers une racine, ensuite la racine effectuera le routage vers la destination, si le cas de mode Storing mode, le paquet s'écoule vers la racine jusqu'à ce qu'il atteigne un ancêtre qui a une route connue vers la destination. Cet ancêtre commun peut être la racine DODAG. Dans d'autres cas, il peut s'agir d'un nœud plus proche de la source ou de la destination.

9. Fonction objectif

La fonction Objectif (OF) définit comment les nœuds RPL sélectionnent et optimisent les itinéraires dans d'une instance RPL. L'OF est identifié par un point de code objectif (OCP) dans l'option de configuration DIO. Un OF définit comment les nœuds traduisent une ou plusieurs métriques et contraintes, pour les buts de, calculer le rang de chaque nœud dans le DODAG, définit également comment les nœuds sélectionnent les parents. Le groupe de travail ROLL a défini deux fonctions objectives dans le RPL originale cette séparation destinée à permettre à la RPL d'être adaptée pour répondre aux critères d'optimisation différents, d'applications et de conceptions de réseaux :

• **OF0** : Objective Function Zero Ici, la métrique d'acheminement adoptée est le nombre de sauts. OF0 est conçu pour permettre l'interopérabilité entre les implémentations diffèrent de RPL. [7]

• **MRHOF** (Minimal Rank with hystérésis Objective Function) : Elle est implémentée pour fonctionner avec les métriques additives [GL12]. Dans sa définition, l'IETF utilise l'ETX comme métrique à optimiser, mais toute autre métrique additive (nombre de sauts, délai) pourrait être également utilisée. MRHOF se sert d'une hystérésis pour limiter les variations liées à l'emploi d'une métrique dynamique [7].

III. Travaux d'optimisation de RPL

Même s'il est proposé pour répondre aux contraintes de routage dans les réseaux LLN. Plusieurs travaux ont montré que RPL souffre de certains défauts. Dans cette partie, nous allons examiner une partie de ces travaux d'amélioration de RPL que nous avons classé en plusieurs catégories :

(A) optimisation de la fonction objectif, (B) optimisation de la topologie logique le nombre de chemins choisis et (C) Optimisation de la fonction Trickle Timer.

1. **Choix des métriques :**

- **Selon une seule métrique**

Par défaut, une seule métrique est utilisée dans les fonctions objectifs définies par ROLL que cela soit le nombre de saut ou l'ETX. D'autres travaux proposent néanmoins d'utiliser de nouvelles métriques visant à améliorer un aspect de façon plus spécifique. Les auteurs dans proposent de s'appuyer sur le délai de transmission moyen ou (Averaged Delay - AVG DEL) qui vise à réduire le délai entre les nœuds, tout en supposant que les nœuds fonctionnent sur des cycles de sommeil et des cycles de réveil différents et ont des cycles de travail très faibles (moins de 1%). L'inconvénient avec cette approche c'est qu'elle rajoute plus de données à un DIO déjà large, ce qui augmente le risque de fragmentation.

- **Selon plusieurs métriques**

Dans cette catégorie d'approche plusieurs métriques sont utilisées en même temps pour calculer le rang des nœuds. Le problème qui se pose est donc de trouver comment combiner ces métriques. Plusieurs solutions ont été proposées dans la littérature. Les auteurs dans s'appuient sur une approche de combinaison additive et pondérée. Dans ce cas les métriques sont normalisées et des nombres réels positifs sont utilisés comme facteurs de multiplication pour ajuster les poids relatifs des métriques de routage en fonction de l'application. Ainsi, ils ont proposé de combines deux métriques : le nombre de saut (Hop Count ou HC) et une métrique d'indicateur de confiance appelée Packet Forwarding Indication ou PFI qui permet de tester la confiance qu'un nœud peut avoir en son parent en calculant la probabilité de transfert des paquets. Cette métrique suit le concept d'ETX mais capture la fiabilité du nœud plutôt que la fiabilité du lien. En utilisant PFI, un nœud peut identifier et exclure des nœuds malicieux et parer ainsi aux attaques du trou noir ou du trou gris (black- and grey-hole attacks)

2. **Choix de la fonction objective**

Une autre approche s'appuie sur les principes de la logique floue pour combiner plusieurs métriques. Une nouvelle fonction objective OF-FL a également été mise en place. Les métriques considérées dans cette approche sont le délai de bout-en-bout, le nombre de saut, la qualité du lien et l'énergie du nœud. La logique floue est utilisée pour évaluer le meilleur voisin comme étant le parent préféré. Les études de simulation sont réalisées sur une implémentation Contiki / Cooja de RPL.

3. Optimisation de la topologie logique

Cette stratégie s'appuie sur le constat que comme il s'agit de réseaux à faible puissance et à perte, il serait intéressant non pas de considérer un chemin unique vers la racine mais plusieurs. De nombreux travaux de recherche ce sont intéressés à cette approche où une myriade de bénéfices a été trouvée tels que la fiabilité, la tolérance aux pannes ou encore l'évitement de la congestion par l'équilibrage de charge efficace. Ainsi, des auteurs proposent un RPL optimisé appelé ORPL qui diminue la latence de routage en utilisant une approche multipath. Ils utilisent la métrique du cycle de service attendu (EDC), qui est revendiquée comme l'équivalent multi chemin de ETX, il utilise également un minuteur Trickle pour diffuser les mises à jour de routage, l'inconvénient de ce protocole et qu'il produit une surcharge significative de trafic de contrôle.

4. Optimisation de Trickle Timer

Trickle timer qui est une sorte de minuterie visant à propager les messages de contrôle tout en essayant de les réduire est l'un des composants phare du protocole RPL. L'une des catégories d'approches pour optimiser RPL s'intéresse justement à Tricke timer. En effet, alors que la RFC 6206 qui décrit le principe de Trickle et son fonctionnement avertit les chercheurs/programmeurs sur la faible probabilité de d'améliorer Trickle, de nombreux travaux d'optimisation de RPL se sont intéressés à cet algorithme. Parmi ces travaux on peut citer Etricke pour Enhanced-Trickle où l'on proposent un nouvel algorithme appelé E-Trickle qui n'a pas de période d'écoute. Au lieu de réinitialiser c, le compteur de cohérence, au début de l'intervalle, il réinitialise c à un moment choisi de manière aléatoire pour éliminer l'effet cumulatif du problème d'écoute courte. Des auteurs ont également proposé une version optimisée de Trickle (appelée opt-Trickle) qui, lorsqu'un nouvel intervalle commence, choisit les valeurs de t en fonction de l'état actuel. Si l'intervalle est réinitialisé, il choisit t de 0 à Imin, et s'il a été configuré ou démarré à partir d'un intervalle expiré, il choisit t de la moitié de l'intervalle à l'intervalle entier [I/2, I].

Conclusion

RPL est un protocole de routage développé par le groupe de travail ROLL pour répondre aux contraintes très spécifiques des réseaux LLN. Le protocole a été conçu pour être très flexible aux différentes variations des ressources du réseau. Sa fonction de construire des routes s'appuie sur la notion de DODAG. Chaque nœud calcule son rang et choisit des parents qui minimisent le coût sur la route vers la racine. Les coûts sont calculés selon une ou plusieurs

métriques, le choix de ces métriques dépend de l'application et de ces objectifs/contraintes. Le RPL original tel que défini dans la RFC 6550 ne peut pas répondre à tous les besoins spécifiques des applications. RPL doit donc être optimisé afin d'atteindre certains objectifs particuliers. Le protocole RPL est sensible à un large éventail d'attaques internes et externes. Ces attaques sont difficiles à détecter et à atténuer en raison de la nature vulnérable des nœuds et du réseau sans fil, de la nature facilement falsifiable des nœuds, de la mobilité des nœuds et des contraintes de ressources. Dans le prochain chapitre nous allons détailler les différentes attaques contre le protocole RPL.

CHAPITRE 3 : LES ATTAQUES CONTRE LE RESEAU RPL ET LES MECANISMES DE SECURITE

I. LES ATTAQUES CONTRE LE RESEAU RPL

Introduction

Comme nous l'avons dit précédemment le protocole RPL est sensible à un large éventail d'attaques internes et externes. Ces attaques sont difficiles à détecter et à atténuer en raison de la nature vulnérable des nœuds et du réseau sans fil, de la nature facilement falsifiable des nœuds, de la mobilité des nœuds et des contraintes de ressources. De nombreux auteurs ont proposé divers mécanismes de sécurité spécifiques à RPL, qui incluent le chiffrement des messages de contrôle et les modes de sécurité. Cependant, la plupart des implémentations RPL ne prennent pas en compte les mesures de sécurité en raison d'une spécification incomplète des mécanismes et des frais généraux d'implémentation. Ces mécanismes de sécurité sont efficaces pour se défendre contre les attaques extérieures. Cependant, ils échouent en cas d'attaques internes. Un attaquant interne peut contourner les mécanismes de sécurité RPL appliqués et perturber la fonctionnalité du réseau. Les attaques contre le réseau RPL peuvent être catégorisées en trois catégories selon leur cible : les attaques basées sur les ressources du réseau, les attaques basées sur la topologie du réseau et les attaques basées sur le trafic :

1. **Les attaques basées sur les ressources**

   Ces genres d'attaques sont de deux types :
   - les attaques directes
   - les attaques indirectes

Les attaques directes :

Hello Flooding (DIO Flooding) :

Hello Flooding attack est une attaque où un nœud attaquant envoie des messages hello périodiquement aux nœuds voisins pour perturber le réseau.

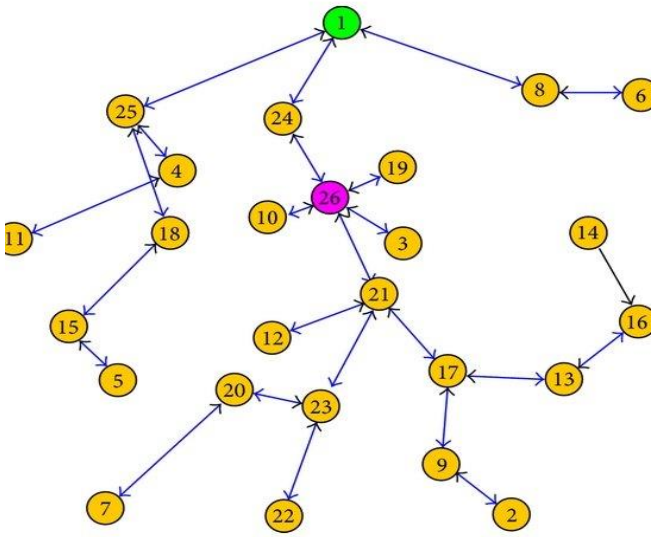


Figure III.1 : Illustration de l'attaque Hello flooding [9]

Les attaques indirectes :

Increase Rank Attack :

C'est lorsque le nœud attaquant change son rang pour un rang supérieur dans le but d'être plus loin de la racine

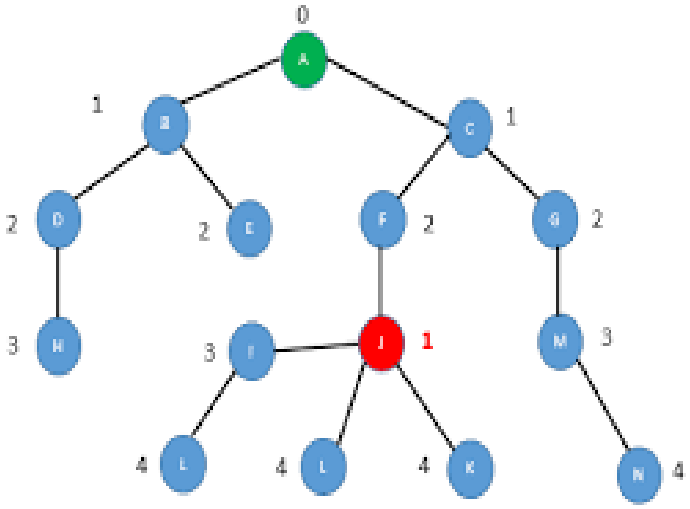


Figure III.2: Illustration de l'attaque Increase Rank Attack [9]

Decrease Rank Attack:

C’est lorsque le nœud attaquant change son rang pour un rang inferieur dans le but d’être plus proche de la racine.

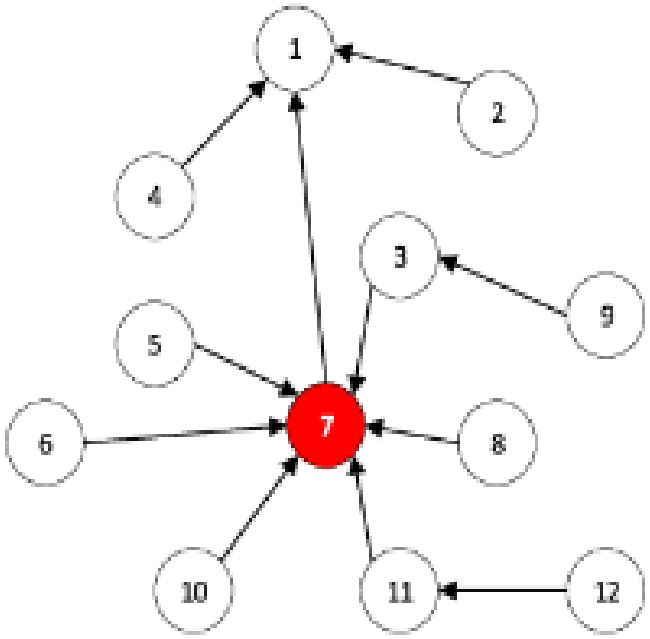


Figure III.3 : Illustration de l’attaque Decrease Rank Attack [10]

Version Number Attack :

Dans cette attaque, l’attaquant modifie le champ numéro de version du message DIO et le transmet aux voisins. Cela conduit à la reconstruction inutile du DODAG complet, ce qui provoque une augmentation de la surcharge des paquets de contrôle, du délai de bout en bout, de la consommation d’énergie, etc.

ETX Manipulation :

Un attaquant exploite la règle empirique du routage optimale (qui dit que la valeur ETX de tout nœud parent doit être inferieure a la valeur ETX d’un nœud enfant sur l’ensemble du réseau) en manipulant délibérément la valeur ETX des nœuds afin de gagner une meilleure position dans le réseau. Cela permet à l’attaquant d’attirer une grande partie du trafic puis lancer des attaques comme le BlackHole et GrayHole.

Local Repair Attack :

La réparation locale qui ne doit être appelé que lorsque le nœud n'a aucun lien avec son parent, l'attaque consiste à déclencher grâce à une des deux méthodes possible la réparation locale a un nœud toujours connecté à son parent. Cela entraine une augmentation de la consommation d'énergie de la victime et une perturbation du processus de routage.

2. Les attaques basées sur la topologie

Ces genres d'attaques qui sont de types :

Les attaques de sous-optimisations :

SinkHole Attack

Il s'agit d'une attaque où le nœud compromis tente d'attirer le trafic réseau en se faisant passer pour un nœud légitime dans le processus de routage. Elle bloque la station de base dans l'obtention des informations légitimes, provoque une menace et ouvre la voie à d'autres attaques aussi. Le nœud compromis essaie de supprimer les paquets.

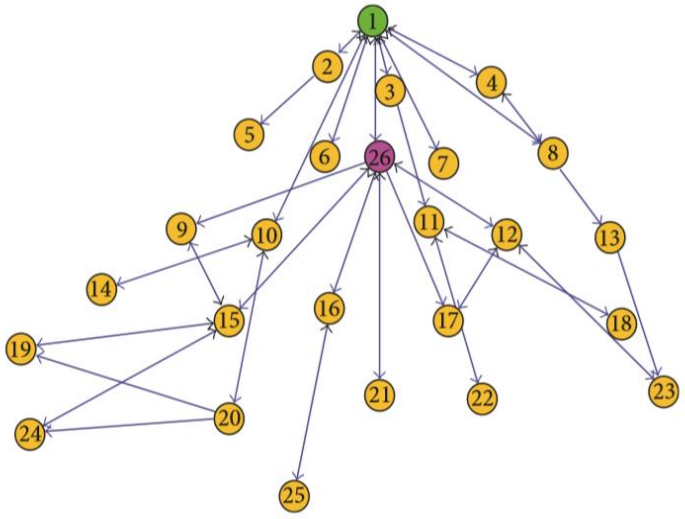


Figure III.4 : Illustration de l'attaque SinkHole Attack [9]

WormHole

L'attaque par trou de ver est une attaque où deux nœuds attaquants complices ou plus sont connectés avec un lien appelé lien de trou de ver et les nœuds forment un tunnel pour diffuser les paquets de données dans le réseau. Cela rend le réseau confus et perturbe le processus de communication.

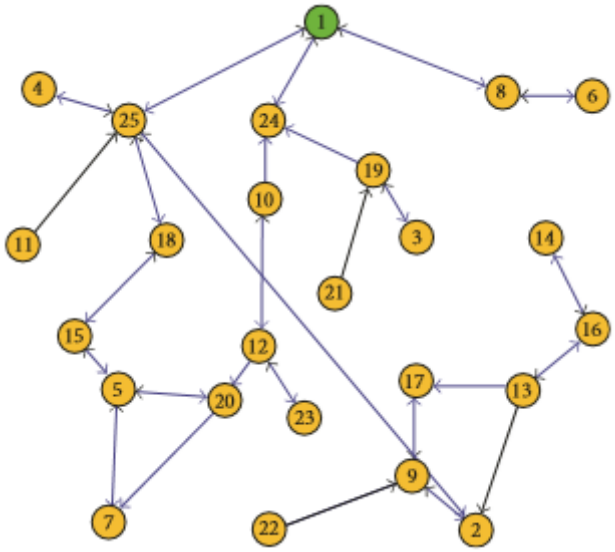


Figure III.5 : Illustration de l'attaque WormHole Attack [9]

Worst Parent

C'est une attaque contre le RPL dans laquelle un nœud malveillant choisit intentionnellement un chemin sous-optimal vers le nœud racine pour transmettre ses paquets de données. Il en résulte des performances sous-optimisées et une mauvaise utilisation des ressources du réseau.

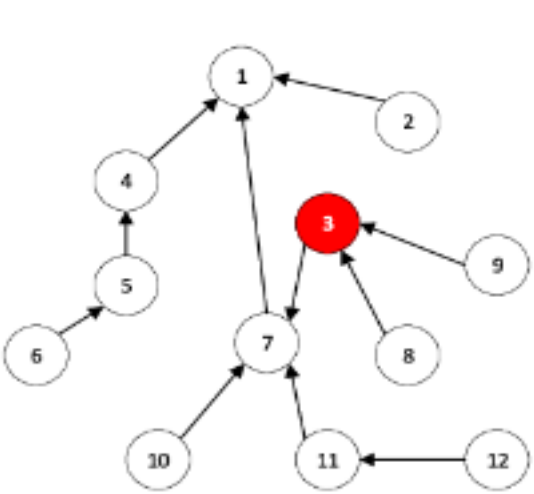


Figure III.6 : Illustration de l'attaque Worst Parent Attack [10]

Replay Attack :

Dans ce cas le nœud attaquant duplique et multi diffuse tous les messages DIO reçu de son parent, les voisins qui reçoivent les DIO rejoués vont penser que le message est reçu d'un nouveau voisin et si les informations de routages sont favorables les voisins victimes peuvent l'ajouter comme parent préféré. Ce type d'attaque possède une variante appelée DIO replay attack.

DIO Replay Attack :

Dans cette variante le nœud compromis multi diffuse des messages DIO obsolètes contenant des anciennes informations de routage ce qui force les victimes à suivre des chemins obsolètes et non optimisés.

Routing Table Falsification :

Le but de cette attaque est de créer une topologie non optimisée en raison de l'augmentation des paquets de bout en bout, cela entraine le retard et la diminution du taux de livraison des paquets (PDR). Elle consiste à ce que l'attaquant falsifie les informations de routage contenues dans les messages DAO, ce qui force les nœuds légitimes à construire des fausses routes descendantes (routes vers fils inexistantes). Ainsi cela conduit à une surcharge lorsque les nœuds tentent de transmettre des données à des nœuds inexistants.

DIO Suppression :

L'objectif de cette attaque est de supprimer la transmission de nouveaux messages DIO requis par les nœuds IoT pour explorer de nouveaux chemins de routages et supprimer les obsolètes. Elle permet alors de créer des chemins non optimises qui conduit a un problème de partition dans le réseau. Elle consiste à recevoir une DIO légitime et le multi diffuser périodiquement autant de fois que nécessaire jusqu'au seuil de suppression, cela fait croire aux nœuds victimes que les DIO cohérents sont reçus de son nœud parent sans changement légitime de l'état du réseau, ainsi il n'y aura aucun changement aussi au niveau du nœud victime donc pas d'amélioration de routage.

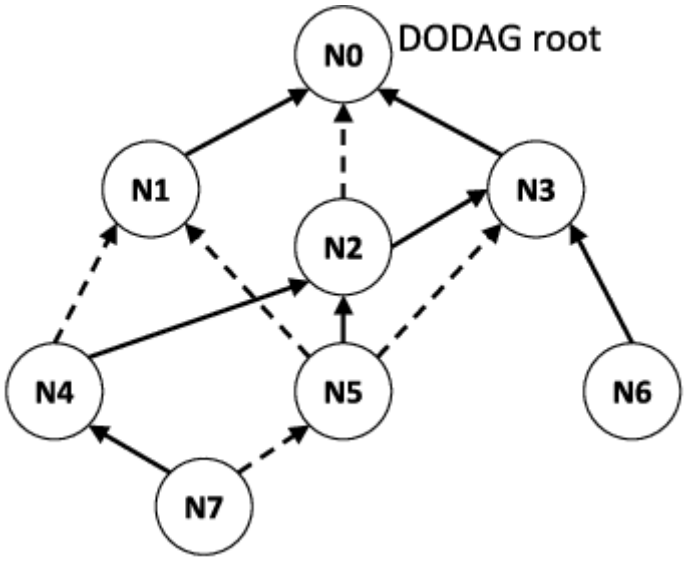


Figure III.7 : Illustration de l'attaque DIO Suppression [11]

Les attaques d'isolements :

Black-Hole Attack :

Dans cette attaque le nœud attaquant prétend qu'il a le chemin le plus court vers la destination après avoir illégalement changé son rang. Il abandonne les paquets de routage reçu de ses victimes et ne propage pas les paquets au point précis de destination.

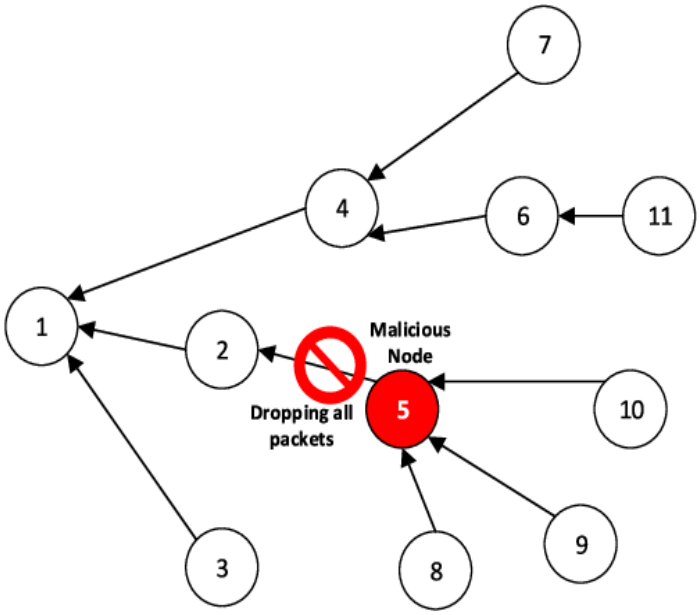


Figure III.8 : Illustration de l'attaque Black Hole [10]

DODAG Inconsistency :

L'attaquant exploite les drapeaux RPL (mécanisme qui permet de reconnaitre les incohérences dans le réseau) pour effectuer diverses attaques qui ensemble sont qualifiées de DODAG Inconsistency (comme par exemple le BlackHole et le Forced BlackHole).

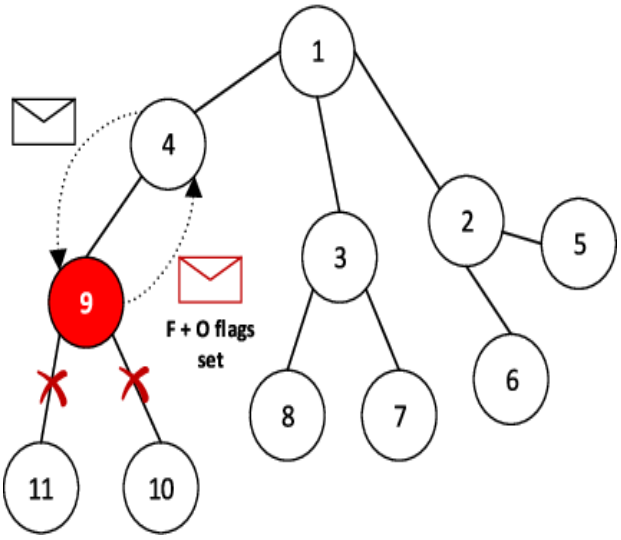


Figure III.9 : Illustration de l'attaque DODAG Inconstancy [10]

Gray-Hole Attack :

Elle suit les mêmes principes que le Black-Hole Attack cependant elle abandonne une partie des paquets et non la totalité et fait parvenir le reste a la destination.

3. Les attaques basées sur le trafic

Ici également ces types d'attaques sont de deux types :

Les attaques d'écoute clandestine :

Sniffing Attack :

Cette attaque consiste à écouter les paquets transmis sur le réseau à l'aide d'un nœud compromis ou par capture direct des paquets sur le support de partage dans le cas des réseaux sans fil.

Traffic Analysis :

Cette attaque consiste a obtenir les informations sur le routage en utilisant les caractéristiques et les modèles de trafics sur un lien. Même principe que le Sniffing pour collecter des informations.

Les attaques d'imitations :

Clone ID :

C'est lorsqu'un nœud malveillant prétend être un nœud existant légitime. Après avoir reniflé les informations du trafic réseau et identifié la racine (root), il usurpe son adresse et prend le contrôle du DODAG

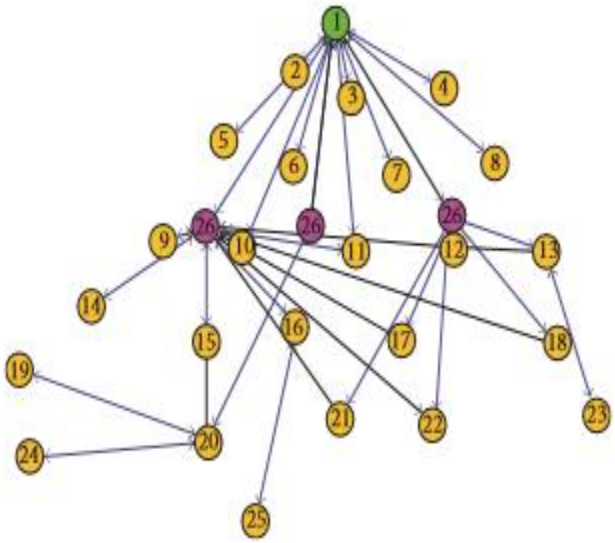


Figure III.10 : Illustration de l'attaque Clone ID [9]

Sybil :

Sybil est une attaque où un nœud malveillant crée plusieurs fausses identités en même temps dans le réseau. Cela empêche les paquets d'un nœud d'atteindre la destination

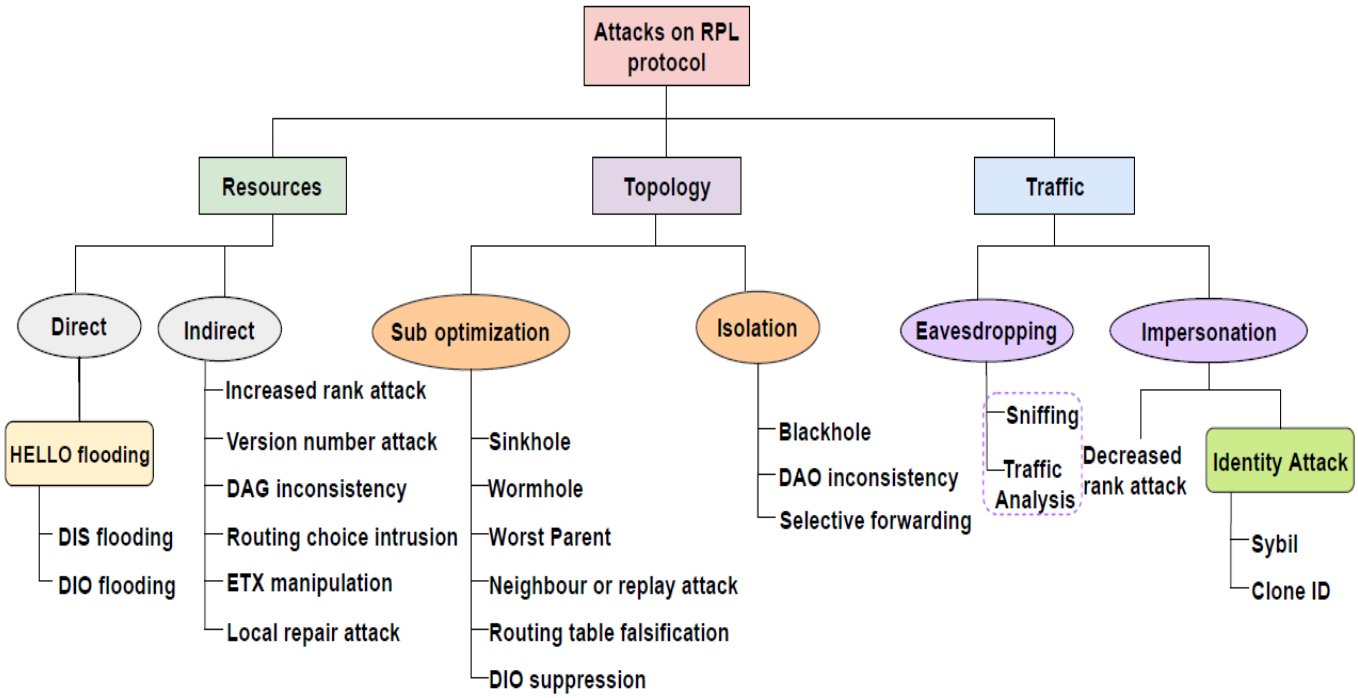


Figure III.11 : Repartition des differentes attaques sur le protocole RPL [12]

II. LES MECANISMES DE DEFENSE DU RESEAU RPL

Introduction

Bien que notre travail ne porte pas sur les mécanismes de défense contre le réseau RPL nous allons essayer d'aborder un certain nombre de ces derniers pour avoir une petite idée de comment le réseau RPL peut-il se défendre. Vu la structure du réseau RPL et de ses caractéristiques tels que la contrainte de ressources, la sécurité physique limitée, la topologie

dynamique et ses liens peu fiables le rende particulièrement vulnérable et difficile à protéger contre les attaques.

Cependant différentes solutions ont été proposées pour la détection et l'atténuation des attaques RPL qui peuvent être réparties en deux catégories à savoir les solutions basées sur le protocole sécurisé et les solutions basées sur le système de détection d'intrusion (IDS).

I. Solutions basées sur le protocole sécurisé

Ces solutions font référence à des mécanismes de défense incorporée dans le protocole RPL lui-même, le sécurisant ainsi contre diverses attaques.

Ces mécanismes sont en outre classés en solutions basées sur la cryptographie, la confiance et le seuil. Les mécanismes de cryptographie utilisent des méthodes de cryptographie traditionnelles pour assurer la sécurité et la défense contre diverses attaques, tandis que les mécanismes basés sur la confiance impliquent le calcul de la fiabilité des nœuds pour faciliter les décisions de routage. Les solutions de défense basées sur des seuils exploitent la fonctionnalité intégrée de RPL et fournissent une amélioration afin de décider de la manière dont la minuterie d'entretien est réinitialisée. Ces mécanismes sont intégrés au protocole RPL, ce qui le rend plus robuste en termes de comportement défensif tout en maintenant des performances réseau souhaitables.

II. Les solutions basées sur le système de détection d'intrusion

Les solutions IDS traditionnelles ne peuvent pas être directement appliquées à l'IoT [90]. C'est en raison des nœuds limités en ressources utilisés dans le réseau, des différentes topologies de réseau et de la connectivité basée sur IP, qui rendent les solutions IDS traditionnelles irréalisables. Cela exige des solutions IDS légères en termes de surcharge de calcul, de communication, de mémoire et d'énergie. En particulier au protocole RPL, IDS fait référence à la deuxième ligne de défense, qui est responsable de la détection des anomalies dans le fonctionnement RPL. Ces solutions de défense peuvent être classées en Signature, Anomalie, Spécification et Hybride.

CONCUSION

Dans ce chapitre nous avons vu les différentes attaques contre le protocole RPL, comment elles agissent et dans quelle catégorie elles étaient à savoir soit une attaque qui agit sur la

topologie soit sur les ressources ou soit sur le trafic, et également nous avons introduit un peu la sécurité comment sans prémunir avec les IDS etc.

En raison des milliards de dispositifs interconnectés en réseau, leur sécurisation et leur protection contre diverses attaques et menaces posent un défi critique. Par conséquent, il est très important de fournir des solutions légères de surveillance des performances et de la sécurité pour protéger les réseaux basés sur RPL.

Dans le prochain chapitre nous allons étudier plus en détails quelques attaques faire leur implémentation et comparer leurs impacts sur les ressources des réseaux RPL.

Chapitre 4 : Etudes des impacts de quelques attaques Iot sur le réseau RPL

Introduction

La plupart des attaques IoT ont pour objectif de rendre difonctionnel le réseau, d'autres d'espionner celui-ci. Dans la plupart des cas celles-ci ont une influence sur les métriques des nœuds du réseau RPL.

Dans ce chapitre qui est le cœur de notre travail nous allons analyser et expliquer les conséquences de quelques attaques IoT sur les métriques des nœuds d'un réseau RPL. Pour cela il nous faut simuler ces attaques qui sont au nombre de 4 après leur implémentation grâce aux outils suivants : VMwrare player, Contiki OS et Cooja.

I. Outils d'implémentations

1. VMware Player :

Il s'agit d'une application propriétaire mise à disposition gratuitement aux utilisateurs pour un usage non professionnel, sous Windows ou Linux fourni par VMware, Inc., une société qui était auparavant une division et dont l'actionnaire majoritaire reste Dell EMC. Elle permet de créer vos propres machines virtuelles, afin d'y installer vos propres systèmes d'exploitation invités et de les faire fonctionner à travers votre système d'exploitation hôte. VMware Workstation Player nécessite un système d'exploitation hôte 64 bits. [13]

Figure IV.1 : Icone de l'application VMWare Player

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. [8]

Contiki est simple, open source, implémente la pile protocolaire et une librairie complète du protocole RPL (contikiRPL), et il est programmé en langage c.

Contiki propose un simulateur de réseau appelé **Cooja**.

3. Cooja :

Ce simulateur permet l'émulation de différents capteurs sur lesquels seront chargés un système d'exploitation et des applications. **Cooja** permet aussi de simuler les connexions réseaux et d'interagir avec les capteurs.

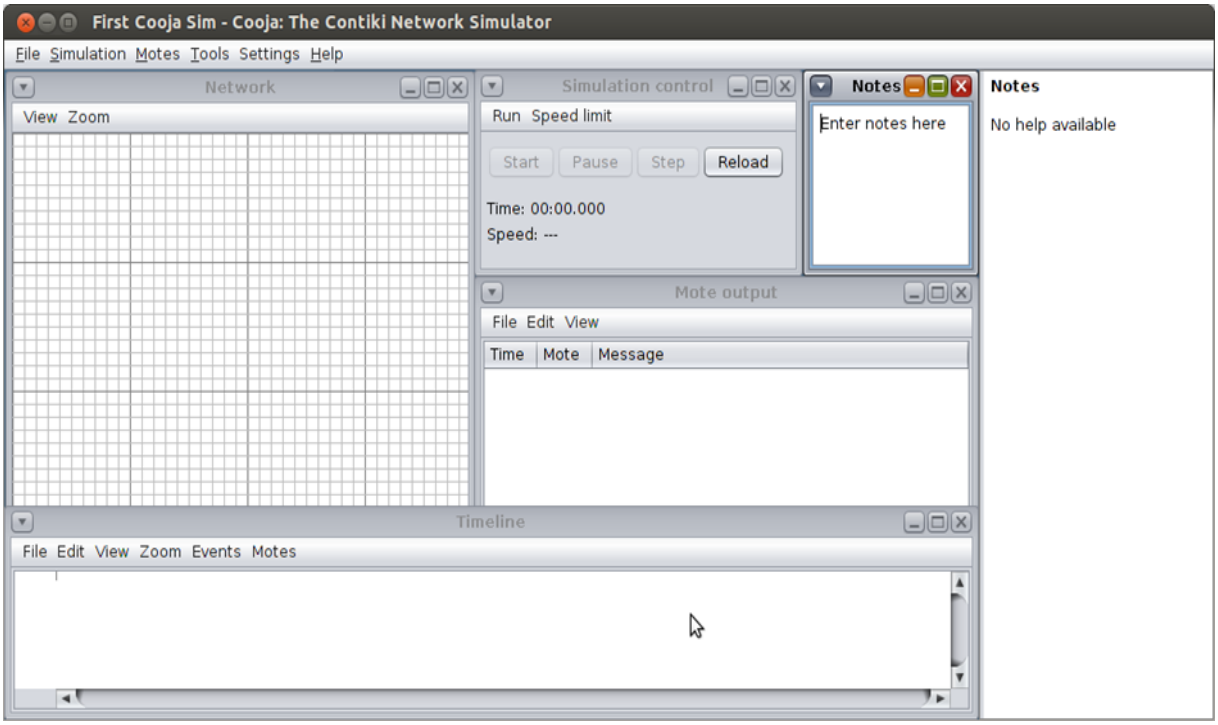


Figure IV.2 : Interface de Simulation Cooja

II. Les différentes métriques d'un nœud en RPL

Les métriques sont des paramètres de test du protocole de routage qui permettent de mesurer les performances de celui-ci. Dans notre étude, nous avons pris en compte les métriques suivantes :

- **Taux de réussite (PDR)** : représente le rapport entre le nombre de paquets de données livrées à la racine et le nombre de paquets envoyés par les différents nœuds du DODAG :

$$PDR = \Sigma\, Messages\ reçus\ par\ la\ racine\ /\ \Sigma Messages\ envoyés\ par\ les\ noeuds\ du\ DODAG$$

- **Taux de perte** : représente le rapport entre le nombre de paquets de données perdus et la somme de paquets livrés et le nombre de paquets perdus :

$$Taux\ de\ Perte = Nombre\ de\ paquets\ perdus\ /\ Nombre\ de\ paquets\ émis$$

- **Energie** : représente l'énergie consommée par l'ensemble des nœuds du réseau.
  RADIO ON : consommation d'énergie au niveau du nœud.
  RADIO TX : consommation d'énergie du nœud a la transmission.
  RADIO RX : consommation d'énergie du nœud a la réception.
  Ces valeurs sont le plus souvent en pourcentage

III. Implémentation et Etudes

Nous avons choisi pour cette étude 4 attaques qui sont les suivantes :

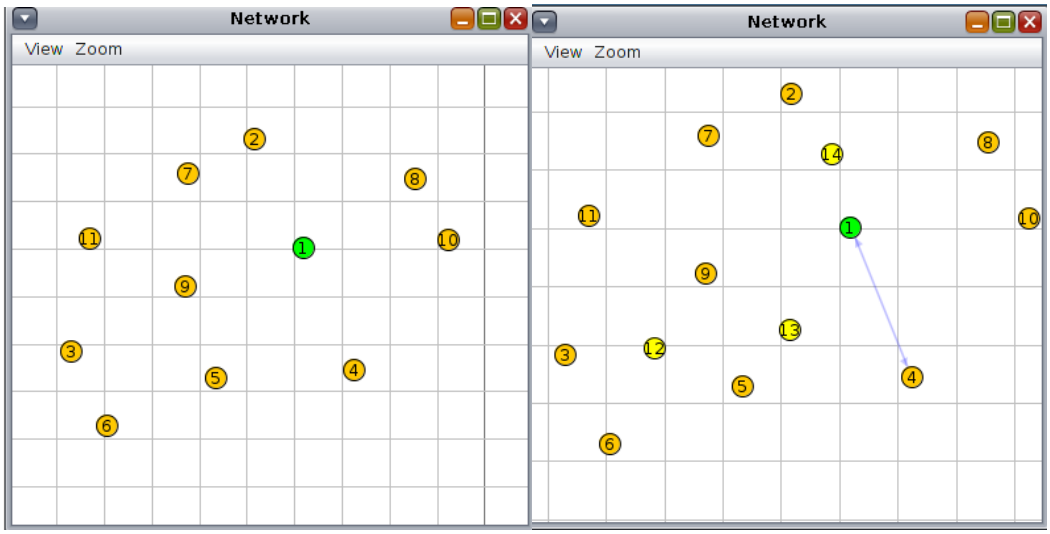
1. DIS Flooding

Il s'agit d'une attaque où un nœud attaquant envoie des messages DIS périodiquement aux nœuds voisins pour perturber le réseau.

Pour simuler cela il faut créer 1 nœud serveur qui est représenté en vert dans les figures a et b et 10 nœuds clients représentés en orange puis lancer la première simulation.

Ensuite nous avons ajouté 3 nœuds malveillants(jaunes) qu'on constate dans la figure b qui sont 12, 13, 14 puis lancer également la seconde simulation.

Nous allons analyser et interpréter les conséquences de cette attaque après simulation d'une durée de 15 minutes.



a) Topologie normale b) Topologie y compris les nœuds malveillants

Figure IV.2 : Construction de la simulation pour l'attaque DIS Flooding.

Pour l'analyse de cette attaque après les 15 minutes de simulation nous avons récupéré les deux métriques qui sont le PDR et la consommation en énergie représentés dans la Figure IV.3

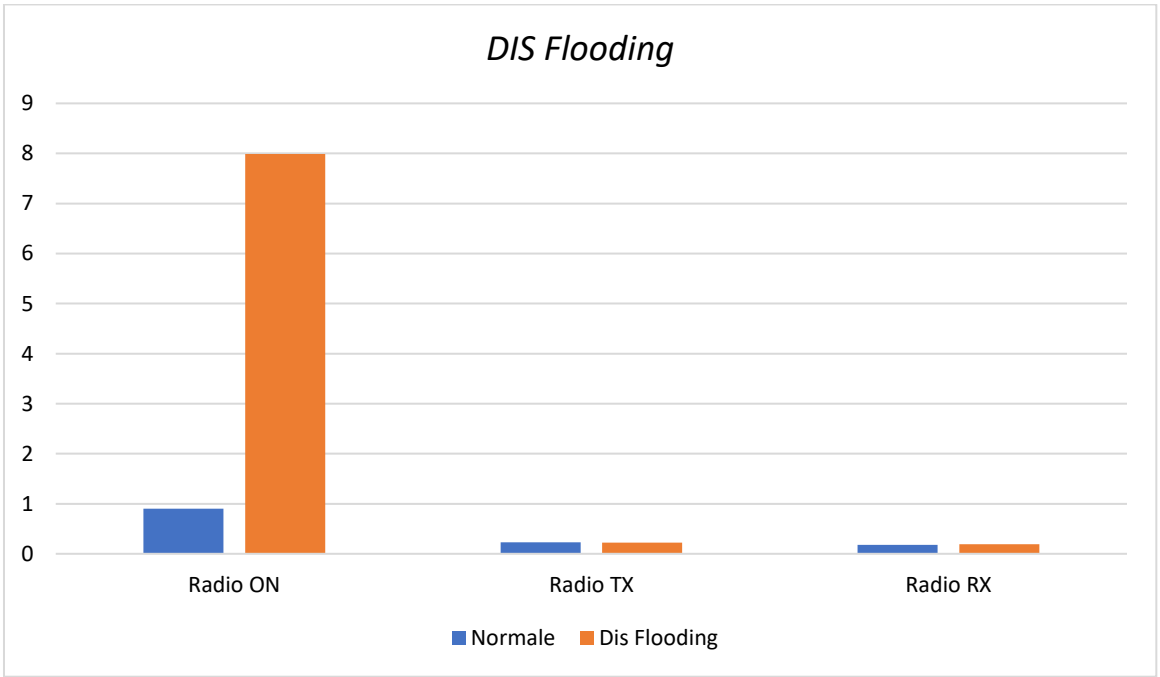


Figure IV.3 : Graphe de comparaison de la consommation d'énergie pendant le DIS Flooding

En revanche à travers le graphe ci-dessus qui représentent la consommation d'énergie des deux cas nous constatons qu'il y'a une variation d'énergie entre les deux. L'attaque DIS Flooding agit énormément sur l'énergie, cela est due à la multiplication des transferts des messages de contrôles engendrés par les nœuds malveillants. Et également nous constatons une variation dans le PDR qui est de 0.72 donc à été affecté par cette attaque comme nous le montre l'image ci-dessous :

```
Script timed out
Performance Calculation
Generated Packets 208 | ReceivedPackets 150
TL = 66774711 |  AE2ED = 0.44530669 |  PDR = 0.7211538461538461
```

Due aux métriques visées et épargnées par cette attaque, nous pouvons en conclure que DIS Flooding est une attaque de type ressources

2. BlackHole Attack

Dans cette attaque le nœud attaquant prétend qu'il a le chemin le plus court vers la destination après avoir illégalement changé son rang. Il abandonne les paquets de routage reçu de ses victimes et ne propage pas les paquets au point précis de destination.

Nous allons analyser et interpréter les conséquences de cette attaque après simulation d'une durée de 15 minutes aussi.

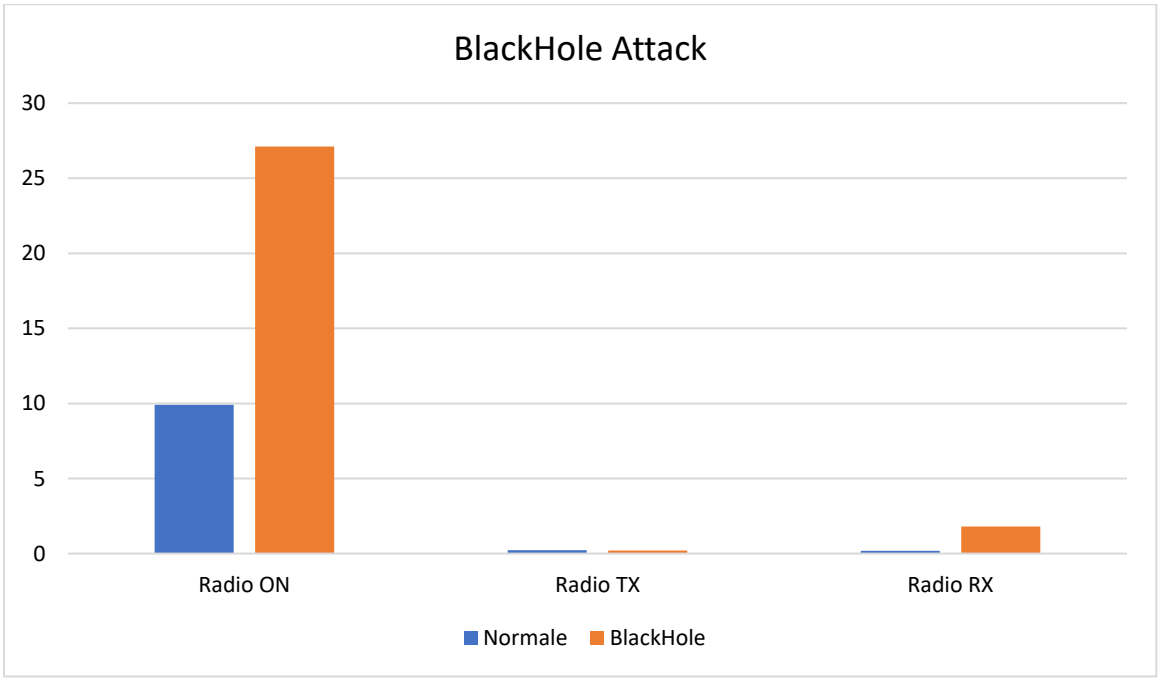


Figure IV.4 : Graphe de comparaison de la consommation d'énergie pendant le BlackHole

Pour l'analyse de cette simulation avec le Blackhole nous avons constaté qu'au niveau de la consommation d'énergie dans le graphe ci-dessus, que la simulation avec le Blackhole a consommée beaucoup plus d'énergie que dans la simulation normale. Et qu'au niveau du PDR nous observons un grand changement est à ce niveau. En effet on est passé d'un PDR avoisinant les 100% à un PDR a peine à 33% comme nous le montre l'image ci-dessous.

```
Script timed out
Performance Calculation
Generated Packets 209 | ReceivedPackets 69
TL = 6400716 |  AE2ED = 0.092764 |  PDR = 0.33014354066985646
```

Conclusion : Cette attaque comme de par son objectif impacte énormément le transfert des paquets dans les réseaux RPL, elle donc très nuisible et dangereuse pour les réseaux RPL de par son impact considérable.

Ainsi nous pouvons déduire à partir de notre analyse que l'attaque du Blackhole est du type topologie.

3. GrayHole Attack

Celle-ci suit les mêmes principes que le Black-Hole Attack étudié ci-dessus cependant elle abandonne une partie des paquets et non la totalité et fait parvenir le reste a la destination.

Nous allons utiliser la même simulation utilisé ci-dessus en remplaçant au niveau de l'implémentation des nœuds leur objectif, c'est-à-dire transmettre un certain nombre de paquet et supprimer le reste (voir Figure IV.2)

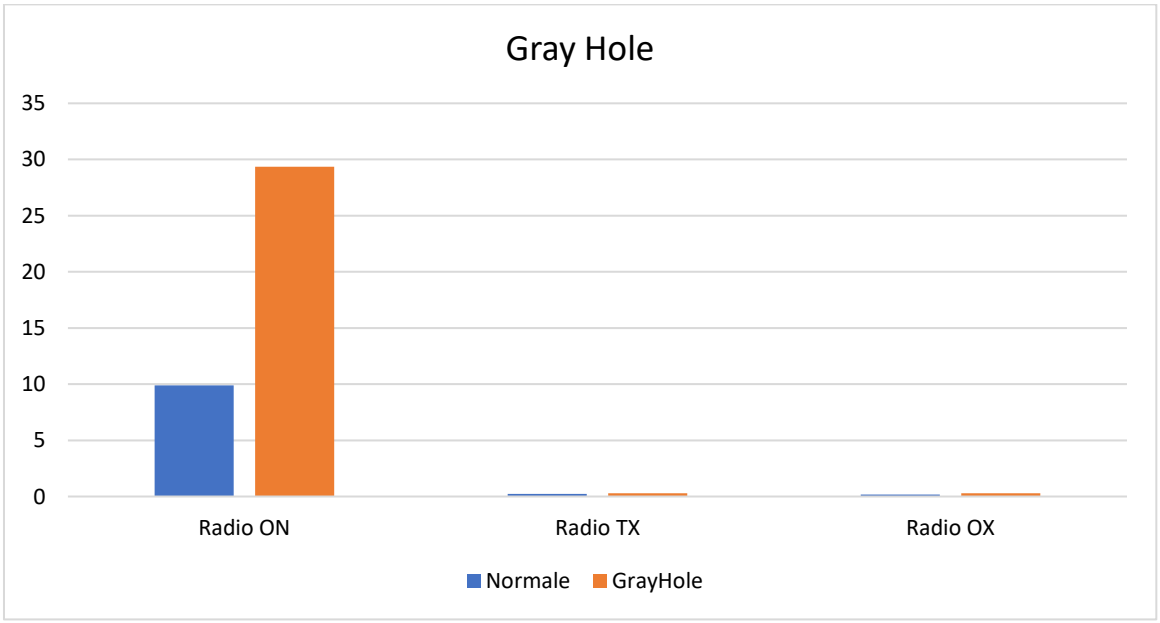


Figure IV.5 : Graphe de comparaison de la consommation d'énergie pendant le GrayHole

Pour l'analyse de cette simulation, pour ce qui concerne la consommation d'énergie on constate que la simulation avec le GrayHole à consommer plus d'énergie que pendant la simulation normale comme nous montre le graphe ci-dessus et que pour ce qui concerne le PDR on observe un grand changement à ce niveau. En effet on est passé d'un PDR avoisinant les 100% à un PDR a peine à 74% comme nous le montre l'image ci-dessous.

```
Script timed out
Performance Calculation
Generated Packets 290 | ReceivedPackets 217
TL = 23138245 |  AE2ED = 0.10662785714285715 |  PDR = 0.7482758620689656
```

En conclusion nous pouvons qu'une attaque du GrayHole sur un réseau agit sur son PDR et sur d'énergie, donc nous pouvons déduire que le GrayHole est du type topologie également tout comme le BlackHole mais en faisant la comparaison des PDR des deux attaques on voit que le BlackHole a un plus grand impact et donc plus dangereuse que le Grayhole.

4. DIO Suppress

L'attaque du Dio suppress est une attaque qui supprime la transmission de nouveaux messages DIO requis par les nœuds IoT pour explorer de nouveaux chemins de routages et supprimer les obsolètes. Elle permet alors de créer des chemins non optimises qui conduit à un problème de partition dans le réseau.

Nous allons également faire une simulation de 15 minutes avec et sans les nœuds malveillants afin de faire l'analyse du PDR et de l'énergie.

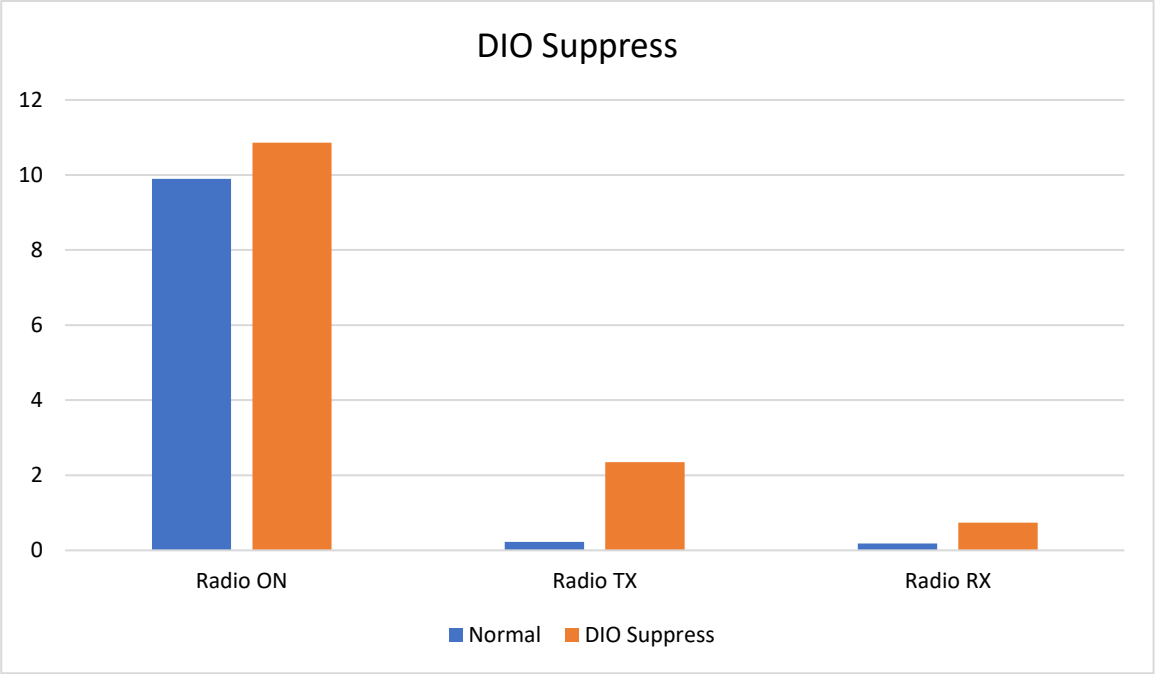


Figure IV.6 : Graphe de comparaison de la consommation d'énergie pendant le DIO Suppress

Pour l'analyse de cette simulation nous constatons que la consommation de l'énergie est plus importante au niveau de la simulation avec l'attaque DIO que sans l'attaque comme nous pouvons le voir dans le graphe ci-dessus, en ce qui concerne le PDR nous constatons qu'il Ya également une chute de ce dernier comme nous le montre l'image ci-dessous.

```
Script timed out
Performance Calculation
Generated Packets 209 | ReceivedPackets 150
TL = 66774711 |  AE2ED = 0.44516474 |  PDR = 0.7177033492822966
```

En conclusion nous pouvons dire que l'attaque du DIO suppress a un impact tant sur l'énergie que sur le PDR. Elle agit comme les deux dernières attaques ci-dessus mais on constate que le BlackHole reste toujours la plus dangereuse. A partir de là nous pouvons déduire qu'elle est une attaque de type topologie.

Figure IV.1 : Tableau récapitulatif des attaques

Liste des Attaques	Description	Impacts sur le réseau
DIS Flooding	Les nœuds légitime sont inondés de messages DIS	Augmente la surcharge des paquets de contrôle et la consommation d'énergie et perturbe le routage
BlackHole Attack	Le nœud malveillant abandonne tous les paquets qu'il reçoit de ses nœuds fils	Diminue énormément le PDR et déstabilise la topologie
GrayHole Attack	Le nœud malveillant supprime une partie des paquets qu'il reçoit de ses nœuds fils et fait parvenir le reste à la racine	Diminue aussi le PDR et affecte négativement la topologie
DIO Suppress	Les messages DIO précédemment reçu sont envoyés aux nœuds voisins jusqu'à la suppression de la nouvelle transmission DIO	Introduit des chemins de routage non-optimisés ce qui conduit à la partition du réseau

Conclusion

Dans ce chapitre nous avons fait la simulation de 4 attaques et analyser deux métriques à savoir le PDR et la consommation d'énergie. Nous avons abouti à la conclusion que de ces quatre attaques à savoir le Blackhole, le DIS Flooding, le Grayhole, et le Dio Suppress sont pour les trois première de types topologie à cause de leur impact sur le PDR et sur la consommation d'énergie et que le Dio Suppress elle était une attaque de types ressources du fait qu'elle consomme l'énergie et sur le PDR. Retenons également que toutes ces attaques déstabilisent le réseau. A la fin nous avons un tableau qui fait le récapitulatif des attaques et leur impact sur le réseau.

Conclusion générale

L'internet des objets (IoT) est un réseau d'une multitude d'appareils parmi lesquels les capteurs, les appareils mobiles etc. qui peuvent se connecter à Internet. Les LLN, réseau à faible puissance et avec perte sont un autre genre de réseaux sans fils et filaires dans lequel les objets fonctionnent le plus souvent avec des contraintes de puissance de traitement, de mémoire et de batterie. Effectivement RPL a été conçu comme un protocole de routage efficace et évolutifs pour les LLN. En effet le manque de ressources de ces types de réseaux les rend particulièrement vulnérables aux menaces de sécurité tant externe qu'interne qui compromettent le réseau c'est pour cela que des mécanismes de protections existe comme les IDS afin de prévenir de ces menaces. Cependant avec tous les systèmes mis en place pour prévenir ces menaces on trouve toujours des nœuds interne qui peuvent être compromis et agirent de manière spécifique sur le réseau afin de le perturbé.

Par conséquent dans ce mémoire, nous présentons quelques types d'attaques, parmi une quinzaine d'attaques décrites, qui agissent sur le réseau RPL à savoir le dis Flooding, le Blackhole, le GrayHole et le Dio Suppress. Nous avons analysé l'impact de ces quatre attaques sur deux métriques du réseau RPL à savoir le PDR et la consommation d'énergie et nous avons constaté que chaque attaque déstabilisait le routage soit en agissant sur les ressources c'est-à-dire l'énergie dans notre cas c'est le dis Flooding et d'autre agissant sur le PDR provoquant au passage la perturbation de la topologie. Pour pouvoir faire l'implémentation de ces dernières nous avons eu recours au simulateur COOJA sous Contiki OS. Nous avons lancer des simulations de 15 minutes pour chacune des attaques et d'autres encore de 15 minutes sans les attaques pour justement a travers les deux métriques faire l'analyse et déduire leur impact sur les ressources d'un réseau RPL.

Le travail que nous avons effectué, nous a permis de découvrir le domaine de l'internet des objets et d'acquérir une vaste connaissance non seulement sur les réseaux a faibles puissances et avec perte mais aussi sur le protocole de routage des LLN et également d'avoir pu appris à programmer dans l'environnement de Contiki et à simuler sur les réseaux LLN sous le simulateur Cooja. Nous espérons plus tard à avoir l'occasion d'être sur un travail qui sera de trouver des méthodes plus avancées pour défendre les réseaux à faibles puissance et avec pertes contre les attaques tant externe mais aussi interne.

Références bibliographiques

[1] Ashton, K. That ‘internet of things’ thing. RFID journal, (2009), 22(7), P. 97-114.

[2] Mayzaud, A., Badonnel, R, & Chrisment, I. (2016, October). Detecting version number attacks in RPL-based networks using a distributed monotoring architecture. In 2016 12th International Conference oon Network ans Service Management (CNSM) P. 127-135.

[3] https://fr.statista.com/statistiques/584662/taille-du-marche-de-l-internet-des-objets-dans-le-monde-2009-2019/ , visité le aout 2015.

[4] Abdoul Fatas Bamogo and Pasteur Poda, Optimizing RPL Routing By A Multi-Metric Combination, EasyChair Preprint, 2020, № 4759, P 1-11.

[5] Mahamat-Saleh and Abdoulaye Ali, Estimation de la Qualité de Lien dans RPL, [mémoire de master], Algerie, Université ABDELHAMID IBN BADIS 6 MONTAGANEM, Faculté des sciences Exactes et d’informatiques, 2021

[6] RPL : IPv6 Routing Protocol for Low Power and Lossy Networks, Seminar SN SS2011, Network Architectures and Services, July 2011

[7] Patrick Olivier KAMGUEU, Configuration Dynamique et Routage pour l’Internet des Objets, [thes en cotutelle], France Cameroun, Université de Lorraine Université de Yaoundé 1, 2017

[8] Ihsane Djabrouhou and Ikram Boursas, Mitigation de l’attaque de numéro de version contre les réseaux IoT basés sur le protocole de routage RPL, [mémoire de master], Algérie, Université Saad Dahlab Blida 1, Faculté des sciences, 2021.

[9] Linus Wallfren, Shahid Raza, Thiemo Voigt. Routing Attacks and Countermeasures in the RPL-Based Internet of Things, 5 june 2013.

[10] Ahmed Raoof, A. Matrawy, Chung Horng Lung. Routing Attacks and Mitigation Methods for RPL-Based Internet of Things, 2019.

[11] Pericle Perazzo, C. Vallati, G. Dini. DIO Suppression Attack Against Routing in the Internet of Things, 11 August 2017.

[12] Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review, 2020.

[13] https://doc.ubuntu-fr.org/vmware_player, visité le 10/02/2022.