

UNIVERSITÉ MOHAMMED V DE RABAT

Faculté des Sciences



Département d'Informatique

Filière Licence Fondamentale
en Sciences Mathématiques et Informatique

PROJET DE FIN D'ÉTUDES

Intitulé :

Sécurité des réseaux IOT Cas du protocole RPL

Présenté par :

ABD EL MONAIME BELKHADRI ET ANASS ASSAL

soutenu le 06 Juin 2023 devant le Jury

Pr Ali Ouacha

M.Hassan ECHOUKAIRI

Pr Abderrahmane EZ-ZAHOUT

Faculté des sciences Rabat/UM5

Faculté des sciences Rabat/UM5

Faculté des sciences Rabat/UM5

Président

Encadrant

Examineur

Année Universitaire 2022-2023

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères Remerciements à notre encadrant Professeur Hassan ECHOUKAIRI , pour tout le temps qu'il nous a consacré, ses conseils précieux, et pour la qualité de son suivi durant toute la période de notre projet.

Nos plus vifs remerciements s'adressent aussi à toutes les personnes qui nous ont aidés à réaliser ce projet de fin d'études.

De plus nous adressons nos fidèles remerciements à Tout le corps professoral de La Faculté des Sciences de Rabat pour leurs qualités d'enseignement.

Nous n'oublions pas de remercier nos amis et nos familles pour leur soutien inconditionnel et irremplaçable.

Résumé

L'Internet des objets (IoT) est en plein essor et constitue l'une des technologies les plus prometteuses, mais la sécurité des réseaux IoT reste une préoccupation majeure. Les réseaux de capteurs sans fil, qui sont une composante essentielle de l'IoT, sont confrontés à des défis spécifiques tels que les ressources énergétiques limitées, la communication sans fil ouverte et l'absence d'infrastructure centralisée. Dans ce contexte, le protocole de routage RPL est largement utilisé pour assurer la connectivité et l'acheminement efficace des données au sein des réseaux IoT. Cependant, le RPL présente des vulnérabilités, notamment l'attaque blackhole, qui peut compromettre la disponibilité du réseau, entraîner une consommation excessive d'énergie et dégrader les performances.

Ce rapport met en évidence l'importance de renforcer la sécurité des réseaux IoT basés sur le protocole RPL pour assurer leur bon fonctionnement et la confiance des utilisateurs.

Mots clés : IOT, RPL, LLN, BlackHole, Sécurité, Attaques, Détection.

Abstract

The Internet of Things (IoT) is booming and is one of the most promising technologies, but the security of IoT networks remains a major concern. Wireless sensor networks, which are an essential component of IoT, face specific challenges such as limited energy resources, open wireless communication, and the absence of centralized infrastructure. In this context, the RPL routing protocol is widely used to ensure connectivity and efficient data routing within IoT networks. However, RPL has vulnerabilities, including the blackhole attack, which can compromise network availability, result in excessive energy consumption, and degrade performance.

This report highlights the importance of enhancing the security of RPL-based IoT networks to ensure their proper functioning and user trust.

Keywords : IOT, RPL, LLN, Blackhole, Security, Attacks, Detection.

Table des matières

Remerciements	1
Résumé	2
Abstract	3
Introduction	6
1 Internet d’objets et RPL	8
1.1 Introduction	8
1.2 Technologies de l’IOT	8
1.2.1 Architecture de l’internet des objets :	8
1.2.2 Fonctionnement de l’internet des objets :	10
1.3 Protocole de communication RPL	11
1.3.1 Introduction :	11
1.3.2 Messages supportés par RPL(DIO, DIS, DAO,DAO-ACK) :	12
1.3.3 Construction du DODAG :	14
1.3.4 Trafics supportés par DODAG :	15
1.3.5 Objectives functions (mrhof et of0) :	16
1.3.6 Trickle Timer :	17
1.3.7 Métriques de routage :	19
1.4 Conclusion :	19
2 Sécurité des réseaux LNN :	20
2.1 Introduction :	20
2.2 Classification des attaques :	20
2.2.1 Classification des attaques basée sur les comportements :	20
2.2.2 Classification des attaques basée sur les critères de sécurité :	21
2.2.3 Classification des attaques basée sur les éléments du réseaux RPL impactés :	21
2.3 Impact de l’attaque de rang sur la topologie du protocole RPL :	22
2.3.1 Attaque d’incohérence DAG :	22
2.3.2 Attaque sur le numéro de version :	23
2.3.3 Attaque du pire parent :	24
2.3.4 Attaque par augmentation de rang :	25
2.3.5 Attaque par diminution de rang :	25
2.3.6 Attaque Blackhole :	26
2.4 Contre-mesures :	27

2.4.1	Protection d'un réseau :	27
2.4.2	Système de détection d'intrusion :	28
2.5	Conclusion :	29
3	Implémentation d'attaque BlackHole :	30
3.1	Introduction :	30
3.2	Implémentation d'attaque Blackhole sous contiki/cooja :	30
3.2.1	Configuration des fichiers :	31
3.2.2	Implémentation sur Contiki :	32
3.3	Evaluation du Rpl (avec et sans attaque) :	36
3.3.1	Throughput :	37
3.3.2	Convergence time :	38
3.3.3	Taux des paquets de contrôle :	39
3.3.4	Consommation d'énergie :	40
3.4	Solution :	41
3.5	Conclusion :	42
	Conclusion	43

Introduction

L'Internet des objets est un concept en pleine expansion ces dernières années et qui devrait voir la plus forte croissance dans les années à venir. Les réseaux de capteurs sans fil font partie intégrante de l'Internet des objets (IoT) et sont largement utilisés pour collecter et mesurer des données dans divers domaines. Cependant, la sécurité de ce type de réseaux est une préoccupation majeure en raison de leurs spécifiques et uniques caractéristiques telles que les ressources énergétiques limitées, la communication sans fil ouverte et l'absence d'infrastructure centralisée.

Dans ce contexte, le protocole de routage RPL (Routing Protocol for Low power and lossy networks) est largement déployé pour assurer la connectivité et l'acheminement efficace des données au sein des réseaux IoT.

Cependant, malgré ces avantages, il présente de potentielles failles de sécurité qui peuvent être exploitées par des attaquants malveillants. Parmi ces vulnérabilités, on trouve l'attaque blackhole qui expose une menace particulièrement préoccupante dans le domaine des IoT. Cette attaque vise à perturber le routage en falsifiant les informations des entités voisines, ce qui peut entraîner des problèmes de disponibilité du réseau, des consommations excessives d'énergie et de dégradation des performances.

Dans ce cadre, notre projet de recherche se concentre sur l'étude et l'évaluation des réseaux IoT sous l'impact de cette attaque. A cet égard, nous proposons une approche qui vise à évaluer les performances du protocole RPL en présence d'une attaque blackhole, en se basant sur les métriques suivantes : la consommation d'énergie, le débit, le temps de convergence et le taux des messages de contrôle. Les résultats obtenus révèlent une augmentation de la consommation d'énergie, une diminution du débit de données, une augmentation du temps de convergence et une réduction du taux des messages de contrôle dans les scénarios avec attaque par rapport aux scénarios sans attaque. Ces conclusions mettent en évidence l'impact négatif de l'attaque blackhole sur les performances et la fiabilité des réseaux IoT étudiés.

À la lumière de cette évaluation, nous mettons en évidence l'influence de cette attaque blackhole sur les performances du protocole RPL. Afin de détecter et d'atténuer l'effet néfaste de cette attaque, nous proposons une approche préventive basée sur l'analyse de trafic qui utilise des seuils prédéfinis en termes de throughput et du taux des messages de contrôle (DAO et DIO) lors d'identification des paquets circulants en réseaux.

Ce rapport vise à fournir une vue d'ensemble complète d'étude sur la sécurité des réseaux IoT, en mettant l'accent sur l'attaque blackhole dans le protocole RPL. Le

travail réalisé est organisé comme suit : le premier chapitre aborde en détail le concept des Internet d'Objets et le fonctionnement du protocole RPL. Le second chapitre traite la sécurité des réseaux LLN. Ensuite, l'implémentation de l'attaque ainsi que l'analyse des résultats obtenus sont exposées au troisième chapitre. Enfin, nous terminions par une conclusion qui résume notre travail et partage , les principales découvertes de notre recherche sur la sécurité des réseaux IoT, tout en proposant des pistes pour de futures avancées dans ce domaine crucial.

Chapitre 1

Internet d’objets et RPL

1.1 Introduction

Les réseaux de capteurs sans fil font partie intégrante de l’Internet des objets (IoT) et sont largement utilisés pour collecter et mesurer des données dans divers domaines. Le marché mondial de l’IoT a connu une croissance significative ces dernières années et devrait continuer à croître dans les années à venir. Selon des estimations récentes, le marché mondial de l’IoT a été évalué à 300,3 milliards de dollars en 2021 et devrait atteindre 650,5 milliards de dollars d’ici 2026 [1].

L’IoT est en train de transformer de nombreux aspects de notre vie quotidienne. Grâce à la capacité de collecter et d’analyser des données en temps réel, les objets connectés peuvent aider à optimiser les performances, améliorer la prise de décision et simplifier les tâches quotidiennes. Par exemple, dans le domaine de la santé, les dispositifs portables peuvent surveiller les signes vitaux et les activités physiques pour aider à diagnostiquer et à traiter les maladies chroniques. Dans l’industrie, les machines connectées peuvent détecter les défaillances avant qu’elles ne se produisent, réduisant ainsi les temps d’arrêt et augmentant l’efficacité de la production. Les villes intelligentes peuvent utiliser des capteurs pour surveiller la qualité de l’air, réduire la consommation d’énergie et améliorer les systèmes de transport. Toutefois, avec l’augmentation du nombre d’appareils connectés, il est important de mettre en place des mesures de sécurité robustes pour protéger les données sensibles contre les cyberattaques. La croissance rapide de l’IoT offre de nombreuses opportunités pour les entreprises, mais nécessite également une planification et une mise en œuvre soigneuses pour assurer la durabilité et la sécurité à long terme.

1.2 Technologies de l’IOT

1.2.1 Architecture de l’internet des objets :

L’architecture IoT (Internet des objets) est un ensemble de composants logiciels et matériels qui permettent de connecter des objets physiques à Internet. L’objectif de l’architecture IoT est de permettre à ces objets de communiquer entre eux et avec des systèmes informatiques pour collecter des données.

L'architecture IoT peut être utilisée dans de nombreux domaines, tels que l'industrie, l'agriculture, la santé, les villes intelligentes, les maisons intelligentes, les voitures connectées, etc. Elle permet aux entreprises et aux organisations de collecter des données en temps réel, de prendre des décisions plus rapidement, d'optimiser leurs processus et de fournir des services plus efficaces et personnalisés.

L'architecture de l'IoT peut être divisée en plusieurs couches, il n'existe pas de norme unique d'architecture de référence pour l'Internet des objets (IoT) car elle englobe une diversité de technologies. Bien qu'il n'y ait pas d'architecture IoT universellement acceptée, le format le plus fondamental et le plus largement reconnu est une architecture IoT composée de quatre ou cinq couches[2].

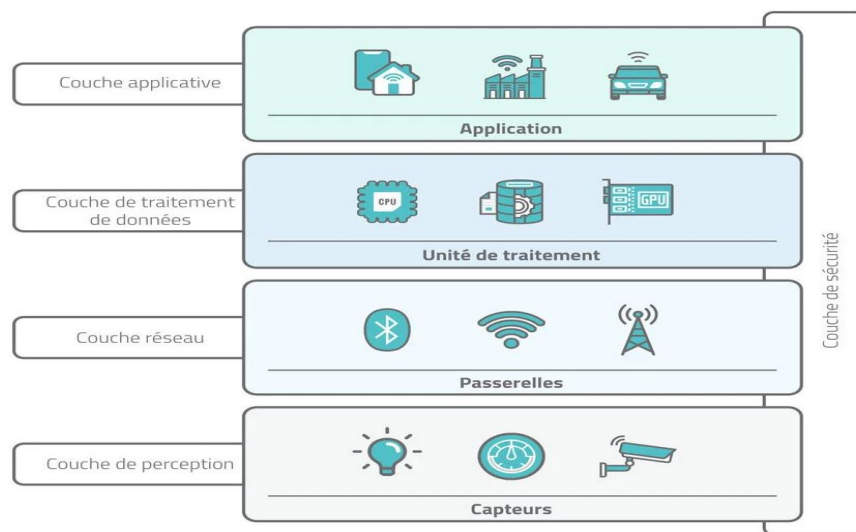


FIGURE 1.2.1 – Architecture de réseaux IoT

1 - Couche de perception : Cette couche se compose des capteurs et des actionneurs qui sont utilisés pour collecter les données à partir de l'environnement physique. Les capteurs mesurent les données physiques telles que la température, la pression, la lumière, etc. tandis que les actionneurs permettent de contrôler les appareils et les machines.

- Capteurs : tels que les sondes, les jauges, les compteurs et autres dispositifs similaires, sont responsables de la collecte de paramètres physiques tels que la température ou l'humidité. Ils convertissent ces paramètres en signaux électriques et les transmettent au système IoT. Les capteurs IoT sont généralement de petite taille et ont une faible consommation d'énergie.
- Actionneurs : interprètent les signaux électriques provenant du système IoT et les transforment en actions physiques concrètes.
- Dispositifs : ils sont connectés soit à des capteurs et des actionneurs, soit ils font partie intégrante de ceux-ci.

2 - Couche réseau : Cette couche est responsable de la connectivité entre les dispositifs IoT. Elle permet la transmission des données collectées entre les différents dispositifs de l'architecture IoT. Elle utilise des protocoles de communication tels que le Wi-Fi, le Bluetooth, le Zigbee, etc. pour assurer la connectivité entre les objets.

- Zigbee : est un protocole de communication sans fil à faible consommation d'énergie et à courte portée, utilisé principalement dans les réseaux de capteurs sans fil et l'Internet des objets (IoT).

3 - La couche de traitement de données : cette couche permet de collecter, stocker et traiter les données générées par les dispositifs connectés. Elle peut être divisée en deux sous-couches (la couche de collecte de données et la couche d'analyse de données).

- La couche de collecte de données est responsable de la collecte des données provenant de différents capteurs et dispositifs connectés. Ces données peuvent être stockées localement sur les dispositifs, dans des passerelles IoT ou dans le cloud.
- La couche d'analyse de données est responsable de l'analyse et du traitement des données collectées. Elle peut utiliser des techniques d'analyse de données telles que l'apprentissage automatique, le traitement du langage naturel et la vision par ordinateur pour extraire des informations utiles à partir des données brutes.

4 - Couche applicative : Cette couche concerne les applications et les services qui utilisent les données collectées par les dispositifs IoT. Les applications peuvent inclure des applications de surveillance de l'environnement, des applications de surveillance de la santé, des applications de contrôle industriel, etc.

5 - Couche de sécurité : Cette couche est responsable de la sécurité de l'architecture IoT. Elle garantit que les données collectées et traitées sont protégées contre les attaques malveillantes. Elle utilise des technologies de cryptage, d'authentification, de contrôle d'accès, etc. pour assurer la confidentialité et l'intégrité des données.

1.2.2 Fonctionnement de l'internet des objets :

Les dispositifs IoT sont nos yeux et nos oreilles lorsque nous ne pouvons pas être présents physiquement. Ils collectent toutes les données pour lesquelles ils sont programmés, et ces données peuvent être analysées pour automatiser les futures décisions et actions. Ce processus implique quatre étapes [3].

Etape 1 : **Capture des données.** Les dispositifs IoT sont équipés de capteurs qui leur permettent de collecter des données dans leur environnement. Cette tâche peut être aussi simple qu'une mesure de température ou aussi complexe qu'un flux vidéo en temps réel, selon les besoins de la situation.

Etape 2 :**Partage des données.** Les terminaux IoT utilisent les connexions réseau disponibles pour transférer ces données vers un système cloud public ou privé (d'un terminal à un système ou d'un terminal à un autre) ou pour les stocker localement afin de les traiter en périphérie.

Etape 3 :**Traitement des données.**À ce stade, le programme est conçu pour déclencher une action en fonction des données collectées, telles que l'allumage d'un ventilateur ou l'envoi d'une alerte.

Etape 4 :**Exploitation des données.** Les informations recueillies à partir de tous les appareils d'un réseau IoT sont analysées pour en tirer des connaissances solides qui permettent de prendre des décisions et des mesures en toute confiance.

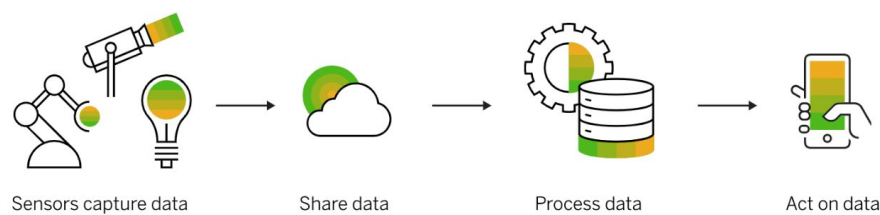


FIGURE 1.2.2 – Fonctionnement de IOT

1.3 Protocole de communication RPL

1.3.1 Introduction :

Avant l'apparition du protocole RPL, les réseaux de capteurs sans fil (WSN) utilisaient des protocoles de routage conçus pour les réseaux filaires, tels que le protocole de routage à vecteur de distance (Distance Vector Routing) ou le protocole de routage à état de lien (Link State Routing). Cependant, ces protocoles ne sont pas adaptés aux caractéristiques des WSN, qui présentent des contraintes importantes en termes de consommation d'énergie, de capacité de traitement et de mémoire.

Les réseaux de capteurs sans fil présentent également des caractéristiques particulières telles que la topologie dynamique, les pertes de paquets fréquentes et les liens peu fiables, qui rendent difficile la mise en place d'un protocole de routage efficace.

En outre, les WSN sont souvent utilisés dans des environnements difficiles d'accès ou dangereux pour les humains, ce qui rend difficile la maintenance ou le remplacement des capteurs défectueux. Par conséquent, il est important que les protocoles de routage des WSN soient résilients et capables de s'adapter à des environnements changeants.

Ces problèmes ont conduit au développement du protocole RPL, qui a été spécifiquement conçu pour répondre aux besoins de routage des réseaux de capteurs sans fil. Le protocole RPL permet un routage efficace et économe en énergie dans les WSN, en

prenant en compte les caractéristiques particulières de ces réseaux.

Le protocole RPL (Routing Protocol for Low-Power and Lossy Networks) est un protocole de routage conçu pour les réseaux de capteurs sans fil et autres réseaux basse consommation et à faible taux de transmission de données. Il utilise une topologie en arbre pour le routage des données et est conçu pour minimiser la consommation d'énergie tout en permettant une communication efficace entre les nœuds du réseau[4].

1.3.2 Messages supportés par RPL(DIO, DIS, DAO,DAO-ACK) :

Les messages RPL sont un nouveau type de messages de contrôle ICMPv6, qui sont spécifiés pour inclure un en-tête ICMPv6 avec trois champs : Type, Code et Checksum.

Ils contiennent également un corps de message qui inclut une base de message et plusieurs options. Le champ Type spécifie le type de message de contrôle ICMPv6 tandis que le champ Code identifie le type de message de contrôle RPL.[5]

il y a quatre codes définis. :

1. **DIS (DODAG Information Solicitation)** : ce message est envoyé par un nouveau nœud peut rejoindre un réseau déjà formé en diffusant un message DIS pour solliciter en réponse un message DIO.
2. **DIO (DODAG Information Object)** : Ce message sert à informer les nœuds parents de l'existence du DODAG et pour propager des informations sur sa structure aux nœuds enfants. Les nœuds parent envoient périodiquement des messages DIO pour informer les nœuds voisins de leur existence et des paramètres de leur parenté dans le DODAG. Le DIO contient des informations telles que l'identifiant du DODAG, l'adresse du nœud parent, le rang du nœud dans le DODAG et les options de configuration.

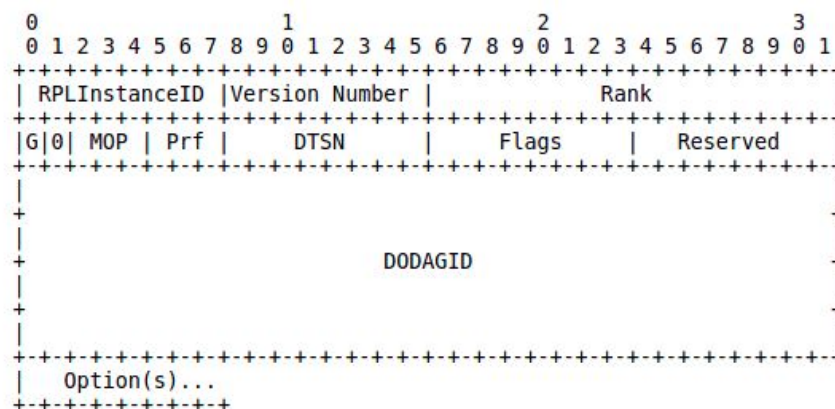


FIGURE 1.3.1 – Champs d'un messageDIO

RPLInstanceID : Le champ RPLInstanceID est un champ de 8 bits qui identifie l'instance RPL à laquelle le message DIO appartient.

Version Number : Le champ Version spécifie le numéro de version du protocole RPL utilisé.

Rank : Le champ Rank est un champ de 16 bits qui indique le rang du nœud émetteur dans le DODAG. Le rang est utilisé pour établir la position du nœud au sein du réseau, ainsi que pour déterminer le chemin le plus direct vers la racine.

G (Grounded) : Le champ Grounded est un champ d'un bit qui indique si le nœud émetteur est connecté directement à la racine du DODAG.

MOP(Mode of Operation) : Le champ MOP permet aux nœuds de synchroniser leur mode de fonctionnement et de prendre des décisions de routage en conséquence.

Prf(Pseudo-Random Function) : est un champ de 16 bits qui indique l'ID du parent préféré pour le nœud émetteur. Il permet de spécifier le nœud vers lequel le nœud émetteur préfère envoyer ses messages de données.

DTSN(Destination Advertisement Trigger Sequence Number) : est un champ de 8 bits qui indique le numéro de séquence associé au dernier message de type DAO (Destination Advertisement Object) reçu par le nœud émetteur.

Flags : est un champ de 8 bits qui contient plusieurs indicateurs d'état et d'informations pour la gestion de la topologie du réseau. Les valeurs des bits dans le champ "flags" indiquent si le DODAG est en train de se construire, si le nœud émetteur est un nœud racine, si le DODAG est orienté ou non, etc.

Reseverd : est un champ de 8 bits est réservé à des fins futures. L'émetteur doit le mettre à zéro et le destinataire doit l'ignorer.

DODAGID : Le champ DODAGID est un champ de 16 octets qui identifie de manière unique le DODAG auquel le nœud émetteur appartient.

Option : le champ option qui indique les options supplémentaires présentes dans le message DIO. Ces options peuvent inclure des informations sur les métriques de coût, les adresses IPv6 des nœuds parents et des informations de sécurité.

Ces champs de message DIO sont utilisés pour permettre aux nœuds du réseau de construire et de maintenir le DODAG, ainsi que pour prendre des décisions de routage efficaces en fonction de l'état actuel du réseau.

3. **DAO (Destination Annonce Objet)** : Chaque nœud, sauf la racine DODAG, envoie des messages DAO pour mettre à jour les tables de routage avec les préfixes de ses enfants et pour publier ses propres adresses et préfixes à ses parents. En envoyant ce message DAO le long du chemin d'un nœud particulier à la racine DODAG via les routes DAG par défaut, un chemin complet entre la racine DODAG et le nœud est établi.
4. **DAO-ACK** : ce message est envoyé par un nœud parent pour confirmer la réception d'un message DAO de son enfant.

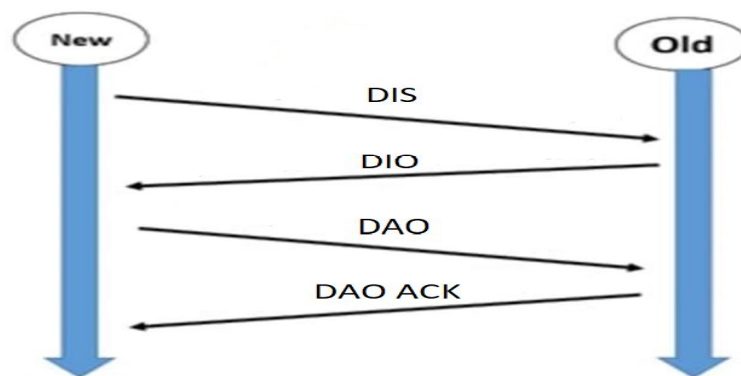


FIGURE 1.3.2 – Messages de contrôle RPL

1.3.3 Construction du DODAG :

Le DODAG est la structure logique sur laquelle repose le protocole RPL. C'est un graphe acyclique orienté vers une destination spécifique. La racine (DODAG root) de chaque DODAG diffuse un message DIO contenant des informations telles que le numéro de version, l'identifiant de l'instance et la fonction objectif utilisée. Une instance RPL est formée par plusieurs DODAGs qui partagent la même fonction objectif et un identifiant appelé RPLInstanceID.

Chaque nœud, après avoir reçu le message DIO, calcule son rang en utilisant la fonction objectif pour s'assurer d'avoir un rang supérieur à celui de son parent, et l'ajoute à sa liste de parents. Si le rang du nœud récepteur est inférieur à celui de l'émetteur, le DIO est ignoré. Pour rejoindre un DODAG déjà formé, un nouveau nœud diffuse un message DIS pour obtenir les informations de configuration nécessaires et recevra en réponse des messages DIO en provenance de plusieurs nœuds. Pour assurer la maintenance du DODAG, les DIO sont envoyés périodiquement pour configurer les routes et annoncer les changements.

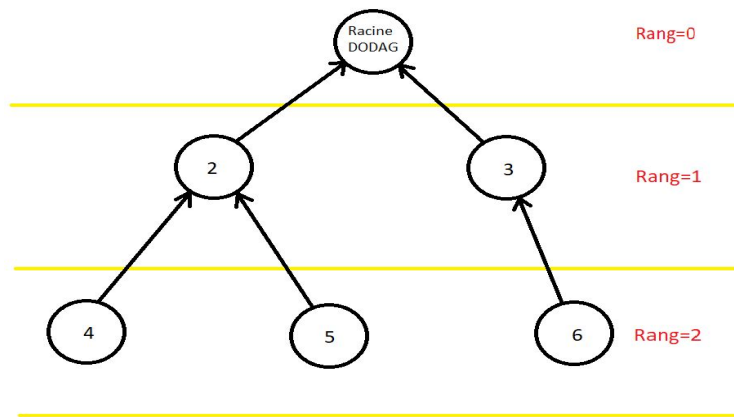


FIGURE 1.3.3 – Construction du DODAG

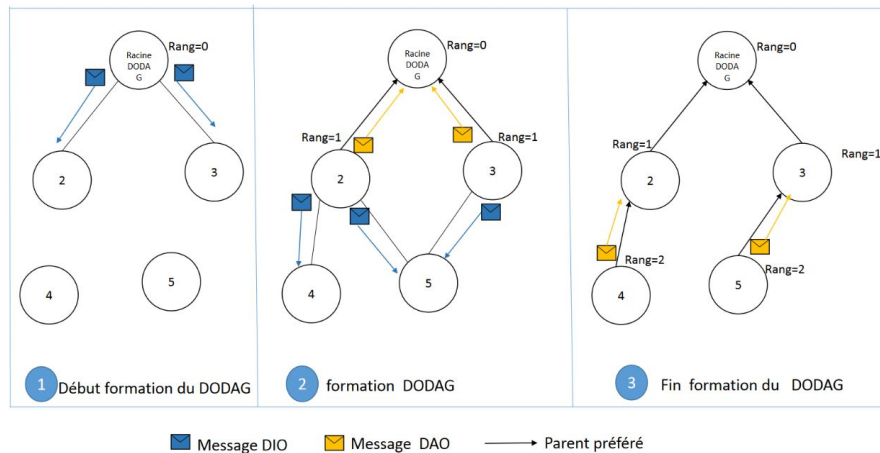


FIGURE 1.3.4 – Construction Du DODAG - Suite

1.3.4 Trafics supportés par DODAG :

Le DODAG supporte différents types de trafic tels que le trafic à faible latence, à faible consommation d'énergie, à haute fiabilité et à haute bande passante, en utilisant des protocoles de routage adaptés.

Trafic à faible latence : ce type de trafic nécessite une communication en temps réel et une faible latence. Il est utilisé pour les applications qui nécessitent une réponse rapide, comme les jeux en ligne, les appels vidéo ou les applications de réalité virtuelle. Les protocoles de routage tels que le MRHOF sont utilisés pour acheminer ces types de trafic, car ils peuvent réduire le temps de transmission des données en choisissant des chemins plus courts et plus rapides.

Trafic à faible consommation d'énergie : ce type de trafic est utilisé pour les ap-

plications qui ont des contraintes d'énergie, comme les capteurs sans fil alimentés par batterie. Les protocoles de routage tels que l'OF0 sont utilisés pour acheminer ces types de trafic, car ils peuvent minimiser la consommation d'énergie en choisissant des chemins qui nécessitent moins de transmission de données et donc moins de consommation d'énergie.

Trafic à haute fiabilité : ce type de trafic est utilisé pour les applications qui nécessitent une transmission de données fiable, comme les systèmes de sécurité ou de surveillance. Les protocoles de routage tels que le MRHOF sont utilisés pour acheminer ces types de trafic, car ils peuvent choisir des chemins plus fiables avec une meilleure qualité de lien.

Trafic à haute bande passante : ce type de trafic est utilisé pour les applications qui nécessitent une transmission de données à haut débit, comme la diffusion de vidéos en direct ou le téléchargement de fichiers volumineux. Les protocoles de routage tels que l'OF0 sont utilisés pour acheminer ces types de trafic, car ils peuvent choisir des chemins avec une bande passante plus élevée pour une transmission de données plus rapide.

1.3.5 Objectives functions (mrhof et of0) :

La fonction objectif (OF) joue un rôle crucial dans la sélection et l'optimisation des chemins dans une instance RPL, en prenant en compte les métriques de routage et les contraintes. Le message DIO utilise un code point objectif (OCP) pour indiquer la fonction objectif à utiliser pour construire le DODAG. Le DODAG contient un nœud racine qui émet un message DIO contenant des informations telles que le numéro de version, l'ID d'instance et la fonction objective. Les nœuds calculent leur rang à l'aide de la fonction objective et s'ajoutent à la liste de leur parent. De nouveaux nœuds peuvent rejoindre en diffusant un message DIS et en recevant des messages DIO de plusieurs nœuds. Le RPL dispose de deux fonctions objectives pour évaluer le rang des nœuds et sélectionner les parents. Le groupe de travail a défini OF0 et MRHOF pour s'adapter à différents critères d'optimisation, applications et conceptions de réseaux.

La fonction OF0 : La fonction OF0 est une des deux fonctions objectives du protocole RPL, qui sert à optimiser les itinéraires d'une instance RPL en se basant sur la DIO. Dans cette fonction, la métrique d'acheminement utilisée est le nombre de sauts, et elle permet de calculer un rang pour chaque périphérique dans l'instance RPL. Son objectif principal est de favoriser l'interopérabilité entre différentes implémentations de RPL[7]. Les caractéristiques principales de OF0 sont :

1. Opérations OF0 : Les fonctions objectives OF0 impliquent le calcul de classement qui évalue une variable appelée **step_of_rank** pour un parent donné, en utilisant des propriétés et des métriques de lien appropriées, ainsi que la sélection des parents préférés ou du successeur réalisable de sauvegarde.
2. Les variables : **step_of_rank** est une étape intermédiaire de calcul qui prend en compte les propriétés de la liaison avec un voisin donné, tandis que le

`rank_increase` correspond à la différence entre le rang du parent préféré et le déclencheur.

3. Les valeurs initiales des constantes sont utilisées pendant la configuration ou l'implémentation.

MRHOF(The Minimum Rank with Hysteresis Objective Function)

Le MRHOF est une fonction objective de RPL qui utilise une stratégie hystérique pour sélectionner le chemin avec la plus petite valeur métrique. La métrique utilisée dans cette fonction est déterminée dans le conteneur de métrique DIO, et est généralement basée sur le nombre attendu de retransmissions (ETX), avec une hystérie pour éviter les différences minimales de rang. Cette métrique permet à RPL de trouver des chemins stables des nœuds vers la racine. Si une métrique n'est pas disponible dans le conteneur DIO, le MRHOF utilise par défaut ETX[8]. Les caractéristiques du MRHOF incluent :

1. Le calcul du coût du chemin entre deux nœuds, qu'ils soient racine ou non, est effectué.
2. Si le coût du chemin d'un voisin candidat ou d'un parent préféré subit une variation, alors la sélection des parents est effectuée.
3. Lorsqu'un nœud non racine choisit son parent préféré, il utilise le coût du chemin vers ce parent pour calculer une valeur de rang qui permettra de classer les nœuds.
4. Le coût du chemin depuis un nœud jusqu'à la racine est calculé lors de la dernière sélection de parent et stocké dans la variable `cur_min_path_cost`. Cette variable représente le coût du chemin via le parent préféré du nœud.
5. Les variables `MAX_LINK_METRIC`, `MAX_PATH_COST`, `PARENT_SWITCH_THRESHO`, `PARENT_SET_SIZE` et `ALLOW_FLOATING_ROOT` sont des paramètres qui contiennent chacun un entier positif. Ces entiers peuvent représenter la valeur maximale autorisée pour une métrique ou le coût d'un chemin spécifique.

1.3.6 Trickle Timer :

Le protocole RPL utilise une technique appelée Trickle Timer pour réduire la surcharge des messages de contrôle dans le réseau. Cette technique permet de ne transmettre que les mises à jour nécessaires en détectant les incohérences dans la topologie du réseau. Lorsqu'un nœud reçoit des mises à jour DIO cohérentes avec sa propre compréhension de la topologie du réseau, un compteur de redondance est incrémenté. Si le nombre de mises à jour cohérentes dépasse le nombre de redondances dans un intervalle de temps, le nœud ne transmet aucune mise à jour et la période d'écoute est doublée. Cependant,

si une mise à jour incohérente est détectée, le Trickle Timer est réinitialisé et une mise à jour est rapidement propagée[9].

Les paramètres et variables : Le Trickle fonctionne comme une minuterie d'où son fonctionnement est pour un temps défini. Les paramètres de configuration de Trickle sont :

1. **Imin** représente la plus petite taille permise pour l'intervalle de transmission.
2. **Imax** c'est la taille maximale de l'intervalle de transmission.
3. **K** entier positif, c'est la constante de redondance.

Les variables de Trickle sont :

1. **I** la taille de l'intervalle actuelle.
2. **t** l'heure de l'intervalle actuelle.
3. **c** le compteur.

Les règles de Trickle :

Le mécanisme Trickle Timer est basée sur les six règles suivantes :

1. Lors de l'exécution, l'algorithme démarre le premier intervalle en initialisant la valeur de **I** dans la plage [**Imin**-**Imax**].
2. Lorsqu'un intervalle commence, l'algorithme remet **c** à zéro et définit **t** à un point aléatoire dans l'intervalle du plage [**I**/2 , **I**].
3. À chaque fois qu'un signal cohérent est entendu par Trickle, le conteur se voit augmenter.
4. Si, au temps **t**, le conteur est inférieur à la constante de redondance **k**, alors Trickle procède à l'émission.
5. Lorsque l'intervalle **I** expire, Trickle double la longueur de l'intervalle.
6. Le minuteur de maintien est réinitialisé si Trickle perçoit une transmission incohérente et que la valeur de **I** est supérieure à **Imax**. Dans le cas contraire, si la valeur de **I** est inférieure à **Imax**, elle est redéfinie sur **Imin**, permettant ainsi de démarrer un nouvel intervalle avec la réinitialisation du minuteur.

1.3.7 Métriques de routage :

Le protocole RPL a défini deux catégories de métriques de routage pour le calcul des chemins. La métrique de nœud, qui prend en considération les attributs spécifiques à chaque nœud, et la métrique de liaison, qui prend en compte les attributs des liens[10].

Métrique de nœud :

- **Les états ou attributs** : fournissent des informations sur les caractéristiques du nœud telle que l'usage du CPU, la mémoire consommée.
- **Le nombre de sauts** : équivaut au nombre de nœud traversé pour atteindre la racine. Plus le nombre de sauts est faible, plus le nœud est proche de la racine.
- **L'énergie** : représente la source d'énergie du nœud (batterie, secteur, etc.).

Métrique de liaison :

- **Le débit** : correspond à la quantité de données qui traverse un lien pendant une période donnée.
- **La latence** : mesure la durée nécessaire pour transmettre un paquet de données depuis l'émetteur jusqu'au récepteur.
- **La fiabilité** : est une mesure abstraite qui exprime la qualité d'un lien, représentée par l'ETX (Expected Transmission Count), c'est-à-dire le nombre de transmissions anticipées qu'un nœud doit effectuer vers une destination pour livrer avec succès un paquet. Lorsqu'il y a des pertes de paquets, la valeur de l'ETX augmente, tandis qu'une augmentation du taux de livraison réussie diminue la valeur de l'ETX.

1.4 Conclusion :

Le premier chapitre de notre rapport a présenté les concepts fondamentaux de l'Internet des objets (IoT) et du protocole de communication RPL. Nous avons examiné l'architecture de l'IoT, le fonctionnement de l'IoT, ainsi que les différents messages de contrôle, la construction du DODAG, les trafics supportés et les fonctions objectives du protocole RPL. Cette compréhension approfondie de RPL jettera les bases pour l'exploration de la sécurité des réseaux LNN, qui sera abordée dans le chapitre suivant.

Chapitre 2

Sécurité des réseaux LNN :

2.1 Introduction :

La sécurité des systèmes IoT est une préoccupation majeure en raison des ressources limitées, des lacunes en matière de mobilité et d'identification, ainsi que de la facilité de capture des appareils IoT. Alors que de plus en plus d'appareils/objets sont connectés chaque jour et que de plus en plus d'appareils intelligents sont installés dans les maisons, les hôpitaux et les bâtiments, le nombre de vulnérabilités que les intrus peuvent exploiter pour compromettre les réseaux IoT continue d'augmenter. De plus, 6LoWPAN, basé sur IEEE 802.15.4 et IPv6, crée des vulnérabilités et génère de nouvelles menaces des deux côtés, étendant ainsi diverses couches de l'architecture IoT de la couche de service/application à la couche de perception physique cible. Selon [4], l'architecture à 3 niveaux emprunte des couches et des concepts à la pile réseau et intègre ainsi les menaces respectives telles que l'accès non autorisé aux données et les attaques DoS ou de disponibilité. Pour protéger ces réseaux, il est essentiel de comprendre les différents types d'attaques auxquelles ils sont exposés.

2.2 Classification des attaques :

Dans le cadre de la classification basée sur les comportements, ces attaques sont classées en fonction des comportements qu'elles induisent dans le réseau.

2.2.1 Classification des attaques basée sur les comportements :

Les attaques sur les réseaux LNN peuvent être classées en deux catégories : les attaques actives et les attaques passives[6]. Les attaques actives sont celles qui ont un effet sur le fonctionnement du réseau en perturbant les communications ou en altérant les données. Les attaques par interruption de service (Dos) sont un exemple d'attaques actives. Elles consistent à envoyer un grand nombre de paquets au réseau pour saturer sa bande passante ou à exploiter une vulnérabilité pour rendre les nœuds indisponibles. Ces attaques peuvent causer des perturbations importantes dans le fonctionnement du

réseau et rendre certains services inaccessibles. Les attaques passives sont celles qui ne modifient pas le fonctionnement du réseau mais cherchent à intercepter les données qui y transitent. Les attaques par écoute (sniffing) sont un exemple d'attaques passives. Elles consistent à intercepter les paquets envoyés dans le réseau pour en extraire des informations sensibles telles que des mots de passe, des clés de chiffrement ou des données confidentielles. Ces attaques sont souvent difficiles à détecter car elles ne modifient pas le fonctionnement du réseau.

2.2.2 Classification des attaques basée sur les critères de sécurité :

La classification des attaques basée sur les critères de sécurité regroupe les attaques en fonction des trois piliers de la sécurité de l'information : la confidentialité, l'intégrité et la disponibilité. Ces critères représentent les objectifs fondamentaux de toute politique de sécurité. :

- Attaques contre la confidentialité : ces attaques visent à accéder à des informations confidentielles, telles que des mots de passe, des données sensibles ou des informations personnelles. Les exemples incluent l'écoute illégale, le vol d'identité, le sniffing de réseau ou le décryptage de données.
- Attaques contre l'intégrité : ces attaques visent à altérer ou à détruire des informations, des systèmes ou des réseaux. Elles peuvent causer des dégâts importants aux entreprises ou aux organisations, par exemple, en modifiant les données ou en introduisant des virus ou des malwares. Les exemples incluent l'injection de code malveillant, la falsification de données ou le détournement de session.
- Attaques contre la disponibilité : ces attaques visent à empêcher l'accès ou l'utilisation légitime des ressources. Elles peuvent paralyser des systèmes, des réseaux ou des services, entraînant des perturbations importantes. Les exemples incluent les attaques par déni de service (DoS), les attaques par saturation ou les attaques physiques.

2.2.3 Classification des attaques basée sur les éléments du réseau RPL impactés :

Les attaques sur les réseaux RPL peuvent viser différents éléments de ce protocole. Voici les classifications des attaques basées sur les éléments du réseau RPL impactés[7] :

- Les attaques qui visent à épuiser les ressources du réseau : Les attaques ciblant les ressources du réseau RPL sont souvent utilisées pour perturber le fonctionnement normal du réseau en épuisant les ressources critiques telles que l'énergie. Les conséquences de telles attaques peuvent être graves car elles peuvent entraîner

une dégradation significative des performances du réseau, une réduction de la durée de vie des batteries des nœuds et même une interruption complète du service.

- Les attaques qui visent la sécurité du Rpl : un attaquant intercepte et surveille les communications entre les nœuds, peuvent compromettre la confidentialité et l'intégrité des données. De même, les attaques de détournement, où un attaquant usurpe l'identité d'un nœud légitime pour intercepter ou manipuler le trafic réseau, peuvent causer des dommages considérables.
- Les attaques contre la topologie du réseau (énergie, mémoire et puissance de traitement) : Ces attaques peuvent prendre différentes formes, telles que des attaques par brouillage qui perturbent les communications sans fil en émettant des signaux sur les mêmes fréquences que celles utilisées par les dispositifs du réseau RPL. Ces perturbations peuvent causer des dysfonctionnements dans la topologie du réseau. Les attaques de falsification de paquets constituent également une menace. Elles consistent à modifier les informations contenues dans les paquets RPL pour induire des nœuds à prendre des décisions erronées lors de la construction de la topologie du réseau.

2.3 Impact de l'attaque de rang sur la topologie du protocole RPL :

2.3.1 Attaque d'incohérence DAG :

Le protocole RPL utilise un algorithme de construction de DAG basé sur la hiérarchie des nœuds, où chaque nœud a un parent et un ou plusieurs enfants dans le DAG. Le parent d'un nœud est choisi en fonction de la qualité de la liaison et de la distance par rapport à la racine du DAG. Le DAG est construit en utilisant des messages de contrôle (DAO, DODAG Information Object) échangés entre les nœuds.

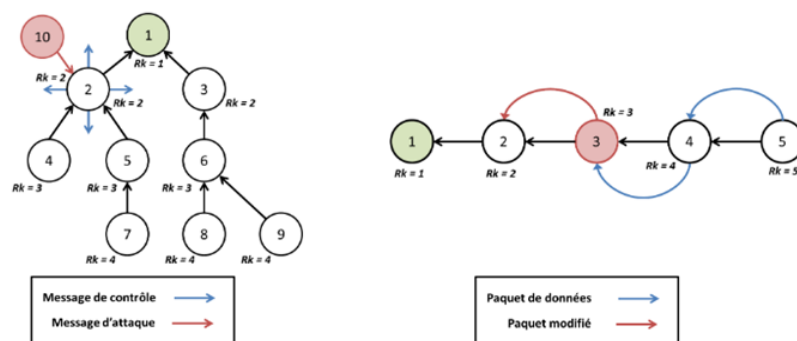


FIGURE 2.3.1 – Attack d'incohérence DAG

L'attaquant a modifié le DAG pour que les nœuds soient redirigés vers un nœud

malveillant plutôt que vers le nœud root légitime

L'attaque d'incohérence DAG dans RPL consiste à modifier la structure du DAG pour tromper les nœuds du réseau en leur faisant prendre des décisions de routage erronées, ce qui peut entraîner des perturbations de la communication et la perte de données[8].

L'attaque d'incohérence DAG peut être lancée en utilisant des messages DAO falsifiés, qui contiennent des informations erronées sur la qualité de la liaison ou la position des nœuds. Les nœuds du réseau peuvent alors prendre des décisions de routage erronées en se basant sur ces informations, ce qui peut conduire à des congestions, des délais de transmission ou même des pertes de données.

Pour éviter ce type d'attaque, il est important d'utiliser des mécanismes de sécurité tels que le chiffrement et l'authentification dans le réseau RPL.

2.3.2 Attaque sur le numéro de version :

Le champ du numéro de version dans les messages DIO est un élément crucial qui doit être transmis sans modification le long du DODAG. Seule la racine est autorisée à l'incrémenter pour créer une nouvelle version du DODAG, permettant ainsi de valider l'intégrité du réseau et de permettre une réparation globale.

L'attaque par numéro de version dans la topologie des réseaux RPL peut illégalement incrémenter le numéro de version du DODAG de la racine par un nœud malveillant lorsque le message DIO est transmis à ses nœuds voisins pour endommager les performances du réseau[9]. Lorsque les nœuds voisins reçoivent le message DIO contenant le numéro de version incrémenté, l'arbre DODAG commence une nouvelle formulation et le « timer trickle » est réinitialisé. Ensuite, les nœuds voisins transmettront fréquemment des versions mises à jour des messages DIO à tous les nœuds. L'attaque par numéro de version a des impacts significatifs tels que :

1. Les opérations du réseau sont endommagées.
2. Les frais de contrôle du réseau sont augmentés de 18 fois, ce qui est inutile.
3. Il y aura des boucles de routage dans la transmission de données.
4. La consommation d'énergie du réseau est augmentée.
5. Les canaux de communication des nœuds présentent des problèmes de disponibilité. En outre, la livraison des paquets est perdue et le délai du réseau est doublé.

Dans ce schéma, l'attaquant envoie un message DIO modifié avec un numéro de version illégitime à un nœud voisin. Ce nœud voisin, pensant que ce numéro de version est valide, propage l'information aux autres nœuds voisins. Ceux-ci propagent ensuite à leur tour

cette information erronée, entraînant la propagation de boucles potentielles dans le réseau.

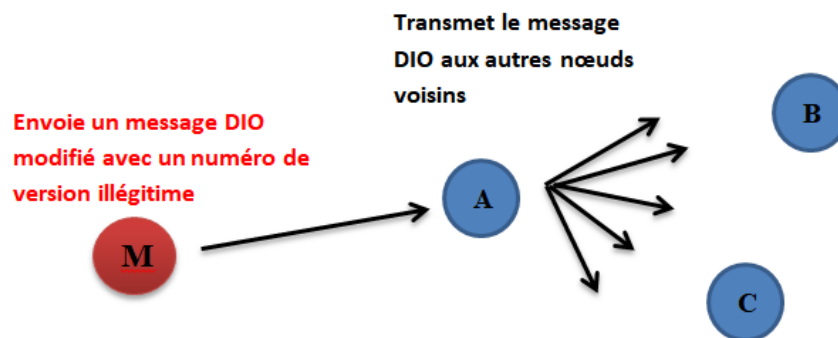


FIGURE 2.3.2 – Version Number Attack

2.3.3 Attaque du pire parent :

L'attaque du pire parent dans un réseau RPL est une menace qui vise à épuiser les ressources du réseau en forçant les nœuds à relayer le trafic de manière excessive. Les pirates modifient les informations de routage pour que les nœuds choisissent un parent qui leur est très éloigné plutôt que celui qui est le plus proche. Cela provoque une surcharge du réseau et une consommation excessive d'énergie, ce qui peut causer des dommages importants au réseau. Les réseaux à faible puissance et basse consommation sont particulièrement vulnérables à cette attaque car elle peut rapidement épuiser les batteries des nœuds.

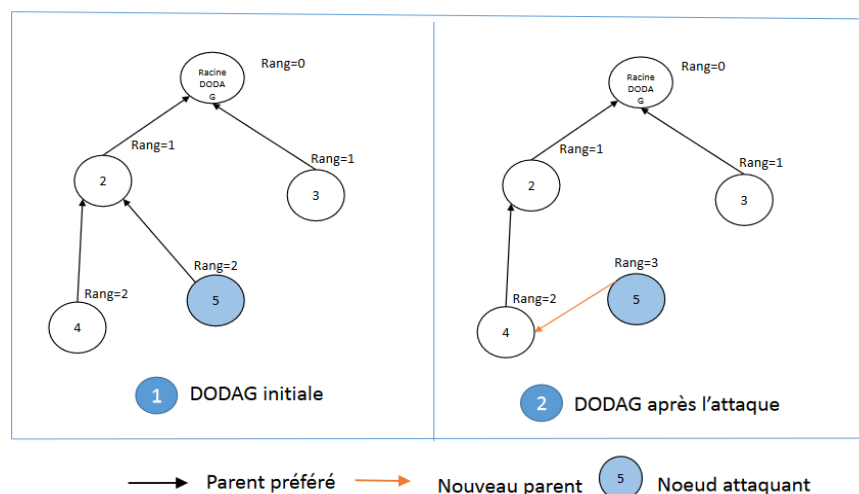


FIGURE 2.3.3 – Attaque du pire parent

Cependant, les mécanismes de sécurité tels que l'authentification des nœuds et le

chiffrement des données peuvent aider à prévenir cette attaque en garantissant que seuls les nœuds autorisés peuvent accéder au réseau et en protégeant les données en transit.

2.3.4 Attaque par augmentation de rang :

L'attaque par augmentation de rang est un type d'attaque qui fait partie des attaques de rang (rank attack)[4], quand un nœud augmente sa valeur de Rank pour qu'elle soit égale à celle du nœud ayant la valeur de Rank la plus élevée parmi ses voisins. Cela peut causer la formation de boucles entre le nœud et ses enfants, ce qui rend le réseau instable et génère plus de messages de contrôle pour récupérer la topologie optimisée. Cette attaque ajoute également plus de retards à tout le trafic acheminé à travers les nœuds compromis.

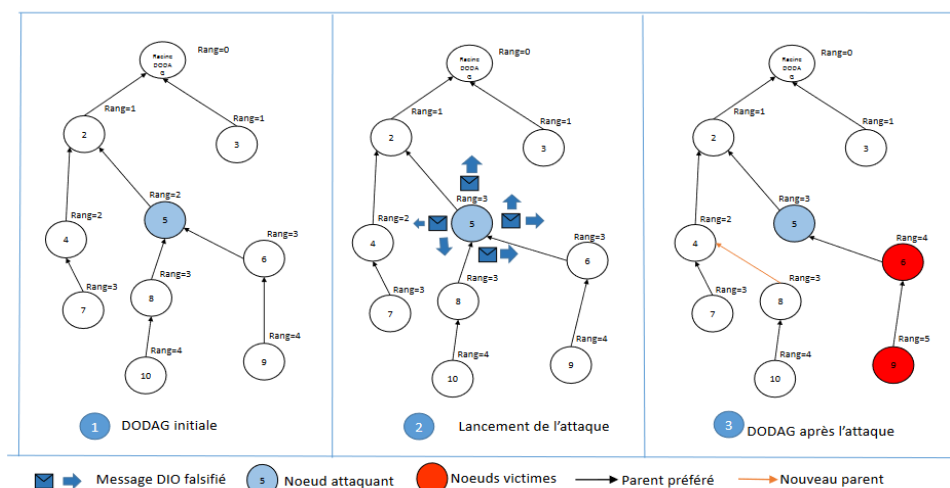


FIGURE 2.3.4 – Attaque par augmentation du rang

2.3.5 Attaque par diminution de rang :

Dans cette attaque, un nœud malveillant utilise une annonce frauduleuse pour prétendre être un nœud proche de la racine dans le graphe DODAG. Les nœuds voisins sont trompés et sélectionnent ce nœud malveillant comme parent préféré pour établir leur connexion avec la racine. Cela entraîne le transfert des communications de plusieurs nœuds vers le nœud malveillant. Cette attaque est particulièrement dangereuse car elle peut servir de point de départ pour d'autres attaques. Le nœud malveillant peut filtrer ou manipuler le trafic en transit, bloquer certains paquets de données et isoler complètement un groupe de nœuds du réseau, y compris le nœud racine. Par conséquent, les nœuds victimes ne reçoivent aucune donnée provenant des autres nœuds.

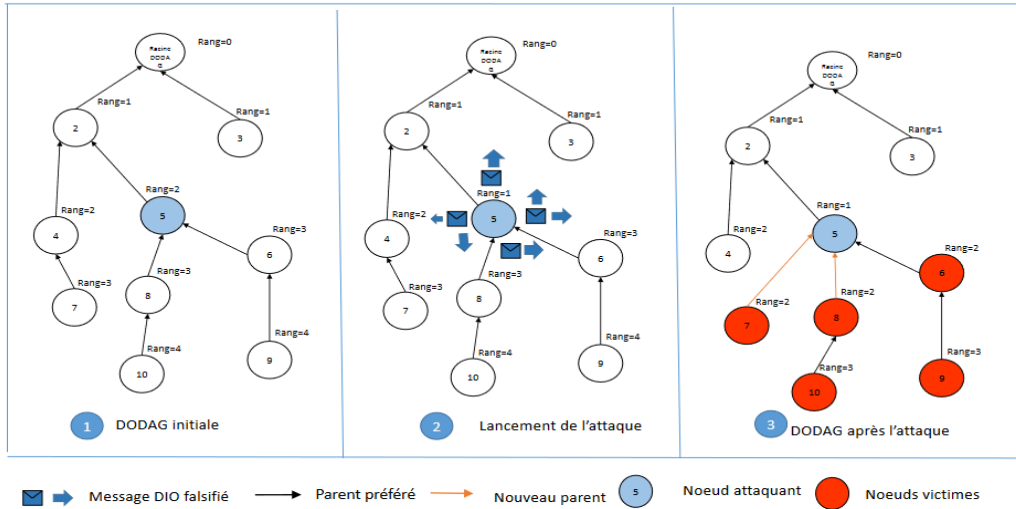


FIGURE 2.3.5 – Attaque par diminution du rang

2.3.6 Attaque Blackhole :

Black Hole attack est un type d'attaque qui peut survenir dans les réseaux de capteurs sans fil (WSN). Une attaque blackhole est une technique utilisée par un intrus malveillant pour supprimer tous les paquets qu'il est censé transmettre. Cette attaque peut causer des dommages considérables. Elle peut être considérée comme une forme d'attaque de déni de service. Si l'attaquant se trouve à une position stratégique dans le réseau, il peut isoler plusieurs nœuds, perturbant ainsi la connectivité. Il existe également une variante de cette attaque appelée trou gris (ou attaque d'expédition sélective) où l'attaquant se débarrasse sélectivement de certains paquets[10].

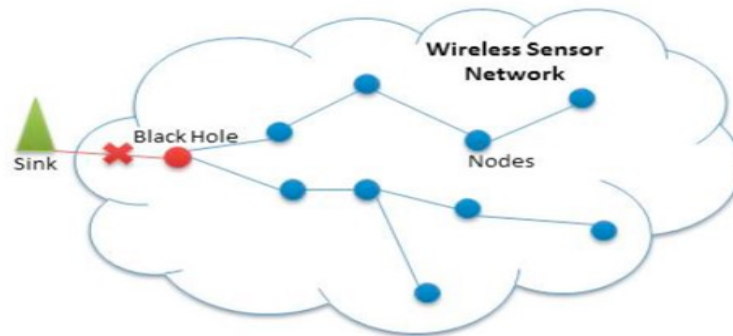


FIGURE 2.3.6 – Blackhole attack

Les attaques de type "Black Hole" sont dangereuses et perturbatrices pour les réseaux, créant des trous de routage et rendant certaines parties du réseau inaccessibles. Elles peuvent causer des perturbations dans les communications, entraîner des pertes de données et une baisse de la qualité de service. Ces attaques sont difficiles à détecter car les nœuds malveillants se font passer pour des routes valides. La prévention de ces

attaques est cruciale pour assurer l'intégrité, la disponibilité et la sécurité des réseaux, ainsi que pour protéger les utilisateurs contre les perturbations potentielles.

Pour tenter de repérer ces attaque, différents indicateurs peuvent être mis en évidence, tels que la consommation d'énergie, la fréquence des messages DIO et DAO, le taux de livraison des paquets. Ces indices permettent d'évaluer les conséquences néfastes de cette attaque sur les performances globales du réseau sans fil. En analysant ces mesures, il est possible de prendre conscience de l'ampleur des perturbations causées par une attaque blackhole et de développer des mécanismes de détection et de prévention plus efficaces pour renforcer la sécurité du réseau.

2.4 Contre-mesures :

Il existe plusieurs contre-mesures possibles pour se prémunir contre les attaques dans les réseaux LLN

2.4.1 Protection d'un réseau :

La protection d'un réseau utilisant le protocole RPL implique généralement la mise en place de mesures de protection à différents niveaux. Ces mesures peuvent être divisées en trois étapes principales pour assurer une sécurité optimale du réseau :

1. **Détection des attaques :** La première étape consiste à détecter les attaques potentielles contre le réseau RPL. Cela peut être réalisé en surveillant le trafic réseau à la recherche de signes de comportements malveillants ou en utilisant des outils de détection d'intrusion pour identifier les tentatives d'attaques.
2. **Prévention des attaques :** Une fois les menaces détectées, la deuxième étape consiste à mettre en place des mesures de prévention pour empêcher les attaques d'affecter le réseau. Cela peut inclure l'utilisation de pare-feu pour bloquer les tentatives d'intrusion, la mise en place de politiques de sécurité pour limiter l'accès au réseau et l'utilisation de protocoles de chiffrement pour protéger les données en transit.
3. **Réponse aux attaques :** La troisième étape consiste à élaborer un plan de réponse aux attaques afin de réduire les impacts en cas de violation de sécurité. Il est important d'avoir des procédures claires pour isoler les parties affectées du réseau, limiter l'exposition des données et restaurer le réseau à son état normal. Il est également important de mener des enquêtes sur les causes profondes des attaques pour améliorer la sécurité globale du réseau RPL.

2.4.2 Système de détection d'intrusion :

Un système de détection d'intrusion (IDS) est un dispositif de sécurité qui surveille le trafic réseau ou les événements système pour détecter toute activité suspecte ou malveillante. Le IDS peut détecter une variété de menaces telles que les attaques de déni de service, les tentatives d'intrusion, les malwares, les virus et les logiciels espions[11].

Il existe deux types de IDS : les systèmes de détection d'intrusion basés sur le réseau (NIDS) qui surveillent le trafic réseau et les systèmes de détection d'intrusion basés sur l'hôte (HIDS) qui surveillent les événements système sur une machine individuelle[12].

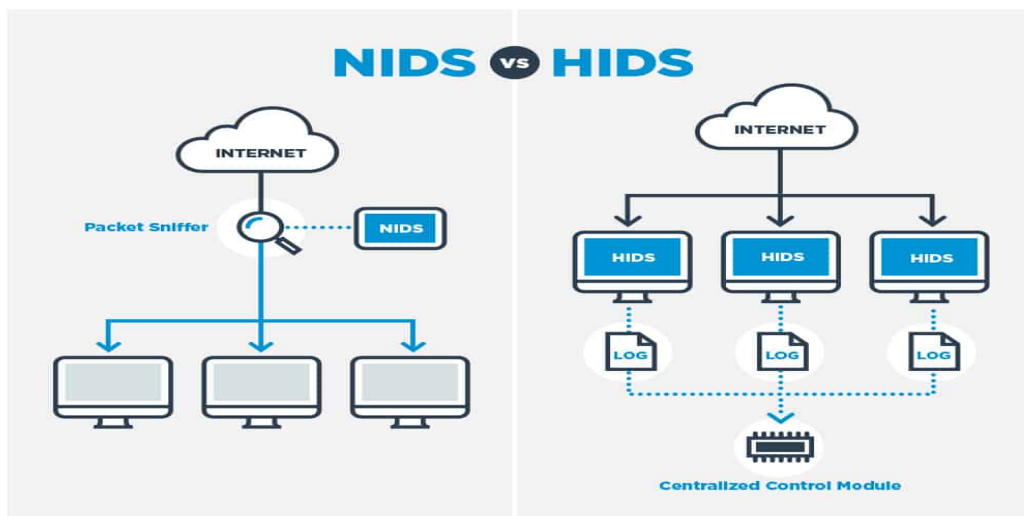


FIGURE 2.4.1 – NIDS -vs- HIDS

Les approches utilisées par les systèmes de détection d'intrusion (IDS) sont variées et dépendent des objectifs et des exigences de chaque système [12] :

1. Signature-based approach : Cette approche se base sur la comparaison des caractéristiques d'un trafic réseau avec une base de données de signatures d'attaques connues. Si une correspondance est trouvée, l'IDS peut générer une alerte ou bloquer le trafic suspecté.
2. Behavior-based approach : Cette approche se concentre sur la détection de comportements anormaux dans le trafic réseau, tels que des modèles de trafic inhabituels, des accès non autorisés, des tentatives de connexion répétées, etc. L'IDS peut utiliser des algorithmes d'apprentissage automatique pour apprendre le comportement normal du réseau et détecter les comportements anormaux.

2.5 Conclusion :

La sécurité des réseaux LNN est un enjeu crucial pour garantir leur bon fonctionnement et protéger les données qui y transitent. Les attaques peuvent être classées selon différents critères, tels que les comportements, les critères de sécurité et les éléments du réseau impactés. Les attaques de rang peuvent avoir un impact important sur la topologie du protocole RPL et nécessitent des contre-mesures appropriées, telles que la protection du réseau et la mise en place d'un système de détection d'intrusion. En somme, la sécurité des réseaux LNN doit être une préoccupation constante pour garantir leur fiabilité et leur sécurité.

Chapitre 3

Implémentation d'attaque BlackHole :

3.1 Introduction :

Le chapitre suivant porte sur l'implémentation d'attaques blackhole, un type d'attaque couramment utilisé dans les réseaux 6LowPAN pour détourner le trafic à des fins malveillantes. Cette attaque est particulièrement préoccupante dans les réseaux de capteurs sans fil, où la sécurité est essentielle pour garantir le bon fonctionnement de l'ensemble du système. L'objectif de ce chapitre est de fournir une compréhension approfondie de cette attaque et de ses conséquences potentiellement dangereuses. Nous discuterons également des différentes méthodes utilisées pour l'implémentation de cette attaque et de la façon dont elle peut être résolue et prévenue.

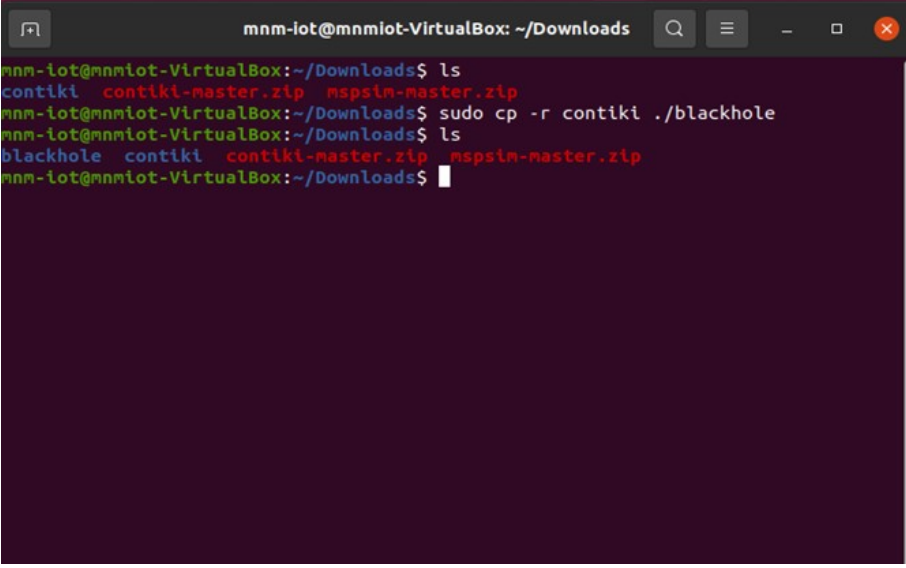
3.2 Implémentation d'attaque Blackhole sous contiki/cooja :

Prérequis.

- Système d'exploitation Linux.
- Contiki 3.0 installé sur l'ordinateur hôte.
- Fichier « uip6-attack.c ».
- Connaissance de base du fonctionnement de Contiki.

3.2.1 Configuration des fichiers :

- 1 - Cloner le dossier Contiki-3.0 (faire une copie) et Renommer le « blackhole »

A terminal window titled 'mnm-iot@mnm-iot-VirtualBox: ~/Downloads' with search, menu, and window control icons. The terminal shows the following commands and output:

```
mnm-iot@mnm-iot-VirtualBox:~/Downloads$ ls
contiki  contiki-master.zip  mspsim-master.zip
mnm-iot@mnm-iot-VirtualBox:~/Downloads$ sudo cp -r contiki ./blackhole
mnm-iot@mnm-iot-VirtualBox:~/Downloads$ ls
blackhole  contiki  contiki-master.zip  mspsim-master.zip
mnm-iot@mnm-iot-VirtualBox:~/Downloads$
```

FIGURE 3.2.1 – Configuration.1

- 2 - Télécharger uip6-attack.c à partir de ce lien : https://github.com/alifa2try/RPL_Attack_Files/blob/main/uip6-attack.c.
- 3 - Déplacez-le dans le dossier : blackhole/core/net/ipv6/
- 4 - Supprimez le fichier uip6.c et renommez uip6-attack.c en uip6.c

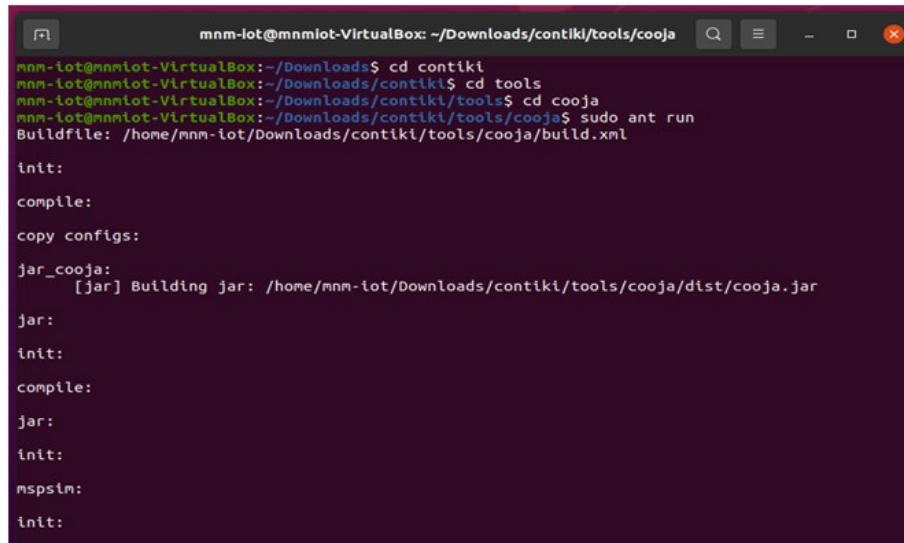
Le fichier, `uip6-attack.c`, est un fichier modifié qui implémente l'attaque blackhole. Les fonctions modifiées dans ce fichier sont principalement liées à la gestion des options RPL, telles que `rpl_verify_header()`, `rpl_process_parent_event()`, et `rpl_process_dio()`.

Les fonctions modifiées comprennent notamment :

- `uip_icmp6_send()` : Cette fonction est utilisée pour envoyer des paquets ICMPv6. Dans la version modifiée, cette fonction a été étendue pour inclure des fonctionnalités permettant d'envoyer des messages ICMPv6 malveillants tels que des paquets de redirection.
- `uip_rpl_input()` : Cette fonction est appelée lorsqu'un paquet RPL est reçu par un nœud du réseau.
- `uip_rpl_add_header()` : Cette fonction est utilisée pour ajouter un en-tête RPL à un paquet IPv6.

3.2.2 Implémentation sur Contiki :

1 - On démarre contiki3.0 :



```
mnm-lot@mnm-lot-VirtualBox: ~/Downloads/contiki/tools/cooja
mnm-lot@mnm-lot-VirtualBox:~/Downloads$ cd contiki
mnm-lot@mnm-lot-VirtualBox:~/Downloads/contiki$ cd tools
mnm-lot@mnm-lot-VirtualBox:~/Downloads/contiki/tools$ cd cooja
mnm-lot@mnm-lot-VirtualBox:~/Downloads/contiki/tools/cooja$ sudo ant run
Buildfile: /home/mnm-lot/Downloads/contiki/tools/cooja/build.xml

init:
compile:
copy configs:
jar_cooja:
[jar] Building jar: /home/mnm-lot/Downloads/contiki/tools/cooja/dist/cooja.jar
jar:
init:
compile:
jar:
init:
mcsim:
init:
```

FIGURE 3.2.2 – Contiki Cooja

2 - Créer une nouvelle simulation :

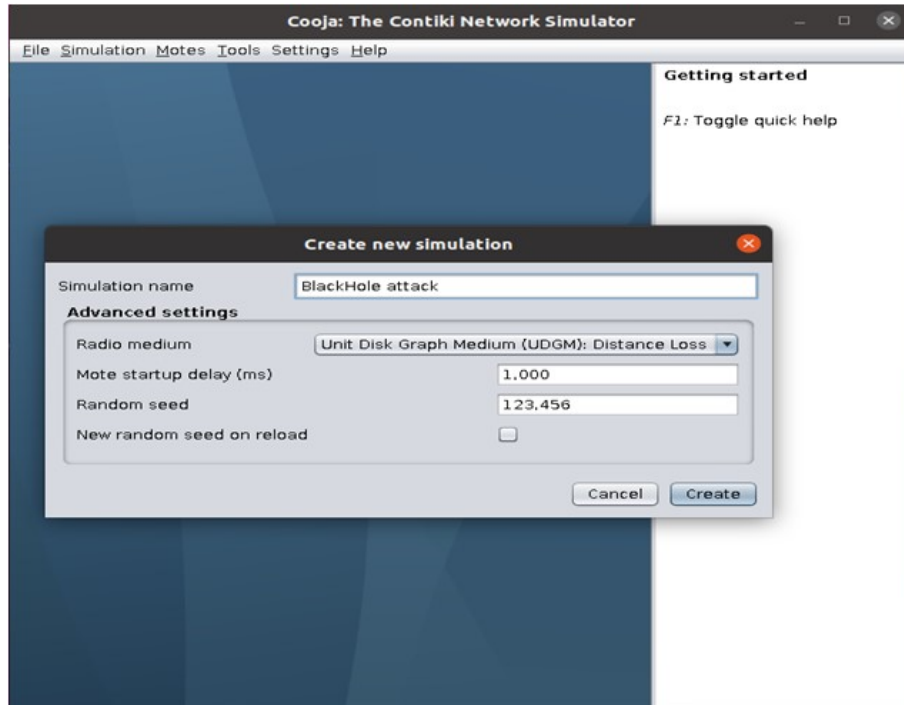


FIGURE 3.2.3 – Creation de la simulation

3 - Créer les nœuds :

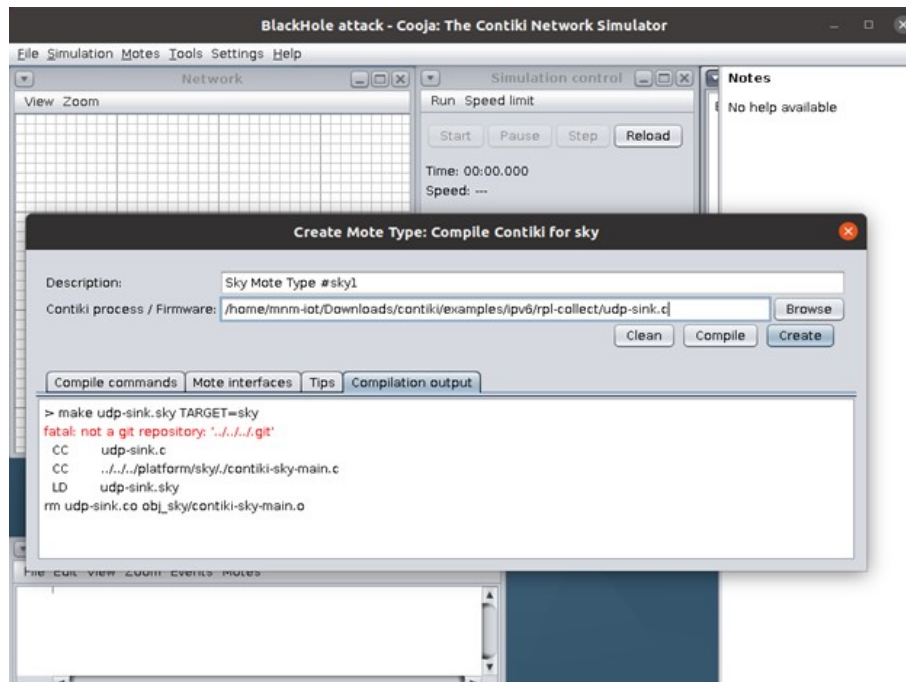


FIGURE 3.2.4 – Creation des noeuds

3.1 - Nœud udp-sink.c :

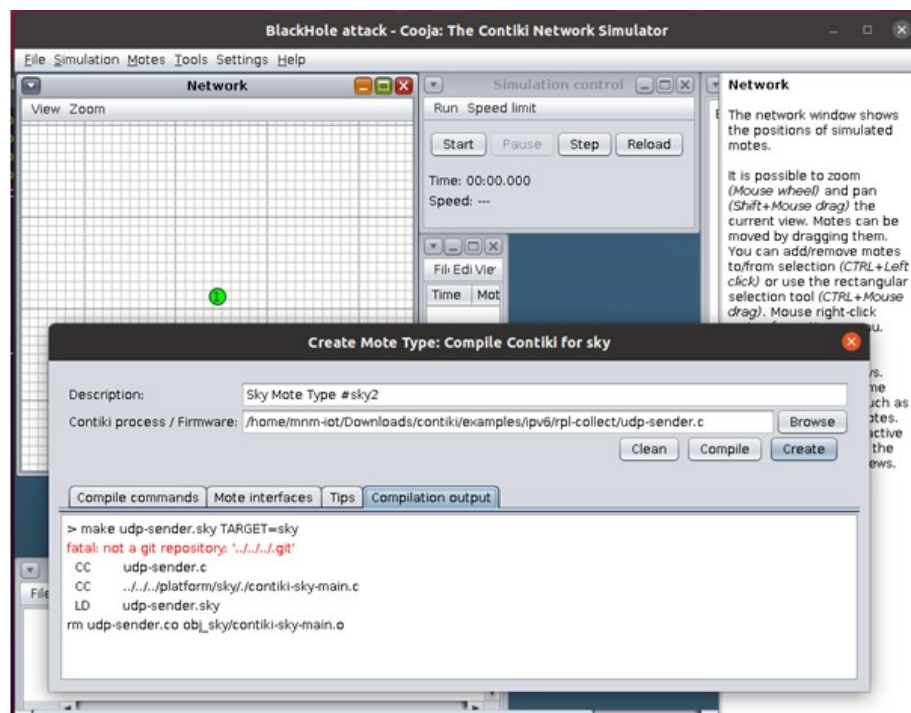


FIGURE 3.2.5 – Nœud udp-sink.c

3.2 - 9 Nœud udp-sender.c normales :

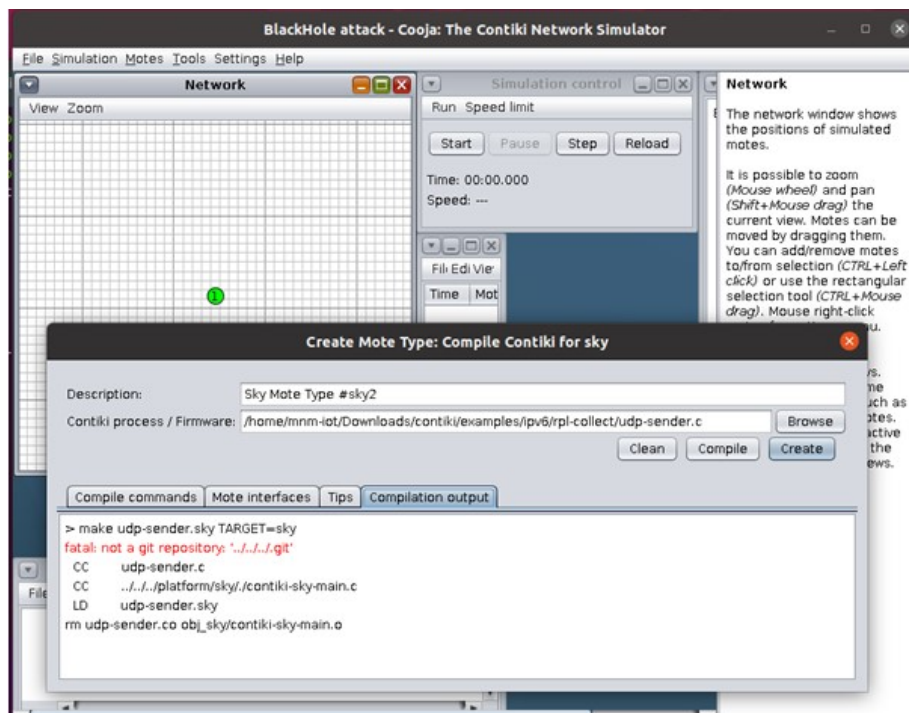


FIGURE 3.2.6 – Nœud udp-sender.c

3.3 - Nœud malicieux udp-sender.c depuis le dossier blackhole :

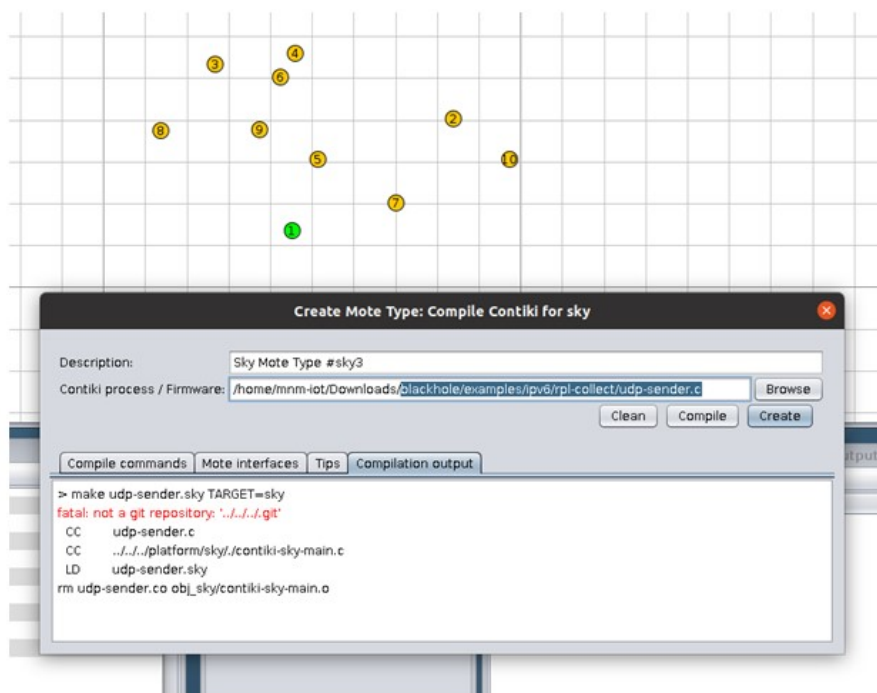


FIGURE 3.2.7 – Nœud malicieux Blackhole

4 - Positionnement des noeuds :

On ajuste le positionnement des noeuds (2,10) pour qu'il sont reliés seulement avec le noeud malicieux :

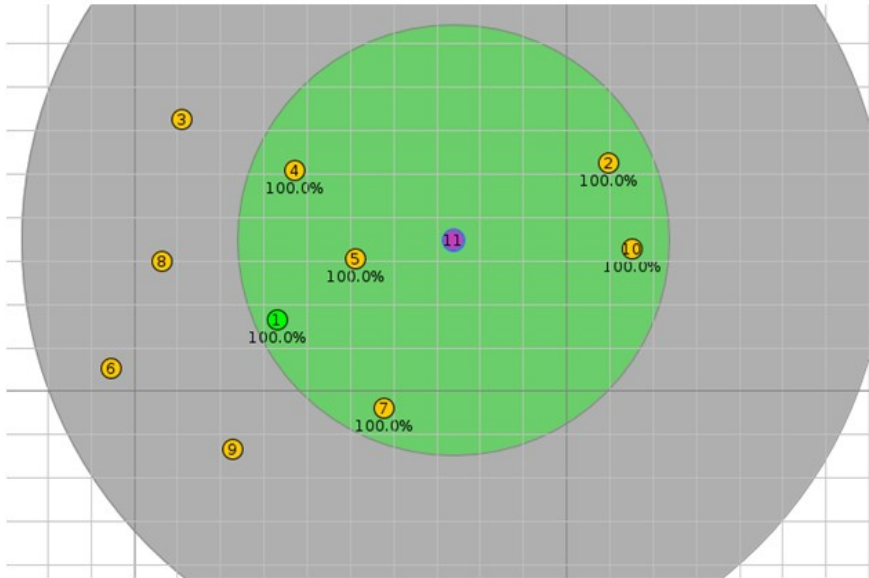


FIGURE 3.2.8 – Configuration du positionnement

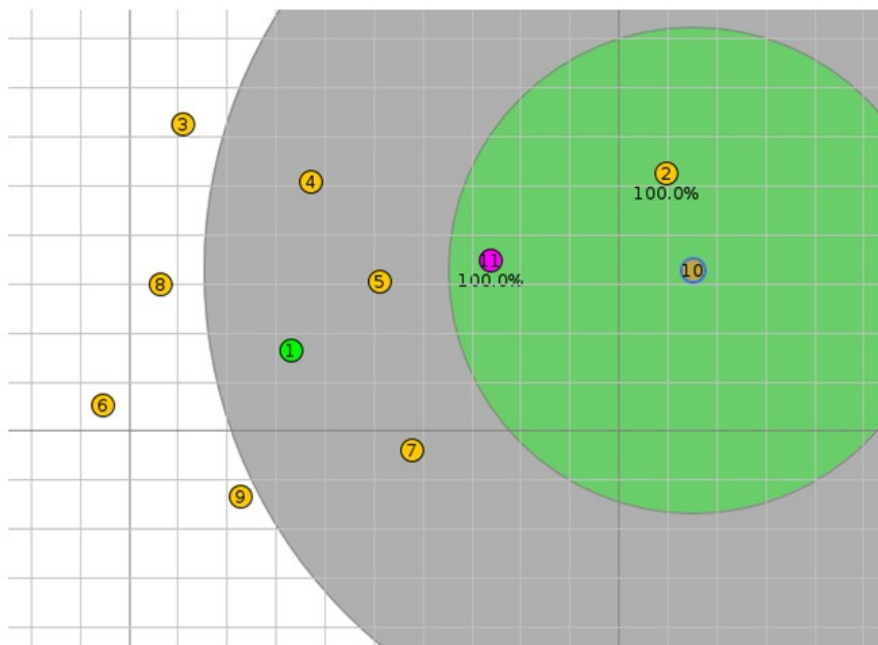


FIGURE 3.2.9 – Configuration du positionnement-2

5 - Lancer « collect-view » et commencer la stimulation :

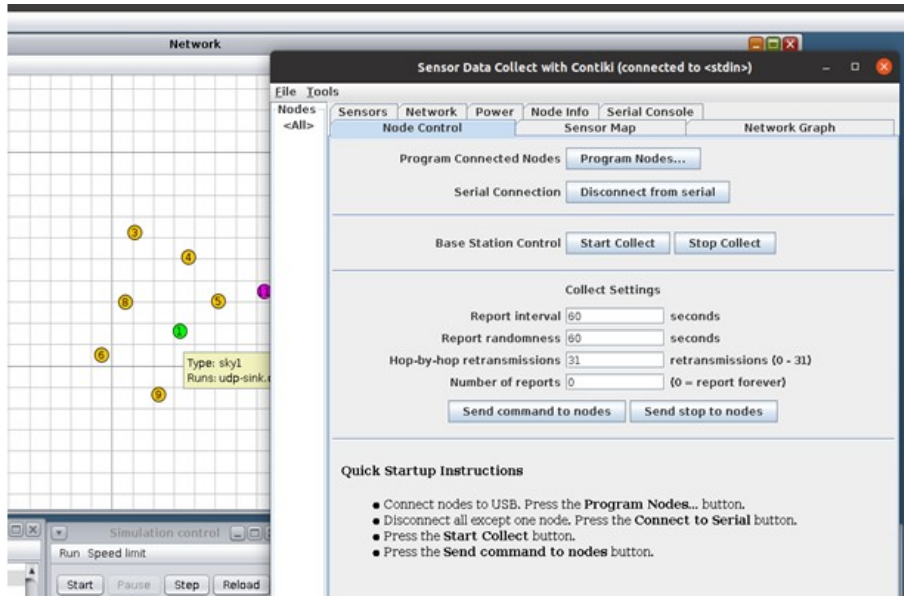


FIGURE 3.2.10 – Lancement du collect-View

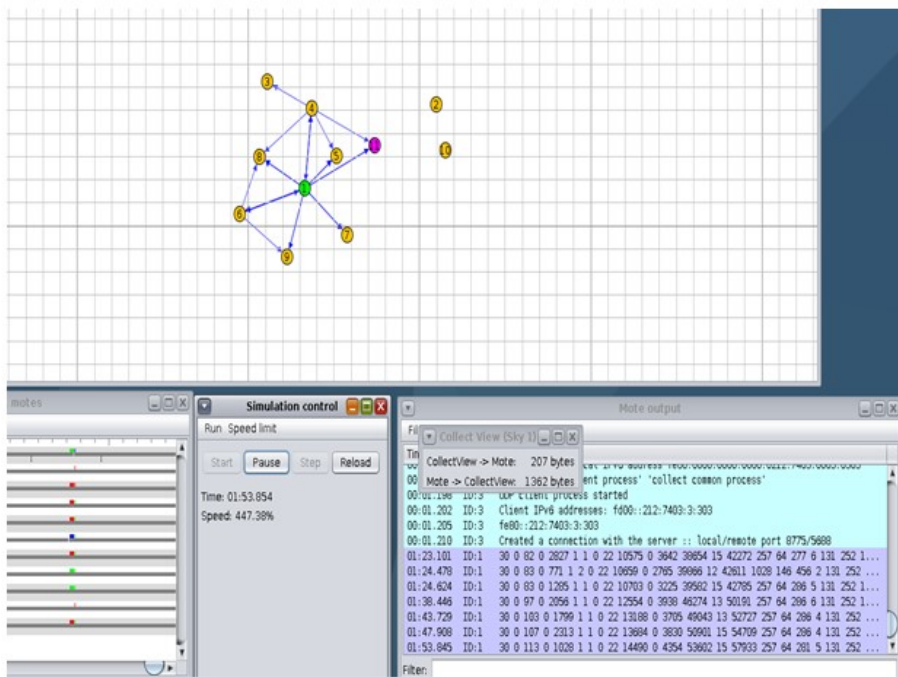


FIGURE 3.2.11 – Simulation Start

3.3 Evaluation du Rpl (avec et sans attaque) :

Pour évaluer l'impact de l'attaque sur un réseau RPL, nous avons effectué plusieurs simulations à l'aide de l'outil Cooja. Chaque simulation a été exécutée pendant une durée de 15 minutes. Au cours de ces simulations, nous avons modifié le nombre de nœuds du réseau, en testant différentes configurations comprenant 15, 25, 35 et 45 nœuds. Les

métriques pertinentes ont été mesurées et comparées entre les simulations avec et sans attaque, certains métriques ont été évaluées à l'aide de scripts Python que nous avons spécifiquement conçus pour cette tâche à l'aide des fichiers radiolog.pcap.

Cette approche comparative nous permettra d'analyser et de visualiser les différences des métriques, nous fournissant ainsi des informations précieuses sur l'impact de l'attaque sur le réseau RPL.

3.3.1 Throughput :

Le métrique Throughput fait référence à la quantité de données qui peuvent être transmises avec succès à travers le réseau par unité de temps. Il mesure l'efficacité du protocole RPL en termes de capacité de transfert de données.

Nous avons mesuré Throughput dans chaque scénario et représenté graphiquement les résultats obtenus.

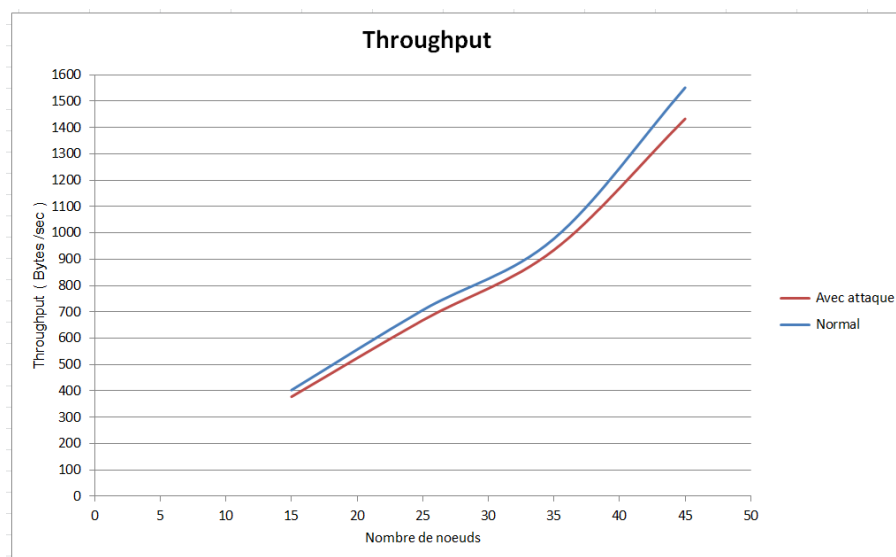


FIGURE 3.3.1 – Variation du throughput sans et avec attaque

On peut observer que dans tous les cas, le réseau RPL sans attaque (Normal) a un throughput légèrement supérieur à celui du réseau RPL avec attaque Blackhole (Avec-attaque) pour chaque configuration. Cela indique que l'attaque Blackhole affecte négativement le débit de données dans le réseau.

De plus, on peut remarquer que le throughput augmente généralement avec l'augmentation du nombre de nœuds dans les deux cas. Cependant, il convient de noter que les augmentations sont moins prononcées dans le réseau RPL avec attaque Blackhole par rapport au réseau RPL normal. Cela peut être attribué à la perturbation causée par l'attaque, qui entraîne une perte de données et une diminution de la qualité de service.

3.3.2 Convergence time :

le temps de convergence (convergence time) représente le temps requis pour qu'un nœud, qui peut être atteint par communication radio, fasse partie de la structure DAG[19]. Cependant, dans les réseaux sans fil, notamment ceux avec des nœuds mobiles et des liens peu fiables, le temps de convergence n'est pas fixe et peut varier.

Le temps de convergence dans un réseau RPL est déterminé par l'intervalle entre le premier DIO (DODAG Information Object) envoyé par le nœud client et le dernier DIO reçu pour rejoindre le DAG. Il peut être calculé à l'aide de l'équation mentionnée dans le paragraphe :

Temps de Convergence = Dernier DIO ayant rejoint le DAG - Premier DIO envoyé.

Nous avons calculé le temps de convergence dans chaque scénario et présenté les résultats graphiquement.

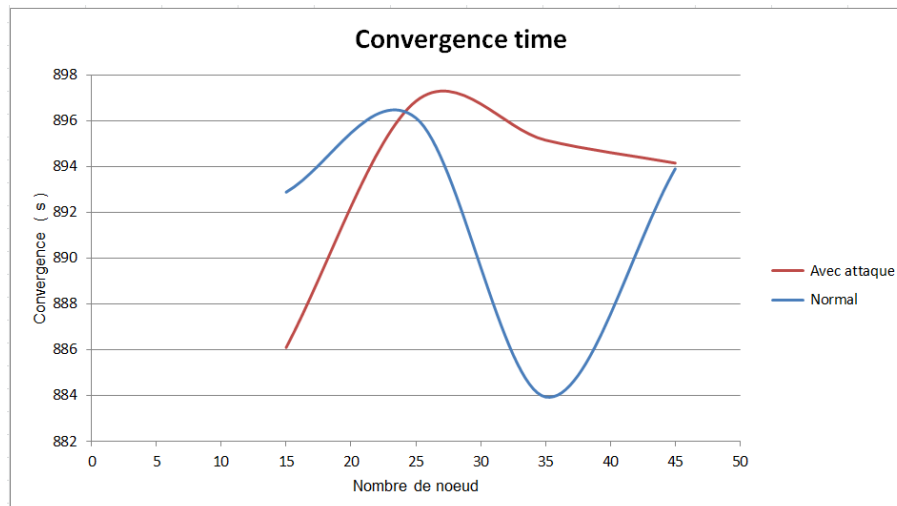


FIGURE 3.3.2 – Variation du Convergence time sans et avec attaque

Dans le scénario RPL normal, le temps de convergence était généralement court pour des densités faibles (15, 25 nœuds), mais il s'est légèrement allongé avec une augmentation de la densité (35, 45 nœuds). En revanche, dans le scénario RPL avec attaque blackhole, le temps de convergence a augmenté de manière significative à mesure que la densité augmentait, dépassant le temps de convergence du réseau normal, notamment pour les densités élevées, indiquant un impact négatif de l'attaque sur le processus de convergence.

Cette observation suggère l'attaque blackhole peut affecter le temps de convergence en introduisant de faux messages de routage qui trompent les nœuds voisins et rallongent le processus de formation du DAG. En conséquence, les nœuds peuvent mettre plus de temps à rejoindre le DAG et à établir une topologie de réseau stable.

3.3.3 Taux des paquets de contrôle :

Les messages de contrôle RPL, tels que les DIO et les DAO, jouent un rôle essentiel dans la gestion de la connectivité et du routage au sein d'un réseau. Les messages DIO sont utilisés pour annoncer la présence et les capacités des nœuds dans le réseau, tandis que les messages DAO sont utilisés pour propager les informations de routage et maintenir les chemins dans le réseau.

En mesurant et comparant le taux de ces messages entre un réseau RPL normal et un réseau RPL avec une attaque blackhole, nous pouvons obtenir des informations précieuses sur l'impact de l'attaque sur la communication et le fonctionnement du réseau.

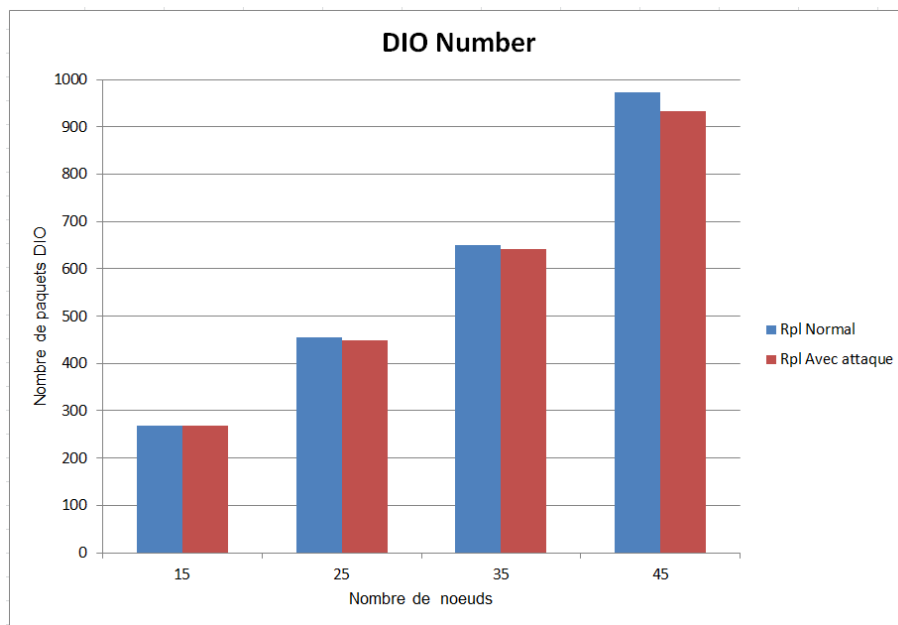


FIGURE 3.3.3 – taux des messages DIO sans et avec attaque

le taux des messages DIO entre un réseau RPL normal et un réseau RPL avec une attaque blackhole. Dans le réseau RPL normal, le taux de messages DIO varie de 269 à 974, en fonction du nombre de nœuds du réseau. En revanche, dans le réseau RPL avec attaque blackhole, le taux de messages DIO varie de 268 à 934. On observe une diminution légèrement plus marquée du taux de messages DIO dans le réseau avec attaque par rapport au réseau normal.

Cette différence peut être attribuée à l'effet de l'attaque blackhole sur la propagation des messages DIO. Lorsqu'un nœud malveillant effectue une attaque blackhole, il peut intercepter et absorber les paquets de routage, y compris les messages DIO. Cela peut entraîner une diminution du taux de messages DIO dans le réseau attaqué par rapport au réseau normal, où les messages sont transmis normalement.

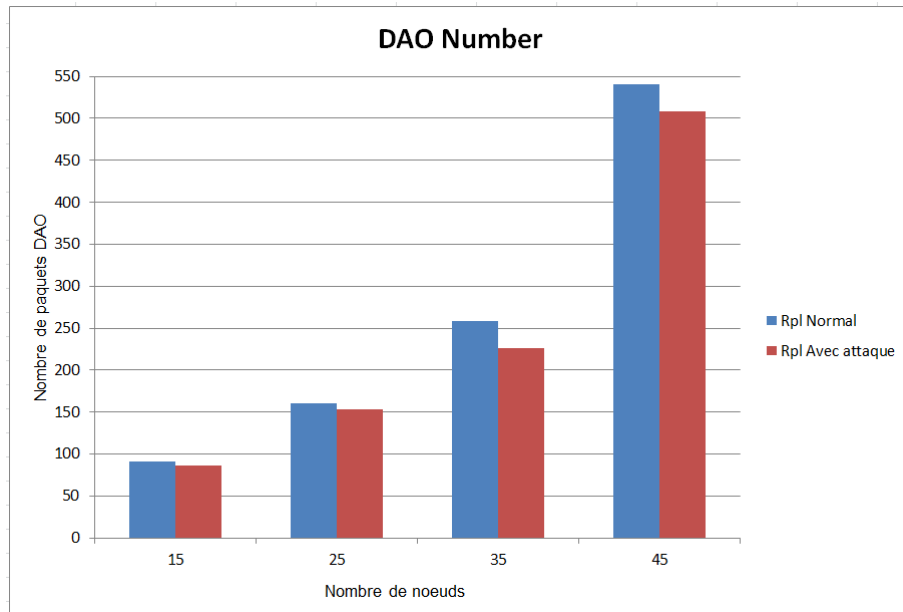


FIGURE 3.3.4 – taux des messages DAO sans et avec attaque

Pour les message DAO ,l'analyse met en évidence une disparité notable dans le taux de messages DAO entre un réseau RPL normal et un réseau RPL affecté par une attaque blackhole. Dans le réseau RPL normal, le taux de messages DAO varie de 91 à 541 en fonction du nombre de nœuds. En revanche, dans le réseau RPL avec attaque blackhole, le taux de messages DAO se situe entre 86 et 508. Cette différence significative souligne une nette diminution du taux de messages DAO dans le réseau touché par l'attaque, comparé au réseau normal.

L'origine de cette disparité réside dans l'impact néfaste de l'attaque blackhole sur la diffusion et la réception des messages de routage DAO. L'attaque blackhole perturbe la diffusion régulière des messages DAO, engendrant ainsi une réduction marquée du taux observé. Cette situation peut entraîner des problèmes de mise à jour et de stabilité des chemins de routage au sein du réseau, entraînant une dégradation de la fiabilité des communications entre les nœuds.

3.3.4 Consommation d'énergie :

La consommation d'énergie des nœuds RPL fait référence à la quantité d'énergie utilisée par chaque nœud du réseau pour exécuter les opérations de routage et de communication conformément au protocole RPL.

L'importance de la conservation d'énergie dans le protocole RPL pour les réseaux IoT est cruciale pour garantir le bon fonctionnement des dispositifs connectés[20]. Cette métrique mesure l'efficacité énergétique du réseau et sensible à des facteurs tels que la taille du réseau, le trafic de données et la présence d'attaques.

Nous avons mesuré la consommation d'énergie dans chaque scénario et représenté graphiquement les résultats obtenus.

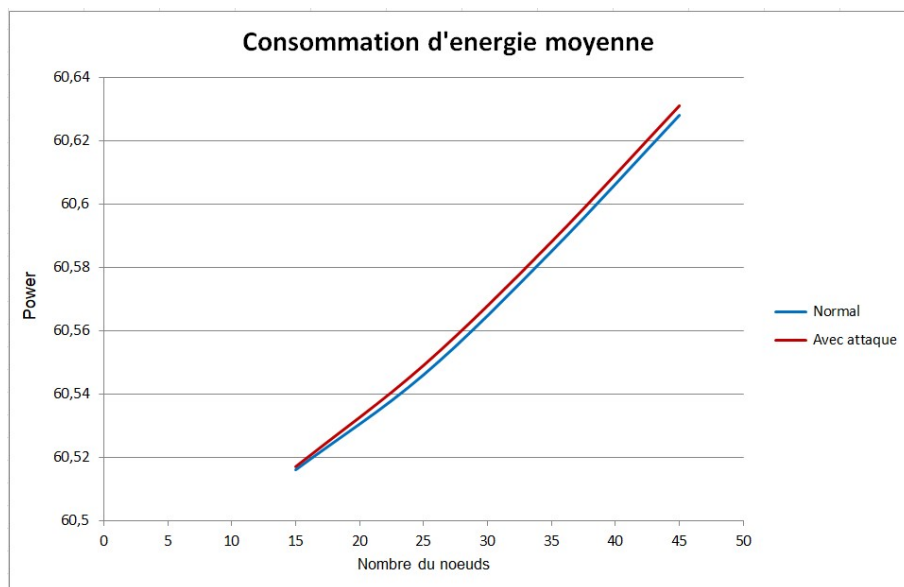


FIGURE 3.3.5 – Variation du consommation d'énergie sans et avec attaque

Les résultats obtenus pour la consommation d'énergie dans nos simulations révèlent une augmentation de la consommation dans les scénarios avec attaque par rapport à ceux sans attaque. Il est important de noter aussi que la consommation d'énergie augmente en fonction de la taille du réseau.

L'attaque blackhole entraîne une augmentation de la consommation d'énergie par rapport aux scénarios sans attaque. De plus, l'augmentation de la consommation d'énergie avec la taille du réseau est expliqué par la nécessité accrue de traiter les paquets de données et de maintenir la connectivité dans un réseau plus étendu.

3.4 Solution :

Dans le cadre de cette étude, basée sur les différentes métriques analysées telles que la consommation d'énergie, le throughput, le temps de convergence et le taux de messages DAO et DIO, nous proposons une approche visant à détecter et atténuer l'attaque blackhole dans un réseau RPL.

Notre approche repose sur l'utilisation de seuils prédéfinis pour le throughput et les messages DAO et DIO. En surveillant en temps réel ces métriques, nous pouvons détecter les anomalies potentielles causées par l'attaque blackhole. Lorsque les valeurs mesurées tombent en dessous des seuils définis, cela indique une possible présence de l'attaque.

Une fois qu'une détection est effectuée, notre approche propose plusieurs mesures d'atténuation. Tout d'abord, nous pouvons déclencher un mécanisme de rejet des messages provenant du nœud malveillant identifié. En bloquant ses messages DAO et DIO, nous réduisons l'impact de l'attaque sur le réseau.

De plus, nous recommandons d'effectuer une réinitialisation périodique des tables de routage et de reconfigurer le réseau en utilisant des mécanismes de découverte de route plus robustes. Cela permet de rétablir l'intégrité du réseau et d'assurer la continuité des communications.

En combinant ces mesures de détection et d'atténuation, notre approche offre une solution proactive pour contrer l'attaque blackhole dans un réseau RPL. Cependant, il convient de noter que cette approche doit être adaptée et optimisée en fonction des caractéristiques spécifiques du réseau et des scénarios d'utilisation. Des tests et validations supplémentaires sont nécessaires pour garantir son efficacité dans des environnements réels.

3.5 Conclusion :

Dans ce chapitre, nous avons réalisé une implémentation de l'attaque blackhole au sein d'un réseau RPL, suivie d'une analyse approfondie de ses conséquences. Les simulations que nous avons effectuées nous ont permis d'évaluer l'impact de cette attaque sur le fonctionnement du réseau RPL. Au cours de cette étude, nous avons examiné de près les métriques clés telles que la consommation d'énergie, le débit (throughput), le temps de convergence et le taux de messages de contrôle (DIO/DAO).

Les résultats obtenus ont mis en évidence les vulnérabilités potentielles du protocole RPL face à l'attaque blackhole. Il est donc essentiel d'adopter des stratégies de sécurité robustes pour contrer cette menace. En mettant en place de telles mesures, nous pourrions préserver l'intégrité des communications, assurer la disponibilité du réseau et garantir la confidentialité des données échangées.

Conclusion

Nous avons mené une étude approfondie sur la sécurité des réseaux IoT, en nous concentrant spécifiquement sur le protocole RPL et l'attaque blackhole. Cette étude met en évidence les vulnérabilités potentielles du protocole RPL face à l'attaque blackhole, soulignant ainsi l'importance de mettre en place des stratégies de sécurité robustes pour contrer cette menace. Les résultats obtenus nous permettent de mieux comprendre les effets de cette attaque sur le fonctionnement du réseau RPL, notamment en termes de dégradation du taux de livraison des paquets, de la convergence du réseau et de la consommation d'énergie.

Il est crucial de poursuivre les recherches dans ce domaine afin de développer des mécanismes de détection avancés et des contre-mesures efficaces pour renforcer la sécurité des réseaux IoT basés sur le protocole RPL. Ces mesures permettront de préserver l'intégrité des communications, la disponibilité du réseau et la confidentialité des données échangées.

En conclusion, notre étude souligne l'importance de prendre en compte les aspects de sécurité dans la conception et l'exploitation des réseaux IoT, en particulier ceux basés sur le protocole RPL. La protection contre les attaques, telles que l'attaque blackhole, constitue un enjeu majeur pour assurer le bon fonctionnement et la confiance dans ces réseaux.

Table des figures

1.2.1	Architecture de réseaux IoT	9
1.2.2	Fonctionnement de IOT	11
1.3.1	Champs d'un messageDIO	12
1.3.2	Messages de contrôle RPL	14
1.3.3	Construction du DODAG	15
1.3.4	Construction Du DODAG - Suite	15
2.3.1	Attack d'incohérence DAG	22
2.3.2	Version Number Attack	24
2.3.3	Attaque du pire parent	24
2.3.4	Attaque par augmentation du rang	25
2.3.5	Attaque par diminution du rang	26
2.3.6	Blackhole attack	26
2.4.1	NIDS -vs- HIDS	28
3.2.1	Configuration.1	31
3.2.2	Contiki Cooja	32
3.2.3	Creation de la simulation	32
3.2.4	Creation des noeuds	33
3.2.5	Noeud udp-sink.c	33
3.2.6	Noeud udp-sender.c	34
3.2.7	Noeud malicieux Blackhole	34
3.2.8	Configuration du positionnement	35
3.2.9	Configuration du positionnement-2	35
3.2.10	Lancement du collect-View	36
3.2.11	Simulation Start	36
3.3.1	Variation du throughput sans et avec attaque	37
3.3.2	Variation du Convergence time sans et avec attaque	38
3.3.3	taux des messages DIO sans et avec attaque	39
3.3.4	taux des messages DAO sans et avec attaque	40
3.3.5	Variation du consommation d'énergie sans et avec attaque	41

Liste des abréviations :

IoT : Internet of Things

LLN : Low Power and Lossy Network

WSN : Wireless Sensor Network

IPv6 : Internet Protocol version 6

RPL : Routing Protocol for Low-Power and Lossy Networks

DODAG : Destination Oriented Directed Acyclic Graph

DIO : DODAG Information Object

DIS : DODAG Information Solicitation

DAO : DODAG Advertisement Object

OF : Objective Function

OCP : Objective Code Point

OF0 : Objective Function Zero

MRHOF : Minimum Rank with Hysteresis Objective Function

ETX : Expected Transmission Count

IDS : Intrusion Detection System

NIDS : Network Intrusion Detection Systems

HIDS : Host Intrusion Detection Systems

Bibliographie

- [1] https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html?gclid=Cj0KCQjwk7ugBhDIARIsAGuvgPY4NOD2eC0hs81k_wcB
- [2] <https://iotindustriel.com/iot-iiot/architecture-iot-lessentiel-a-savoir/>
- [3] <https://www.sap.com/france/insights/what-is-iot-internet-of-things.html>
- [4] https://en.wikipedia.org/wiki/IPv6_Routing_Protocol_for_Low-Power_and_Lossy_Networks
- [5] <https://www.ietf.org/archive/id/draft-ietf-roll-rpl-13.html#RPLControlMessage>
- [6] T. Winter, Ed : IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012 URL : <https://www.rfc-editor.org/rfc/rfc6550>
- [7] THUBERT (P.) - Objective function zero for the routing protocol for low-power and lossy networks (RPL)
- [8] GNAWALI (O.) - The minimum rank with hysteresis objective function. <https://datatracker.ietf.org/doc/rfc6719/>
- [9] <https://www.rfc-editor.org/rfc/rfc6206#section-4.1>
- [10] RFC 6551[Ref.bib. :VASSEUR (J.)-Routing metrics used for path calculation in rpl]
- [11] Le, A. ; Loo, J. ; Lasebae, A. ; Vinel, A. ; Chen, Y. ; Chai, M. : The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sens. J. 13(10), 3685–3692 (2013)
- [12] Ismail Butun, Patrik Osterberg , and Houbing Song : Security of the Internet of Things : Vulnerabilities, Attacks and Countermeasures.
- [13] Ayzaud, A., Badonnel, R., Chrisment, I. : A Taxonomy of Attacks in RPL-based Internet of Things, International Journal of Network Security, 18(3), May 2016.
- [14] Anthéa Mayzaud, Anuj Sehgal, Rémi Badonnel, Isabelle Chrisment : Gestion de risques appliquée aux réseaux RPL, Dec 2014
- [15] Almusaylim, Z.A. ; Alhumam, A. ; Mansoor, W. ; Chatterjee, P. ; Jhanjhi, N. Z. : Detection and mitigation of RPL rank and version number attacks in smart Internet of Things (2020)
- [16] Hossein Keipour : Blackhole Attack Detection in Low-Power IoT Mesh Networks Using Machine Learning Algorithms, Faculty of Engineering, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden.
- [17] Shahid Raza , Linus Wallgren , Thiemo Voigt : SVELTE : Real-time intrusion detection in the Internet of Things.

- [18] Amrit Pal Singh and Manik Deep Singh, “Analysis of Host-Based and Network-Based Intrusion Detection System” I.J. Computer Network and Information Security (IJCNIS) vol. 6, No. 8, pp. 41-47, August 2014.
- [19] M.Asvial, A.Cracias, M.Asnoer Laagu, A.Setyo Arifin : Design and Analysis of Low Power and Lossy Network Routing System for Internet of Things Netwok. p :554
- [20] Zheng Min Wang et al 2018 J. Phys : Analysis of Energy Consumption and Topology of Routing Protocol for Low-Power and Lossy Networks