République Algérienne Démocratique et Populaire

Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida 1

Faculté des Sciences
Département d'informatique

MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME DE MASTER EN INFORMATIQUE

Thème :

Détection de l'attaques Sinkhole dans Les réseaux de capteur sans fil

Domaine : MI

Filière : Informatique

Option : Sécurité des Systèmes d'informations

Réalisé par :

Bahri Khadidja

Président : Mr. Mohamed Ould Khaoua

Examinateur : Mr. Ahmed Ould Aissa

Promoteur : Mr. Ahmed LOUAZANI

Co-Promoteur : Mr. Abdelkader Lamamri

Année universitaire : 2022/2023

REMERCIEMENTS

Mes remerciements tout d'abord ALLAH le Tout-Puissant de m'avoir donné le courage et la volonté pour réaliser ce mémoire.

Je remercie et témoignons ma reconnaissance à mon Promoteur : **Mr. Ahmed LOUZANI**, de leurs orientations, leurs précieux conseils, leurs soutiens constants et leurs aides qui mes permis de mener à bien ce travail.

Mes remerciements s'adressent également aux membres du jury pour avoir accepté d'examiner et de porter leur jugement sur mon travail.

Mes vifs remerciements à ma chère mère pour tous ses encouragements.

Mes vifs remerciements à tous mes amis « Ikrem,Nora,Malika… » qui me soutenues et encouragées au cours de la réalisation de ce modeste travail.

Dédicaces

Je dédie ce modeste travail :

À mon professeur de mémoire Mr. Ahmed Louzani, pour leurs suivis, leurs soutiens,

À mes chers parents, pour tous leurs amours, leurs patiences, leurs grands sacrifices et leurs soutiens tout au long de mes études,

À mes chères sœurs pour leurs encouragements permanents, et leur soutien moral,

À mes chers frères pour son appui et ses encouragements,

À toute ma famille qui m'a donné de l'amour et de la vivacité,

À mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

Khadidja

Résumé

Les contraintes limitantes sur les nœuds de capteurs sans fil sont leurs caractéristiques, notamment la faible mémoire, la faible puissance de calcul, la nature de la communication par canal, l'hostilité de l'environnement de déploiement et la faible capacité énergétique. Ces contraintes physiques rendent le réseau vulnérable à plusieurs attaques.

L'attaque Sinkhole en fait partie, où les nœuds infectés attirent le trafic réseau en émettant leurs fausses mises à jour de routage. L'un des effets de l'attaque sinkhole est qu'elle peut être utilisée pour lancer d'autres attaques, telles que des attaques de transfert sélectif, des attaques d'usurpation d'identité et la perte ou la modification d'informations de routage. Il peut également être utilisé pour envoyer de fausses informations aux stations de base.

Dans notre mémoire, nous proposons une stratégie de détection basée sur IDS avec des algorithmes dédiés capables de détecter l'attaque sinkhole sous le protocole AODV et identifier les nœuds malveillants à l'origine de l'attaque sinkhole. Les résultats de la simulation montrent que l'approche proposée défend de manière fiable l'attaque sinkhole dans les RCSFs.

Mots-clés : Réseau de capteurs sans fil, sécurité du réseau, attaque Sinkhole, système de détection d'intrusion (IDS).

Abstract

The limitations constraints of the wireless sensor node are their characteristics which include low memory, low computation power, canal communication nature, the deployment environment hostility, and low energy capabilities. These physicals` limitation makes such network vulnerable to several attacks.

Sinkhole attack is one of them were compromised node attracts network traffic by advertise its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information. It can also use to send false information to the base station.

In our thesis, we propose a detection strategy based on IDS with dedicated algorithms capable of detecting the attack and identifying the malicious nodes at the origin of the sinkhole attack. The simulation results show that the proposed approach reliably defends the sinkhole attack in RCSFs.

Keywords: Wireless Sensors Network, Network Security, Sinkhole attack, Ns2 simulator, Intrusion detection system (IDS).

ملخص

ينطوي مفهوم القيود لعقد أجهزة الاستشعار اللاسلكية في خصائصها، بما في ذلك الذاكرة المنخفضة، وقوة الحوسبة المنخفضة، وطبيعة الاتصال لكل قناة، وعداء بيئة النشر، وقدرة منخفضة للطاقة. تجعل هذه القيود المادية الشبكة عرضة للعديد من الهجمات.

يعد هجوم Sinkhole أحد هذه الهجمات، حيث تقوم العقد المصابة بإيقاع حركة مرور الشبكة عن طريق إصدار تحديثات التوجيه المزيفة الخاصة بها. أحد آثار هجوم Sinkhole هو أنه يمكن استخدامه لشن هجمات أخرى، مثل هجمات إعادة التوجيه الانتقائية وهجمات الانتحال وفقدان معلومات المستخدم أو تعديلها. التوجيه. يمكن استخدامه أيضًا لإرسال معلومات خاطئة إلى المحطات الأساسية.

في هذه الأطروحة، نقترح استراتيجية كشف تعتمد على نظام كشف التسلل (IDS) مع خوارزميات مخصصة قادرة على اكتشاف الهجوم وتحديد العقد الخبيثة في أصل هجوم المجرى. تظهر نتائج المحاكاة أن النهج المقترح يدافع بشكل موثوق عن هجوم المجرى في. RCSFs

الكلمات المفتاحية: أجهزة الاستشعار اللاسلكية، أمن الشبكة، هجومSinkhole، برنامج المحاكات Ns2، نظام كشف التسلل . (IDS)

Table des matières

Chapitre II : Sécurité dans les réseaux de capteur sans fil

Chapitre III : Proposition de l'approach

Chapitre VI : Modélisation de l'approche

Conclusion générale

Perspectives

Bibliographie

Liste des figures

Liste des Tableaux

Introduction générale

Ces dernières années, les chercheurs se sont de plus en plus intéressés au domaine de recherche sur les Réseaux de capteurs sans fil (RCSF), en raison de sa large diffusion dans de nombreux domaines de la vie, tels que le domaine public et militaire, le monitoring médical, la surveillance dans les environnements hostiles, l'Agriculture de précision ...etc.

Donc il se trouve dans les rues, dans les maisons, dans les bureaux, dans la voiture, aux frontières d'un pays, sous l'eau, dans les barrages et dans les forêts, qui génèrent des informations (de surveillance, de commande, etc.) et nécessitent des protocoles pour assurer leur organisation et sécurisation pour l'améliorent la vie quotidienne des personnes. [1]

Les réseaux de capteurs sans fil se composent de milliers de minuscules nœuds de capteurs à faible coût et à faible consommation d'énergie avec des ressources limitées à des fins de surveillance. Les RCSFs sont utilisés pour surveiller les conditions environnementales telles que la température, la pression et d'autres conditions atmosphériques. Par conséquent, un réseau de capteurs sans fil est un ensemble de petits appareils qui permettent de faire fonctionner des appareils tels que des actionneurs, des moteurs et des commutateurs qui contrôlent les conditions et offre une communication fiable des données détectées. [1]

En raison de la petite taille et du grand nombre de ces nœuds de capteurs, ces réseaux sont vulnérables aux différente attaques. Il peut y avoir de nombreux types d'attaques sur les réseaux de capteurs sans fil, telles que l'attaque sinkhole, l'attaque par trou noir, l'attaque DOS, le brouillage, etc. [1]

L'attaque sinkhole est l'une des attaques de routage les plus destructrices. Le problème avec les attaques sinkhole est qu'un nœud compromis ou malveillant annonce des informations de routage attrayantes et force les nœuds à lui acheminer des données et crée une sphère d'influence. Par conséquent, une attaque sinkhole est une attaque qui dégrade les performances du réseau. De nombreuses attaques telles que l'écoute clandestine, le transfert sélectif et les trous noirs, etc. peuvent être renforcées par l'attaque sinkhole.[1]

Le protocole AODV (Ad-hoc On-demand Distance Vector) est un protocole de routage réactif, ce qui signifie que la route vers la destination n'est établie qu'en cas de besoin, est considéré comme un protocole de routage léger pour les RCSF et les réseaux ad hoc,

Le protocole AODV est largement utilisé dans les environnements où la topologie du réseau change fréquemment ou lorsque des nœuds se joignent ou quittent le réseau de manière dynamique. Il permet d'établir des routes de manière efficace tout en minimisant la surcharge du réseau et en prenant en compte les contraintes de ressources des nœuds mobiles.

Le fonctionnement du protocole AODV repose sur la notion de demande de routage à la demande. Lorsqu'un nœud a besoin d'envoyer des données à une destination pour laquelle il n'a pas de route préétablie « un protocole de routage réactif » ce qui signifie que la route vers la destination n'est établie qu'en cas de besoin.

Ce mémoire est structuré en quatre chapitres comme suit :

Chapitre 1 : Est consacré à la présentation des Réseaux de capteur sans fil et leurs principaux caractéristiques, leurs Architectures, ainsi que leurs différents domaines d'applications.

Chapitre 2 : Est une présentation de la sécurité de cette technologie, ses principaux concepts, ses fonctionnements et les mesures de sécurité.

Chapitre 3 : Est une étude de l'attaque Sinkhole dans le protocole AODV et une présentation de notre approche contre cette attaque.

Chapitre 4 : Est une modélisation de notre approche proposée sous l'outil **tina (Time Petri Net Analyzer)**.

Nous terminons notre mémoire par une conclusion générale, ainsi que quelques perspectives pour des travaux futurs.

Objectif :

Le but de ce mémoire est de détecter les attaques sinkhole sous le protocole AODV dans les réseaux de capteurs sans fil.

Problématique :

Dans ce mémoire, nous étudierons l'attaque sinkhole, les techniques existantes pour la détection de cette attaque, puis nous proposerons et implémenterons une approche légère (lightweight en anglais) et efficace pour contrer l'attaque sinkhole.

1.Introduction

Les réseaux de capteurs sans fil (RCSF[1]) est une technologie émergente en raison de sa large gamme d'applications dans le domaine public et militaire, tel que le monitoring médical, la surveillance dans les environnements hostiles, l'Agriculture de précision ...etc. Ces réseaux de capteurs se composent de milliers de petits nœuds de capteurs avec des ressources limitées avec une station de base et des nœuds de capteurs à faible coût et faible puissance qui sont utilisés à des fins de surveillance. [1]

Dans ce premier chapitre, nous présentons les Réseau de capteur sans fil, leurs définitions et concepts fondamentaux, nous définissons aussi leur architecture et composants. Nous aborderons également les domaines d'application des RCSF et les défit face à la conception d'un RCSF, et nous terminons notre chapitre par une conclusion.

2.Définitions et concepts fondamentaux

2.1 Types des réseaux sans fil

I. Réseau ad hoc

Un réseau sans fil Adhoc ou WANET (Wireless Adhoc Network) est un type de réseau sans fil décentralisé[2], autoconfiguration et dynamique[3] dans lequel les nœuds sont libres de se déplacer.[2]

Un réseau ad hoc ne repose pas sur une infrastructure préexistante, telle que des routeurs dans un réseau câblé ou des points d'accès dans un réseau sans fil géré. Au lieu de cela, chaque nœud participe au routage en transmettant des données à d'autres nœuds, de sorte que les nœuds transmettant des données sont sélectionnés dynamiquement en fonction de la connectivité du réseau et de l'algorithme de routage utilisé. [2]

II. Réseau Manet

Le "réseau MANET" est un type particulier de réseau ad hoc, qui est un réseau sans fil dans lequel les nœuds se connectent de manière dynamique et autonome sans l'aide d'une infrastructure de réseau préexistante. Les nœuds d'un réseau MANET peuvent être des ordinateurs portables, des smartphones, des tablettes, des capteurs sans fil, des drones ou tout autre appareil mobile capable de communiquer sans fil.

Dans un réseau MANET, chaque nœud peut agir comme un nœud d'envoi et de réception. Les nœuds communiquent directement entre eux à l'aide d'une technique appelée routage ad

[1] **RCSF :** Réseau de Capteur Sans Fil.
[2] **Décentralisé :** les opérations pour la découverte et la maintenance du réseau se font localement par chaque nœud « chaque nœud est un routeur » (autoorganisé).
[3] **Dynamique :** les nœuds de capteur sont libres de se déplacer par rapport aux topologies du réseau.

hoc[4]. Les nœuds peuvent également servir de relais, retransmettant les paquets aux nœuds hors de portée.

Donc, un réseau MANET est un type spécifique de réseau ad hoc tous les réseaux MANET sont des réseaux ad hoc, mais tous les réseaux ad hoc ne sont pas nécessairement des réseaux MANET. En résumé, la principale différence entre les réseaux ad hoc et les MANET réside dans la mobilité des nœuds, la taille et la complexité des réseaux, ainsi que dans les cas d'utilisation et les applications spécifiques pour lesquels ils sont conçus. « Https://chat.openai.com/chat »

III. Réseau RCSF

Les réseaux de capteurs sans fil, sont des réseaux ad hoc où les nœuds incluent des capteurs à des fins de surveillance, par exemple de température...etc. Ce sont d'autres applications très importantes dans plusieurs domaines. [3]

IV. Discussion

Tableau 1:Tableaux comparative Adhoc vs Manet vs RCSF.

Caractéristiques	**Adhoc**	**Manet**	**RCSF**
Création	Début des années 70.	A partir des années 90.	1994.
Lancé par	Le département de la défense américaine DARPA.	Le groupe de travail MANET.	Récents progrès des techniques sans-fil.
Vulnérabilité aux attaques	Élevé.	Élevé.	Très élevé.
Nombre de nœud	Petit.	Petit.	Très grand.
Mode de communication	Point au Point.	Point au Point.	Emission.
Consommation d'énergie	Bas, puisque les dispositifs peuvent être rechargés.	Bas, puisque les dispositifs peuvent être rechargés.	Très haut, puisque les dispositifs ne peuvent pas être rechargés.
Coût	A moindre coût (car Le déploiement d'un réseau Ad Hoc ne nécessite pas d'installer des stations de base).	A moindre coût (car Le déploiement d'un réseau Manet ne nécessite pas d'installer des stations de base).	Coût Très élevé. (Car Les nœuds de capteur sont très chers).

[4] **Le routage ad hoc :** les nœuds transmettent des paquets de données les uns aux autres pour atteindre une destination spécifique.

2.2 Réseau de capteurs sans fil

I. Définition

Un réseau de capteurs sans fil (RCSF) est un réseau qui se compose de petits dispositifs sans fil coopérants indépendants (nœuds) qui sont capables de collecter et de transmettre des données de manière autonome. Les emplacements de ces nœuds ne sont pas nécessairement prédéterminés. Ils peuvent être répartis aléatoirement sur une zone géographique dite zone d'intérêt. [3]

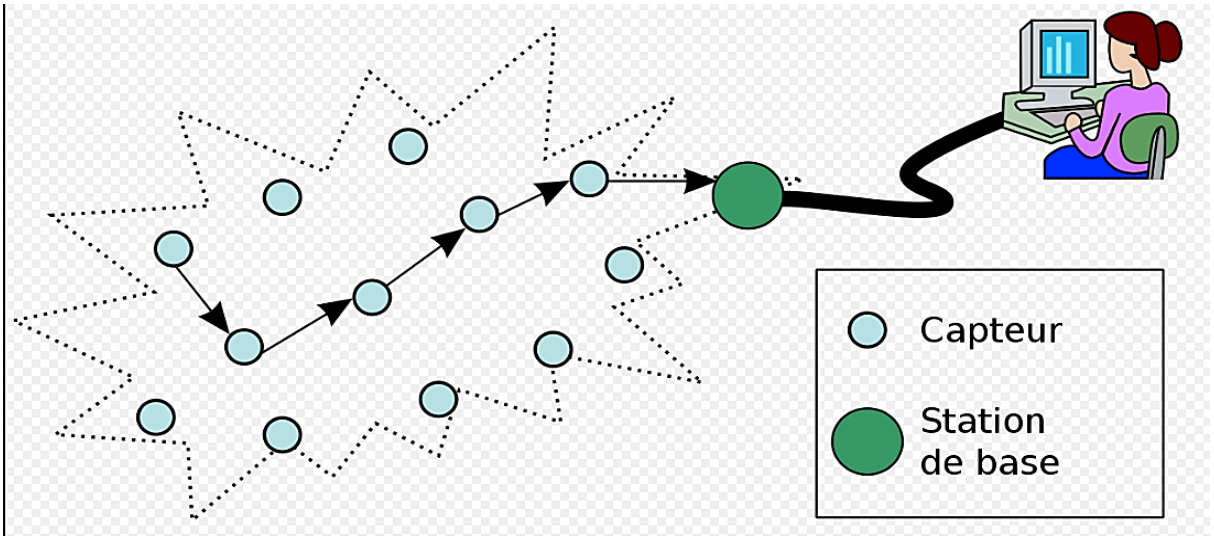


Figure 1:*Réseau de capteur sans fil. [3]*

II. Domaines d'application des RCSF

- **Application environnementale :** détection de feu des forêts, surveillance des tremblements de terre, détection des inondations, surveillance automatique des habitats écologiques agricoles, etc. [4]
- **Applications militaires :** surveillance des équipements, surveillance du champ de bataille, détection d'attaques nucléaires, biologiques et chimiques, suivi de cible, surveillance de l'ennemi, etc. [4]
- **Applications santé :** suivi à distance des données physiologiques pour la prévention des maladies, etc. [4]
- **Applications domicile :** sécurité maison, détection incendie, Gaz(co1) etc. [4]
- **Applications commerciales :** surveillance environnementale de bâtiments industriels et bureaux, Suivi de véhicules, Détection de réseaux industriels et commerciaux, Surveillance des flux de trafic, etc. [4]

III. Architecture et composants d'un Nœud de capteur

1) Matériel :

- **Processeur** : qui est le responsable des tâches de calcul sur les dispositifs RCSF comprennent le traitement des informations détectées localement ainsi que des informations fournies par d'autres nœuds de capteurs. [4]
- **Mémoire/stockage** : pour le stockage, à la fois la mémoire programme (la mémoire du jeu d'instructions du processeur) et la mémoire de données (utilisée pour stocker les données de mesure et d'autres informations locales, telles que les positions des nœuds), la taille de la mémoire est généralement limitée pour des raisons économiques. [4]
- **Émetteur-récepteur radio** : les appareils RCSF comprennent des radios à faible bande passante et à courte portée (10-100 kbps, <100 m). La communication radio est généralement l'opération la plus gourmande en énergie dans un appareil RCSF, de sorte que la radio doit utiliser des modes de veille et de réveil économes en énergie. [4]
- **Capteurs avec unité ADC** : en raison des contraintes d'alimentation et de bande passante, les périphériques RCSF ne prennent généralement en charge que la détection de faible débit de données. Dans de nombreuses applications, la détection multimodale est requise, de sorte que chaque appareil peut avoir plusieurs capteurs. Le capteur spécifique utilisé est basé sur l'application. L'unité de conversion analogique-numérique convertit le signal analogique fourni par le capteur en un signal numérique qui peut être traité par l'unité de traitement. [4]
- **Source d'alimentation** : habituellement, la source d'alimentation est une petite batterie ni rechargeable ni remplaçable. Cependant, dans certaines applications, quelques nœuds peuvent être reliés à une source d'énergie continue ou des techniques de récolte d'énergie peuvent fournir une petite quantité d'énergie renouvelée (les cellules solaires). [4]

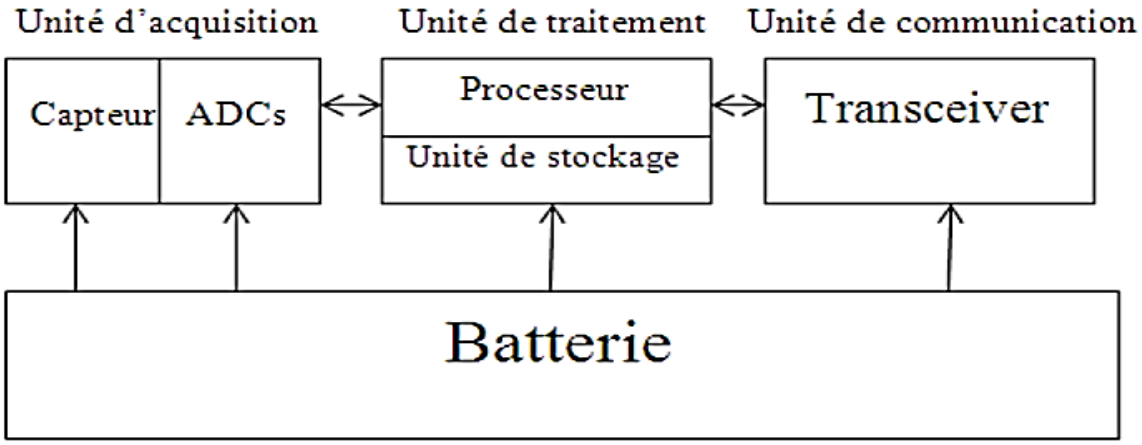


***Figure 2**:les composant matériel d'un nœud de capteur. [5]*

2) Logiciel :

- **Microcode de système d'exploitation** : également appelé middleware. Il représente le code, qui est utilisé par les modules logiciels de haut niveau pour soutenir une variété de fonctions. Le middleware couvre également le logiciel à partir de la fonctionnalité au niveau de la machine du microprocesseur tel que (TinyOS). [4]

- **Pilotes de capteurs** : sont des modules logiciels qui gèrent les fonctions de base des émetteurs-récepteurs de capteurs. Selon le type de capteur, ils parviennent à y charger la configuration et les paramètres appropriés. [4]
- **Processeurs de communication** : le processeur de communication gère les fonctions de communication, notamment le routage, la mise en mémoire tampon et le transfert de paquets, la maintenance de la topologie, le contrôle d'accès au support et le cryptage. [4]
- **Pilotes de communication** : ces modules logiciels exploitent les détails de la liaison de transmission du canal radio, y compris l'horlogerie et la synchronisation, l'encodage du signal, la récupération des bits, le comptage des bits, les niveaux de signal et la modulation. [4]
- **Mini-applications de traitement des données Applications de base** : traitement des données, stockage et manipulation de la valeur du signal, etc. Elles sont prises en charge au niveau du nœud pour le traitement en réseau. [4]

IV. Architecture et composants d'un RCSF

Le réseau de capteur sans fil (RCSF) est composé d'un ensemble de nœuds de capteurs. Ces nœuds de capteurs sont organisés en champs « sensor Fields ». Chacun de ces nœuds à la capacité de collecter des données et de les transférer au nœud passerelle (dit "sink" en anglais ou puits) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par Internet ou par satellite à l'ordinateur central « Gestionnaire de tâches » pour analyser ces données et prendre des décisions. [3]

V. Pile protocolaire

Nous réduisons les sept couches traditionnelles du modèle Open System InterConnect (OSI) à cinq couches : Physique, Liaison de données, Couche réseau, Couche transport et Couche présentation. La figure 3 représente le rôle de chaque couche.

- **Plan de gestion d'énergie :** Gérer l'énergie consommée par les capteurs, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un nœud voisin afin d'éviter la réception des messages dupliqués. De plus, quand un nœud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage, et conserver l'énergie restante aux fonctionnalités de captage. [5]
- **Plan de gestion de mobilité :** Ce niveau détecte et enregistre tous les mouvements des nœuds capteurs, d'une manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les nœuds voisins, cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie. [5]

- **Plan de gestion des tâches :** Lors d'une opération de capture dans une région donnée, les nœuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme. Cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau afin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, et par conséquent, prolonger la durée de vie du réseau. [5]

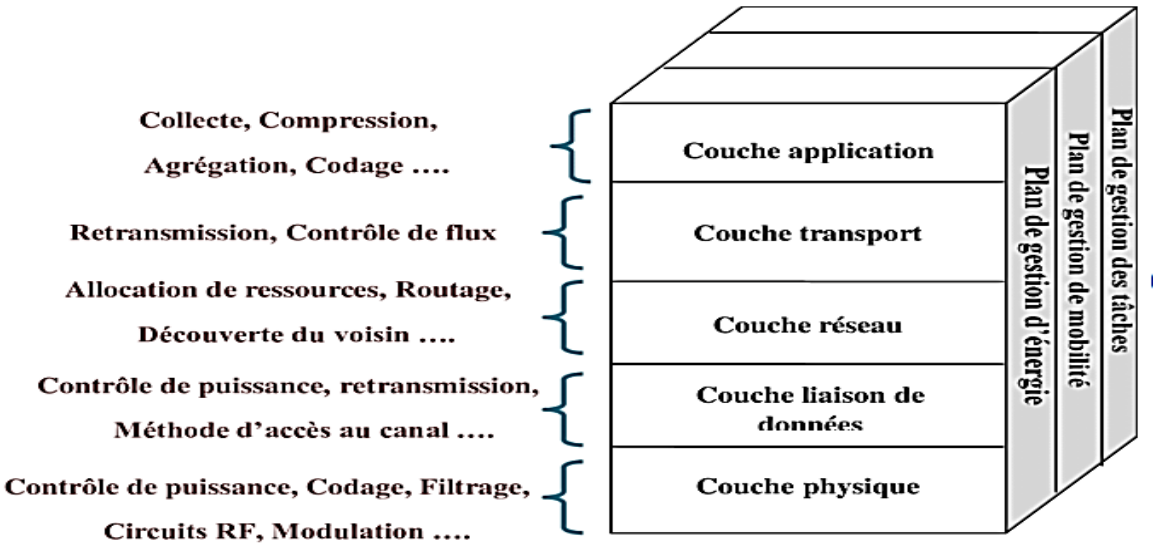


Figure 3: *La pile protocolaire d'un RCSF.[5]*

VI. Défit face à la conception d'un RCSF

- **Ressources énergétiques limitées** : Sans infrastructure fixe, les nœuds de capteurs sans fil sont obligés de gérer la petite batterie qu'ils fournissent. Cela limite leur puissance de calcul et leur taille de mémoire et les empêche d'utiliser toute la bande passante en raison des coûts énergétiques plus élevés. L'utilisation uniquement de l'alimentation par batterie signifie également qu'après une certaine durée de vie, les nœuds de capteur mourront, ce qui entraînera de graves problèmes de sécurité. [4]
- **Débit de données inférieur** : L'un des plus gros problèmes des réseaux sans fil en général est le faible débit de données. La quantité de données pouvant être transférées en un cycle dépend de la fréquence utilisée. Des fréquences plus élevées entraînent des débits de données plus élevés, mais causent en même temps plus de problèmes d'interférence. Cela empêche les réseaux sans fil d'être aussi rapides que les réseaux câblés. [4]
- **Échec de la communication** : Les réseaux sans fil ont un taux d'erreur plus élevé que les réseaux câblés. Ils utilisent des ondes électriques pour transmettre des paquets de données, et ces ondes peuvent être affectées par des phénomènes tels que la réflexion, la réfraction, la diffraction ou la diffusion. Ces phénomènes peuvent éclater ou déformer les colis, entraînant des erreurs de transmission. [4]

- **Problèmes de sécurité** : Les réseaux sans fil en général sont beaucoup plus faciles à attaquer de l'extérieur que les systèmes câblés. Le canal sans fil est accessible aux auditeurs indésirables et plusieurs attaques passives et actives peuvent être menées. Les méthodes comme le cryptage sont également limitées par les ressources énergétiques, qui tendent à être petites dans les RCSF, ce qui renforce les problèmes. [4]
- Un autre problème spécial sur RSCF est mort ou dysfonctionnent des nœuds de capteurs, tel que chaque nœud qui tombe augmente le risque que le réseau de capteurs ne soit pas en mesure d'approfondir les données de surveillance de manière à garantir la sécurité. [4]

3.Conclusion

En conclusion de ce chapitre, on peut dire que la fin de la recherche sur les RCSF n'est pas en vue. La technologie de réseau de capteurs sans fil a un potentiel incroyable pour améliorer la qualité de vie dans tous les aspects. Pour réaliser le plein potentiel de cette technologie, il y a beaucoup de travail supplémentaire à faire dans d'autres moments. La recherche doit se concentrer sur les aspects liés à la sécurité. [4]

Ce premier Chapitre vise à donner une description globale sur les RCSF, nous avons brièvement présenter des généralités et quelques notions sur les RCSF. Dans le prochain chapitre on va aborder l'aspect de la sécurité sur ces réseaux.

1.Introduction

Comme nous l'avons vu dans le chapitre précédent (chapitre I), les réseaux de capteurs sans fil sont des réseaux ad hoc spéciaux avec un nombre de nœuds plus conséquent surveillent une zone et obtiennent une réaction lorsque des données critiques sont détectées, et comme tout autre réseau les RCSF[5] sont vulnérables aux différentes attaques.

Dans ce deuxième chapitre, nous présentons les vulnérabilités sur les Réseaux de capteur sans fil, les attaques existantes contre ce dernier, nous définissons aussi l'attaque sinkhole et leur mécanisme, les contre mesure et les solutions existantes contre ces attaques, et nous terminons notre chapitre par une conclusion.

2. Règle de sécurité sur un RCSF

Les critères de sécurité sur n'importe quelle application ou réseau qui doit être prise en considération sont les suivants :

- **Confidentialité :** protéger la confidentialité des messages échangés et de ne pas les révéler à des nœuds non autorisés. Le moyen standard d'assurer la confidentialité est de crypter les données. [6]
- **L'intégrité :** L'intégrité des données garantit que les données reçues n'ont pas été modifiées en transit. L'intégrité est assurée en utilisant les fonctions de hachage. [6]
- **L'authenticité :** L'authentification des données permet au destinataire de vérifier que les données ont bien été envoyées par le prétendu expéditeur. Elle peut être effectuée en calculant un code d'authentification de message (MAC) des données de communication. [6]
- **Disponibilité :** Le service devrait être accessible en tout moment. [1]
- **Autorisation :** garantit que seul l'utilisateur autorisé qui peut accéder aux ressources du réseau. [1]

Au plus Dans un RCSF :

- **Fraîcheur :** La fraîcheur des données indique que les données sont à jour, garantissant qu'aucun ancien message n'est rejoué. Pour résoudre ce problème, un compteur de temps peut être ajouté au paquet. [6]
- **Non-répudiation :** Cela signifie qu'un nœud ne peut pas refuser d'envoyer un message qu'il a déjà envoyé. [1]

La sécurité physique des capteurs, nécessaire pour empêcher l'accès au contenu de la communication ou au matériel crypté.

3. Vulnérabilité sur RCSF

- **La tolérance aux fautes :** Dans un réseau de capteurs sans fil, un ou plusieurs capteurs peuvent ne pas fonctionner correctement. En effet, les capteurs sont des entités sensibles aux phénomènes climatiques (humidité, chaleur, électromagnétisme) ou aux changements d'état comme une batterie faible. [7]

[5] **RCSF** : Réseau de capteur sans fil.

- **Mise à l'échelle :** Le nombre de capteurs utilisés dans un réseau de capteurs sans fil peut varier de quelques entités à des dizaines de milliers, et ils doivent pouvoir s'autoorganiser à grande échelle et être efficaces quel que soit le nombre. Pour cela, le protocole du réseau de capteurs sans fil doit pouvoir fonctionner et s'ajuster en fonction du nombre de nœuds. [7]
- **Des ressources limitées (mémoire et espace de stockage limitées) :** L'utilisation des algorithmes de sécurité nécessitent des ressources de mémoires pour la mémorisation du code et des données, des ressources en énergie et en calcul Donc le code de sécurité et les données relatives doivent être très petites. [8]
- **Limitation en énergie :** C'est la contrainte la plus forte, puisque généralement les capteurs sont déployés à des endroits inaccessibles, donc on ne peut pas changer les batteries ou les recharger. Alors L'ajout des fonctions de sécurité a un et à prendre en considération sur la consommation des ressources, de temps processeur et par la suite sur la consommation en énergie. [8]
- **Communication non fiable :** Les données sont transmises dans l'air, donc chaque capteur qui se trouve dans le rayon de couverture peut écouter les messages échangés. [8]
- **Exposition aux attaques physique :** Le capteur est généralement déployé dans un environnement ouvert aux ennemis, et peut faire face à des conditions climatiques difficiles. [8]
- **Gestion à distance :** La gestion à distance du réseau rend la détection d'une attaque physique et la maintenance des capteurs (rechange ou recharge de batterie) impossible. [8]
- **Pas de station de base :** Le réseau de capteurs doit être conçu pour être un réseau distribué sans point de gestion central. Mais s'il y a une erreur de conception, l'organisation du réseau peut devenir difficile. [8]

4. Attaques sur un RCSF

Les RCSF sont particulièrement vulnérables à plusieurs types d'attaques :

On peut classer ces attaques à des attaques active et attaque passive :

- **Attaque passive** : si un attaquant ne cherche qu'à écouter le réseau. [10]

Écoute passive du réseau : L'attaquant, qui dispose d'un équipement puissant (vitesse de calcul, espace de stockage, ressource en énergie, etc.), Collecte les informations échangées dans le réseau de capteurs si elles ne sont pas chiffrées. [10]

Compromission du nœud : En compromettant un nœud, l'attaquant peut récupérer les informations incluses : programme, clés cryptographiques. [10]

Injection de nœuds malveillants : L'attaquant peut ajouter dans le réseau des nœuds malveillants pour injecter des données falsifiées dans le réseau. [10]

- **Attaque Active** : si un attaquant modifie l'état du réseau. [10]

Transmission sélective : supposons que tous les nœuds participent à la propagation des messages dans le réseau. Dans cette attaque, le nœud malveillant supprime quelques messages au lieu de les transmettre. L'efficacité de cette attaque dépend de deux facteurs. Le premier est

la place du nœud malveillant, plus il est proche de la station de base plus il reçoit de messages. Deuxièmement est le pourcentage des messages qu'il supprime. [10]

Attaque du trou noir : L'attaque du trou noir consiste tout d'abord à insérer un nœud malicieux dans le réseau. Ce nœud, par divers moyens, va modifier les tables de routage pour obliger le maximum de nœuds voisins à faire passer l'information par lui. A but pour toutes les informations qui vont passer en son sein ne seront jamais retransmises. [7]

La figure1 représente un trou noir mis en place par un nœud malicieux X qui a modifié le routage pour que les clusters[6] 1, 2, 3 et 4 fassent passer l'information par lui pour communiquer entre clusters. Dans ce cas de figure, le trou noir X ne retransmettra aucune information, empêchant toute communication entre les déférents clusters. [7]

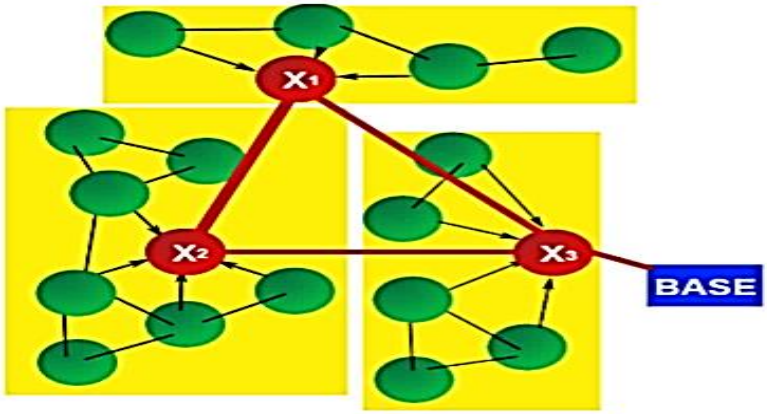


Figure 4:*Attaque du trou noir.[7]*

Attaque du trou de ver : L'attaque du trou de ver nécessite l'insertion d'au moins deux nœuds malicieux.

Ces deux nœuds sont reliés entre eux par une connexion puissante comme par exemple une liaison filaire. [11]

Le but de cette attaque est de tromper les nœuds voisins sur les distances. Généralement le protocole de routage cherche le chemin le plus court en nombre de sauts (hop). Dans le cas d'une attaque du trou de ver, les deux nœuds malicieux permettent d'atteindre un lieu éloigné avec un saut unique. Cette possibilité va tromper les autres nœuds sur les distances réelles qui

[6] **Clusters** : Un cluster est constitué d'un chef (cluster-head) et de ses membres (nœud de capteur).

Figure 5:*Attaque du trou ver.[7]*

Séparent les deux nœuds, mais va surtout obliger les nœuds voisins à passer par les nœuds malicieux pour faire circuler les informations. [11]

Cette attaque est représentée par la figure 2 où deux nœuds malicieux X1 et X2, reliés par une connexion puissante, forment un trou de ver. Les nœuds A et B vont alors privilégier la route la plus rapide formée par le trou de ver, et donc l'information pourra être récupérée par l'attaquant. [7]

Attaque sinkhole : on va la définir en détails dans la séquence suivante (5).

5. Attaque sinkhole

Définition : L'attaque sinkhole se produit à la couche réseau. C'est une attaque active. Elle dégrade lentement la performance du réseau. C'est une variante de l'attaque du trou noir. [7]

Dans l'attaque sinkhole Le nœud malveillant se place à un endroit stratégique (proche de la station de base[7] par exemple) et supprime tous les messages qu'il doit retransmettre. Cette attaque est grave lorsqu'il n'y a qu'une seule station de base dans le réseau. [10]

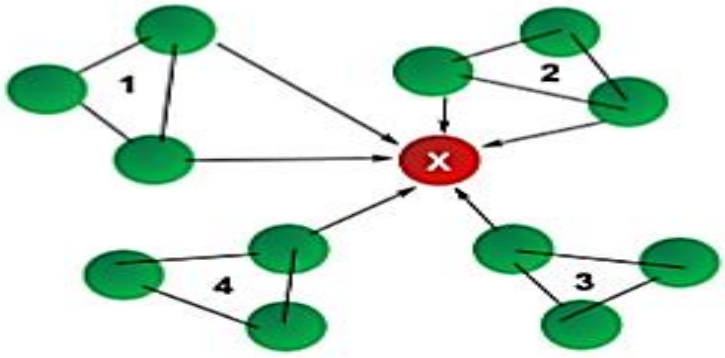


Figure 6*:utilisation de l'attaque trou de ver pour réaliser une attaque sinkhole.[7]*

[7] **Station de base :** un nœud de capteur plus puissant qui envoie ou reçoit un message via un certain nombre de nœuds et aussi stocke des informations reçues par d'autres nœuds de capteur.

La figure 3 représentée la situation d'utilisation de l'attaque trou de ver pour réaliser une attaque sinkhole, où les nœuds malicieux X1, X2 et X3 sont reliés par des connexions puissantes et forment des trous de ver. X3 est lui relié à la base par une connexion puissante pour réaliser une attaque du sinkhole. On parle alors d'une sphère d'influence exercée par l'attaquant sur le réseau, car il est ainsi capable de récupérer l'intégralité des informations qui circulent dans le réseau de capteurs sans fil donc les performances et l'efficacité du RCSF diminuent et la perte de paquets augmente.

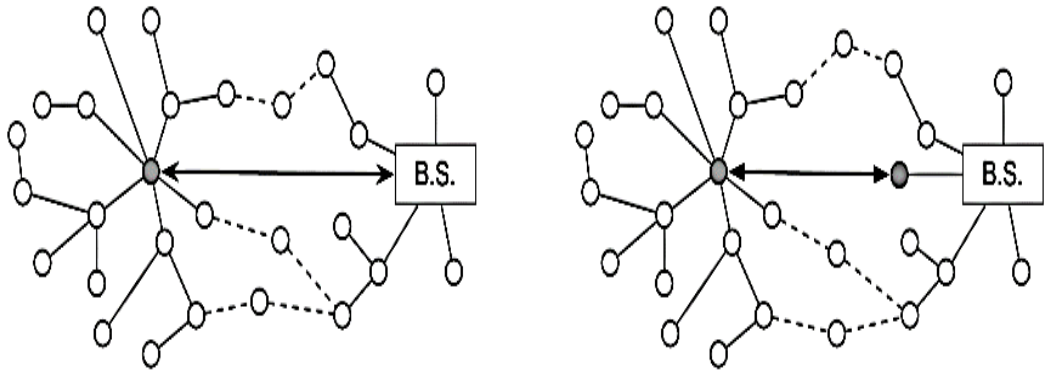


Figure 7:*Attaque sinkhole vs attaque sinkhole par attaque trou de ver.[14]*

Types de l'attaque sinkhole :

Dans cette attaque, les nœuds malveillants promettent d'être un meilleur chemin vers la station de base, donc trompant ses voisins pour utiliser la route la plus fréquemment. [14]

Ainsi, le nœud malveillant a la possibilité de trafiquer les données, d'endommager le fonctionnement régulier ou même de mener de nombreux défis supplémentaires à la sécurité du réseau. [14]

1. **Attaque sinkhole par un nœud interne compromis**

Un adversaire utilise un nœud compromis pour lancer l'attaque dans laquelle une route est annoncée pour tromper les voisins. [14]

2. **Attaque sinkhole par un nœud externe malveillant**

Un adversaire de classe ordinateur portable équipé d'une puissance de calcul et de communication hautes performances conduit une route à saut unique de sa zone environnante à la station de base, convainquant les voisins de transférer tout le trafic par cette route. De plus, un routage de haute qualité attirera non seulement les voisins du sinkhole, mais aussi presque tous les nœuds qui sont plus proches du sinkhole que la station de base (peut-être à plusieurs sauts de distance), ce qui amplifie la menace. [14]

3. **Attaque sinkhole par l'utilisation d'une attaque trou de ver**

Dans ce type d'attaque, un nœud malveillant capture d'abord un paquet de routage de l'un de ses voisins et utilise un tunnel secret pour envoyer le paquet à un autre nœud complice. Les nœuds

en collusion transmettent finalement le message à la station de base. Même si les extrémités du tunnel peuvent être plus éloignées que d'autres routes, cela peut empêcher la source de découvrir d'autres routes légitimes à plus de deux sauts de la destination, perturbant ainsi la fonctionnalité du réseau. [14]

6.Mécanisme de l'attaque sinkhole

1. À la première étape, l'attaquant sélectionne les nœuds (source et destination) qui doivent être ciblés pour l'attaque. [7]
2. Ensuite, le trafic est attiré vers des nœuds malveillants. [1]
3. Les autres nœuds attirent l'attention de leurs nœuds voisins en envoyant de faux idéaux en utilisant des capacités d'attractivité ou de transmission de données. [1]
4. Les nœuds voisins piégés dirigent ensuite leurs messages vers les nœuds malveillants et par conséquent les paquets sont abandonnés par les nœuds malveillants. [1]

La figure 4 est un diagramme schématique de l'attaque sinkhole qui attire tout le trafic environnant vers le nœud malveillant local, et le chemin à travers le nœud malveillant est optimal. Un sinkhole est créé au centre car tous les nœuds environnants envoient des paquets au nœud malveillant. Comme le montre la figure, le trafic du nœud source est rejeté par le nœud malveillant.[1]

De nombreuses attaques telles que l'écoute clandestine, la transmission sélective et le trou noir, etc. Peut être amélioré avec des attaques sinkhole.

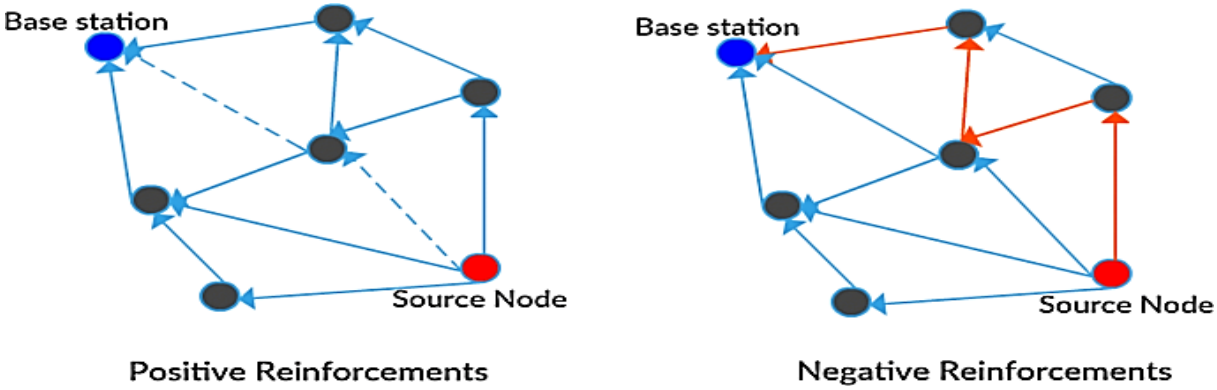


Figure 8:*Mécanisme de l'attaque sinkhole dans un RCSF.[1]*

7. Solution et contre mesure de l'attaque sinkhole dans RCSF

Diverses défenses peuvent être utilisées pour répondre aux besoins de sécurité des RCSF et les protéger contre l'attaque sinkhole.

Ces solutions doivent bien sûr prendre en compte les particularités des réseaux de capteurs sans fil. Il faut donc trouver des solutions simples qui permettent de sécuriser le réseau tout en consommant le moins d'énergie possible et adapter ces solutions à une puissance de calcul faible.[12]

- L'Algorithme de **Ngai et al**

Ngai et al proposent un algorithme lighweight pour détecter les attaques sinkhole, Dans leur approche, les stations de base collectent des informations sur le trafic réseau à l'aide d'une

approche distribuée, puis des algorithmes de reconnaissance analysent les données collectées pour localiser le sinkhole. Leur travail tient également compte de la présence de plusieurs attaquants complices dans le réseau. [14]

1. Collecte des données de capteurs : Les données de capteurs, telles que les adresses de destination, sont collectées pour une période donnée.
2. Division des données en groupes : Les données sont divisées en groupes de points similaires en utilisant une méthode de clustering, telle que l'algorithme DBSCAN.
3. Calcul de la densité de chaque groupe : La densité de chaque groupe est calculée en utilisant la densité moyenne des points de données dans le groupe.
4. Détermination des groupes anormaux : Les groupes qui ont une densité inférieure à un seuil fixe sont considérés comme anormaux, car ils peuvent indiquer une attaque sinkhole. Les groupes qui sont plus denses que la densité globale de l'ensemble des données sont également considérés comme anormaux, car ils peuvent indiquer une surcharge du trafic.
5. Identification des nœuds suspects : Les nœuds qui se trouvent dans les groupes anormaux sont identifiés comme suspects. Les nœuds qui sont connectés à plusieurs groupes anormaux sont considérés comme les plus suspects.

- **DTMS (**Dynamic Trust Management System**) :** Système de gestion dynamique de la confiance. [15]

Le DTMS a été décrit pour les réseaux ad hoc, mais il s'applique également aux capteurs. Il peut ou non nécessiter des frais de calcul supplémentaires et abordables.

Dans le monde réel, il est impossible d'attribuer une valeur discrète à la confiance d'une personne envers une autre dans la société, et personne dans la société ne peut faire entièrement confiance. Attribuer une confiance totale et/ou une méfiance, ou même des représentations discrètes de la confiance, à des capteurs/nœuds du réseau ne peut être considéré comme pertinent. La confiance s'exprime donc par une valeur continue comprise entre 0 et 1, où 0,5 est une valeur neutre, et c'est ainsi que fonctionne cette méthode.

- Méthode de détection **LQI-based routing.** [16]
- Système IDS proposé par **Krontiris et al**.

8. Travaux connexe sur la détection de l'attaque Sinkhole dans les RCSFs

Tableau 2: Tableaux sur les Travaux Connexe sur la détection de l'Attaque Sinkhole.[20]

Approche	Solution proposée	Résultat	Limites/Avantages
Basé sur des règles. Krontiris et al 2007	Ils ont prolongé leurs IDS qui peut détecter attaque sinkhole.	-le succès de l'intrusion système de détection dépend de l'augmentation du nombre de chien de garde. -Lorsque la densité du réseau	**Limites** -Surcharge mémoire et réseau a été créé. -Ils ont utilisé le protocole MintRoute. -L'emprunt d'identité de nœud était le

		augmenter le taux de faux négatifs diminuer.	centre des règles. **Avantages** -Mesure plus sûre et robuste peut être développé sur la base principe précieux qu'ils développent.
Basé sur des règles. Krontiris et al 2008.	Ils ont proposé règles de détection qui gardera conscient nœud légitime l'existant de attaque.	Ils montrent comment les vulnérabilités de MultihopLQI peut être exploité par nœud doline et suggérer les règles qui rendre le protocole plus résilient.	**Limitation** -They did not show practically how those rules can prevent attack. -All the rules are only detecting attack but cannot give ID of sinkhole node. -They assume attacker has the same power as normal node and can capture sensor node and change the internal state.
Anomalie basé. Tumrongwitta yapak, C et Varakulsiripun Je, R 2009	Ils ont proposé détection basé sur des solutions à la réception force du signal indicateur (RSSI) Leur solution proposée requis soutien de moniteur supplémentaire nœud	-Pour 0 à 40 % de pourcentage de message laisser tomber la détection le taux est de 100% -Le taux de faux positifs était de 0 pour 0- 40 % des messages sont abandonnés, mais augmenter lorsque le pourcentage baisse augmenter -La même chose s'applique au faux	**Limitation** -Ils supposent que le réseau de capteurs est Statique. -Pas d'attaque instantanée -La station de base reste en position 0,0 -Station de base et moniteur supplémentaire nœud sont physiquement protégés. -Leur solution proposée ne peut pas détecter l'attaque si elle s'est produite

		taux négatif avec plus de message drop plus taux négatif.	instantanément après le réseau déploiement.
Anomalie basé. Choi et al 2009	Ils ont proposé méthode qui peut détecter gouffre attaque qui a utilisé LQI (lien qualité indicateur).	-La probabilité de détection augmenter lorsque le nombre de les nœuds détecteurs augmentent. -augmentation du taux de détection lorsque augmentation du nœud détecteur. -Le taux de faux positifs dépend sur l'étendue de la valeur de tolérance (valeur constante qui montrer si les changements sont au-delà anormal).	**Limites** -Tous les nœuds de capteur n'ont pas de mobilité. -La détection du gouffre se produit lorsque le nœud du détecteur est entre nœud gouffre et nœud source et gouffre et station de base. -Les nœuds détecteurs ont des source d'énergie que le capteur nœuds. **Avantage** -Le nœud détecteur communique eux-mêmes par le biais exclusif canaliser.
Anomalie basé. Sharmila, S. et Umamaheswar je, G. 2011.	-Ils ont proposé résumé des messages algorithme pour détecter gouffre nœud.	-Les résultats montrent l'algorithme a bien fonctionné lorsqu'il était malveillant les nœuds sont inférieurs à 50 % -Le taux de faux positifs était de 20 % (en raison de la perte de paquets) ce chiffre obtenu lorsque le nœud malveillant atteindre 50	**Limitation** -Débit réseau, surcharge et le coût de la communication n'était pas calculé -Les performances n'étaient pas bonnes lorsqu'il y a collision de nœuds, puissance transmise limitée et gouttes de paquets -Une seule annonce est considérée à la

		-L'erreur de faux négatif était de 10 % mais augmentait quand nœud malveillant atteint plus de 40.	fois, après un autre calcul a lieu. **Avantage** -L'algorithme atteint les données intégrité et authenticité.

9. Conclusion

Les solutions fournies par la communauté scientifique ne garantissent pas toujours la plus grande solution de sécurité au RCSF. La faible puissance du capteur, en particulier leur énergie limitée, donc le déploiement de technologies doit être plus avancées. Nous devons toujours rechercher des solutions qui peuvent concilier la sécurité, la vie et la vitesse d'exécution. [12]

Le chapitre 2 passe en revue l'état de l'art sur les problèmes de sécurité et les solutions proposés pour s'adapter aux contraintes spécifiques de ces réseaux. Cependant, divers travaux sont encore théoriques et difficiles à appliquer dans la plupart des cas en raison des contraintes d'énergie et de mémoire des nœuds de capteur dans RCSF.

Dans le prochaine chapitre3 on va proposer une solution pour détecter l'attaque sinkhole dans un RCSF.

1.Introduction

Comme nous l'avons vu dans le chapitre précédent (chapitre II), les RCSFs sont vulnérables aux différentes attaques.

L'attaque sinkhole est l'une de ces attaques dont l'objectif principal est de rediriger le trafic vers un serveur ou un dispositif compromis, souvent appelé "sinkhole", afin de permettre à l'attaquant d'analyser et de contrôler les données qui y transitent.

Dans ce troisième chapitre, nous allons expliquer le fonctionnement du protocole AODV (Ad-hoc On-demand Distance Vector) dans les RCSFs, le mécanisme de l'attaque sinkhole dans le protocole AODV, afin de présenter notre stratégie de détection de l'attaque sinkhole dans le protocole AODV dans les RCSFs afin de le sécuriser, et nous terminons notre chapitre par une conclusion.

2. les protocoles de routage dans les RCSFs

Les protocoles de routage pour les réseaux de capteurs sans fil ont été largement étudiés et diverses études ont été publiées. Ces protocoles doivent garantir que les informations circulent entre n'importe quel nœud du réseau et la station de base à un moindre coût énergétique. Dans les réseaux de capteurs, chaque nœud joue le rôle de source et de relais.

Voici quelque protocole existant dans les RCSFs :

- EACH (Low-Energy Adaptive Clustering Hierarchy).
- AODV (Ad-hoc On-demand Distance Vector).
- DSR (Dynamic Source Routing).
- SPIN (Sensor Protocols for Information via Negotiation).
- CTP (Collection Tree Protocol).

Ces protocoles ne sont qu'une sélection parmi de nombreux protocoles de routage développés pour les réseaux de capteurs sans fil. Le choix du protocole dépend des caractéristiques du réseau, des contraintes spécifiques et des exigences de l'application.

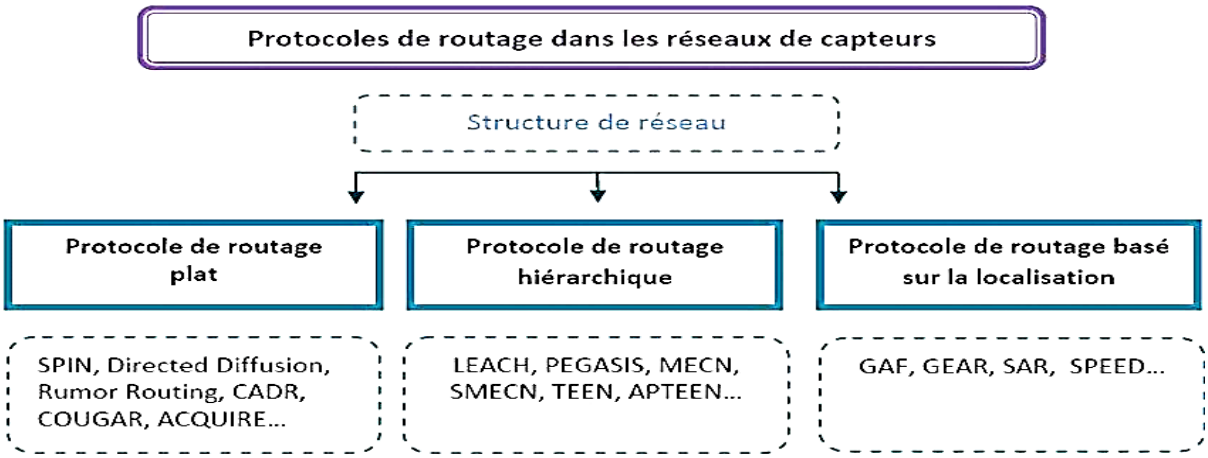


Figure 9:*Classification des protocoles de routage selon la topologie du réseau.*

3. le protocole de routage AODV (Ad-hoc On-demand Distance Vector)

Avec Le protocole AODV (Ad-hoc On Demand Distance Vector), chaque nœud dispose d'une table de routage qui fournit des informations sur ses voisins, et la table est importante pour décider quel voisin transfère les paquets de la source vers la destination. Lorsque la source a des données à envoyer à la destination, elle diffuse une Demandes d'acheminement **RREQ** (Route Request), Lorsqu'un nœud reçoit un **RREQ** il met à jour ses informations (Ajoutez une nouvelle route valide pour le nœud source à sa table de routage pour accéder à la source qui a envoyé le **RREQ)**. Lorsque **RREQ** atteint sa destination, il génère une réponse Type de réponse de routage **RREP** (Route Reply). **RREP** remonte à la source suivant le chemin inverse de **RREQ** comme indiqué sur la figure2. [18]

Chaque nœud a un numéro de série et peut choisir le chemin le plus proche.

La mise à jour s'effectue par l'échange de trois types de messages :

• **RREQ** Route Request, un message de demande de route.

• **RREP** Route Reply, un message de réponse à un RREQ.

• **RERR** Route Error, un message qui signale la perte d'une route.

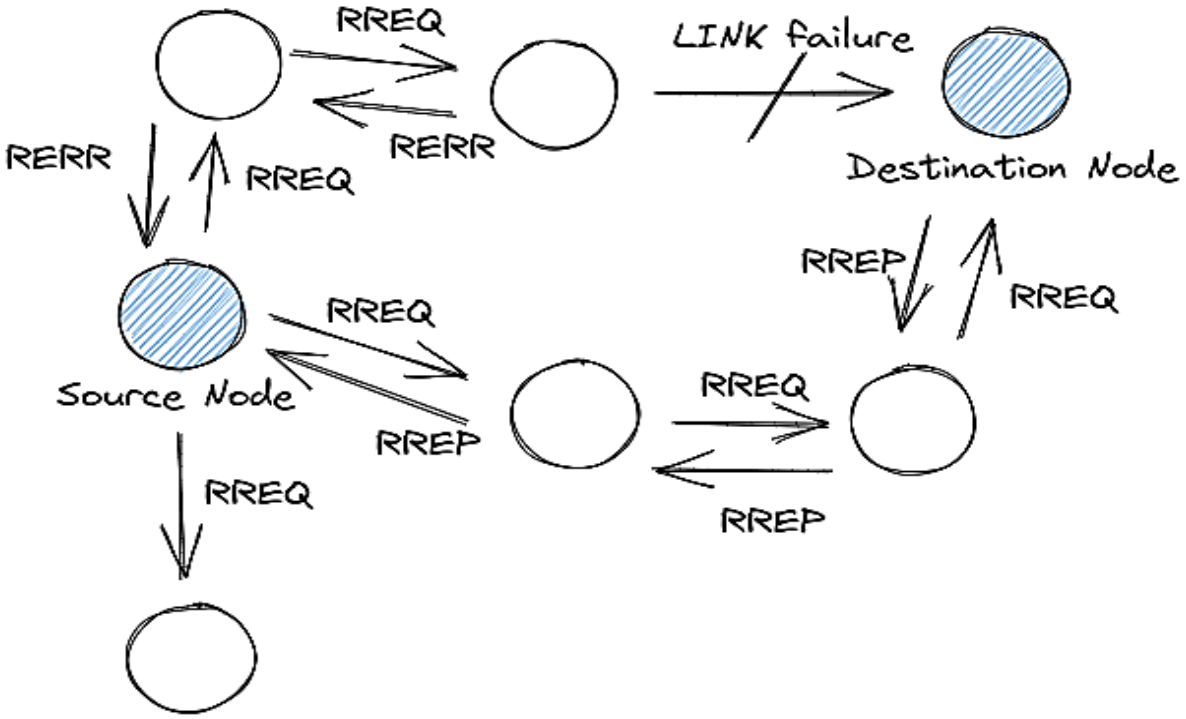


Figure 10:*fonctionnement de protocole AODV.*

Fonctionnement de protocole AODV :

Le message de contrôle sur le protocole AODV est divisé en trois [19] :

1. Demande de routage (**RREQ**) : Il envoie d'abord en mode diffusion RREQ aux nœuds voisins ou plus précisément au nœud cible.
2. Acheminement de la réponse(**RREP**) : si l'un des nœuds est un nœud de destination ou à une route valide vers la destination, alors le message de réponse RREP prendra le chemin vers la source génératrice de RREQ.
3. Message d'erreur(**RRER**) : informer les nœuds du réseau qu'une route vers une destination spécifique n'est plus valide.

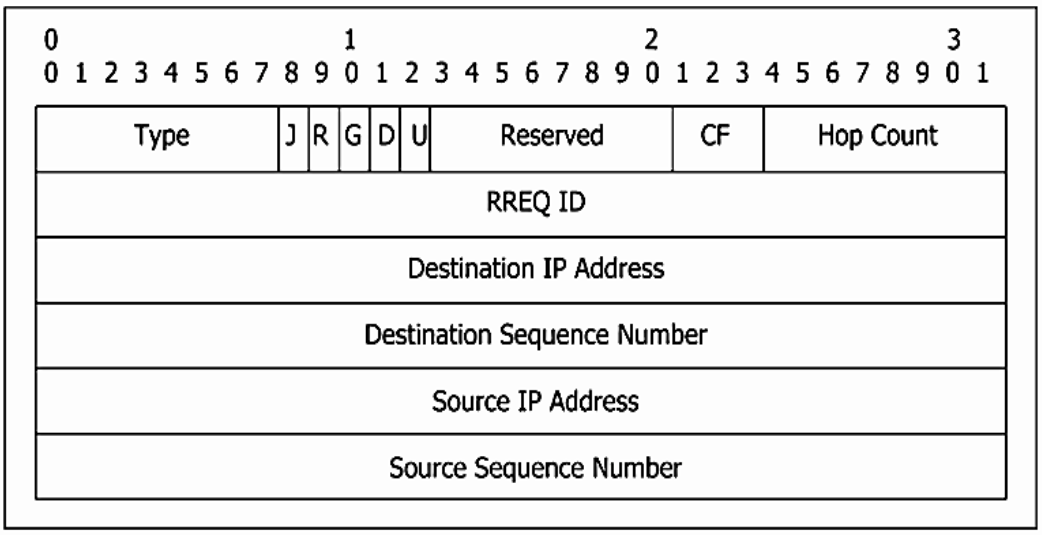


Figure 11:*format d'une RREQ(Route Request).*

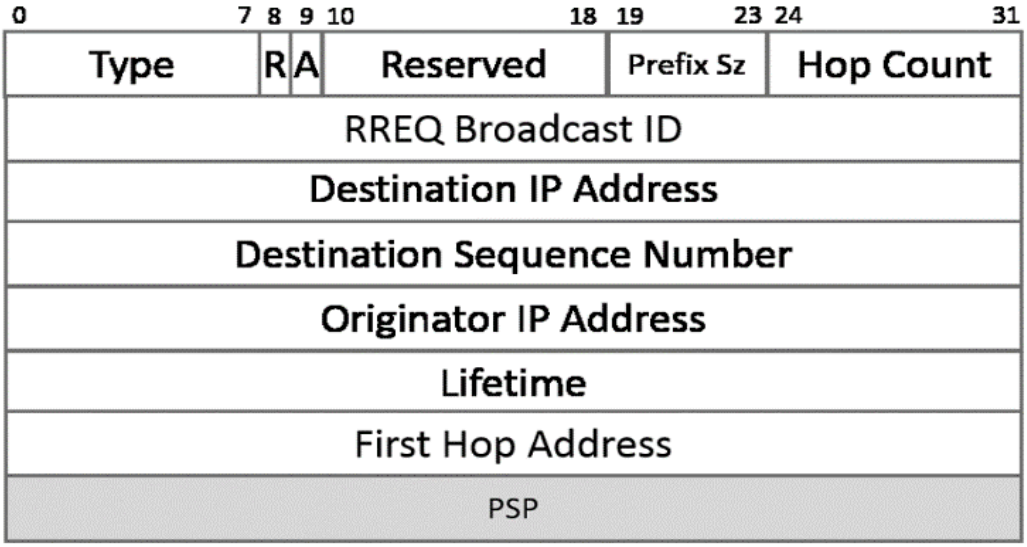


Figure 12:*format d'une RREP(Route Reply).*

4. Mécanisme de l'attaque sinkhole dans le protocole AODV

Comme toute les protocoles de routage dans les RCSFs, AODV est également vulnérable à diverses attaques, y compris l'attaque de sinkhole. [19]

L'attaque de sinkhole vise à perturber le processus de routage en incitant les nœuds à acheminer leur trafic via un nœud malveillant, appelé « **Sinkhole** ». [19]

Le nœud sinkhole se fait passer pour un nœud de routage légitime et attire les paquets de données en diffusant de fausses informations de routage.

Une fois que les nœuds de capteurs sont piégés dans le sinkhole, l'attaquant peut **surveiller**, **modifier** ou **supprimer** les paquets de données, compromettant ainsi **l'intégrité** et **la confidentialité** du réseau.

Dans le protocole AODV l'attaque sinkhole est définie en modifiant « **le numéro de séquence du RREQ** » (**Destination sequence number**) plus le numéro de série est élevé Plus la route sera récente plus.

- Le processus se déroule comme suit : [19]

Cas1 : fonctionnement de routage sous le protocole AODV en cas normale.

1.un nœud crée un paquet à envoyer à la destination.
2.lorsque le paquet arrive à un nœud, le paquet est vérifié par la table de routage de ce nœud pour vérifier qu'il existe actuellement des chemins disponibles pour se rendre au nœud de destination ou non.
3.s'il y en a, le paquet sera directement transmis au saut suivant.

- Mais s'il n'y en a pas, le processus de détermination de La route se poursuit : [19]

Cas2 : en cas d'une attaque sinkhole.

a. Il commence par envoyer une diffusion de RREQ à un nœud voisin ou plus précisément au nœud de destination (Ces annonces indiquent que le nœud de l'attaquant « sinkhole » a une route plus courte ou meilleure vers une destination spécifique que les autres nœuds).
b. les nœuds qui reçoivent une RREQ, le relient à la table de routage appartenant à chaque nœud.
c. Pour répondre au RREQ d'un nœud, il doit être listé sur la table de routage de nœud source (Le nœud source doit avoir des entrées non expirées dans sa table de routage vers le nœud de destination),La valeur de l'ordre du numéro de destination dans le RREQ doit être au moins égale à celle du nœud source (L'ordre du numéro de destination est utilisé pour éviter les boucles de routage),la valeur de l'ordre du numéro de destination est supérieure ou égale à celle du nœud source alors on garantit que le nœud source est sur le chemin le plus court vers la destination.
d. Si la condition de l'étape «**c** » est remplie et que l'adresse IP de destination est égale à RREQ, alors envoyez le message RREP au nœud source avec une méthode de monodiffusion au lieu de diffuser en utilisant plusieurs chemins.
e. Mais si la condition de l'étape «**c** » n'est pas remplie, le nœud source augmentera le nombre de sauts et le retransmettra à ses voisins.

5. Méthode de détection (l'approche proposée)

❖ Notre proposition est basée sur «la variation du nombre de sauts » dans un réseau statique.

Car en cas d'un réseau sans attaque, le nombre de sauts pour atteindre une destination devrait être relativement stable.

Lorsqu'une attaque de sinkhole se produit, le nœud malveillant « sinkhole » attire le trafic et les nœuds capteurs piégés choisissent ce nœud comme prochain saut.

Dans cette technique on suit **la variation du nombre de sauts** pour détecter un possible attaque de sinkhole. (Techniques de détection d'intrusion).

Cet algorithme « surveille le nombre de sauts dans le protocole AODV » pour détecter toute variation anormale qui pourrait indiquer une attaque de sinkhole.

❖ **L'Algorithme proposée en langage naturel :**

1. Créez le réseau.
2. Créez les nœuds du réseau de capteurs sans fil.
3. Créez le canal de communication.
4. Configurez l'interface sans fil, y compris les paramètres physiques et de la couche MAC.
5. Configurez la couche de liaison de données (LL) pour l'ARP type sans fil.
6. Configurez le protocole AODV et attachez-le aux nœuds.
7. Configurez les routes initiales pour le protocole AODV.
8. Définissez une fonction de détection de l'attaque de sinkhole.

Hypothèse

On suppose que notre Réseaux aux caractéristiques suivant :

- Le Réseaux est Plat.
- Le Réseaux est statiques, les nœuds immobiles.
- L'attaque survient lors de la 3ème phase (la phase déploiement et découverte des chemins supposent que le réseau est sain).
- L'attaque survient pendant la communication (transfère des paquet).

❖ Ce code est une représentation simplifiée en langage algorithmique de l'algorithme de détection de l'attaque Sinkhole basé sur la surveillance des variations du nombre de sauts dans un réseau de capteurs sans fil, Si une attaque est détectée, le code affiche le message correspondant et la variation du nombre de sauts pour chaque nœud. Sinon, il affiche simplement un message indiquant qu'aucune attaque n'a été détectée.

```
❖ Algorithme Detectsinkhole ;
❖ Début
❖     Si il y a des données à transmettre alors
❖         var paquet : Paquet;
❖         FormerLePaquet(paquet);
❖         paquet.nb_hop <- 0;
❖         envoyer(paquet);
❖         attendreACK;
❖         Si ACK.nb_hop ≠ nb.saut alors
❖             ecrire("Il y a une attaque");
❖         Fin Si;
❖     Sinon
❖         Si réception alors (Routeur)
❖             Recevoir(paquet) ;
❖             paquet.nb_hop <- paquet.nb_hop + 1;
❖             envoyer(paquet);
❖         Sinon
❖             Rien;
❖         Fin Si;
❖     Fin Si;
❖ Fin.
```

❖ Cet algorithme suppose que chaque nœud du réseau de capteurs sans fil maintient une table de routage pour enregistrer les informations de routage, y compris « le nombre de sauts vers chaque destination ». L'algorithme vérifie périodiquement les paquets de données reçus et compare le nombre de sauts actuel avec le précédent enregistré dans la table de routage. S'il Ya une différence entre les deux, une détection d'anomalie est signalée. Si une attaque est détectée, il affiche le message correspondant « il ya une attaque ». Sinon, rien il sort de l'algorithme.

Déploiement de l'algorithme detectsinkhole :

« Avant d'injecter l'algorithme dans les nœuds il doit assurez que les nœuds du réseau prennent en charge le protocole AODV. »

a. Intégrez l'algorithme Detectsinkhole dans le code principal du protocole AODV, en ajoutant la fonctionnalité de détection de sinkhole, **Pour chaque nœud**.
b. Lors de la formation du paquet (dans la partie "S'il y a des données à transmettre "), ajoutez la variable « nb. Saut » informations spécifiques à la détection de sinkhole au paquet.
c. Chaque nœud « routeur » du réseau de capteurs sans fil doit inclure une étape de détection de sinkhole lorsqu'il reçoit un paquet.
d. Envoyer(paquet) : Cela signifie que le nœud envoie le paquet de données à la destination prévue. Le paquet contient les données à transmettre et la variable nb. Saut.
e. attendreACK: Après avoir envoyé le paquet, le nœud attend un accusé de réception (ACK) de la part du destinataire. L'ACK est une confirmation que le paquet a été reçu avec succès par le destinataire.
f. Si (ACK.nb_hop ≠ nb.saut) alors : Dans cette condition, nous comparons le nombre de sauts (nb_hop) dans l'ACK avec le nombre de sauts prévu (nb.saut). Le nombre de sauts indique le

nombre de nœuds ou de routeurs traversés par le paquet depuis son émission jusqu'à sa destination.

- Si ACK.nb_hop est différent de nb.saut, cela signifie que le nombre de sauts dans l'ACK est différent de ce qui était attendu. Cela peut indiquer qu'il y a eu une attaque ou une manipulation sur le chemin de transmission du paquet.
- Si ACK.nb_hop est égal à nb.saut, cela signifie que le nombre de sauts dans l'ACK correspond à ce qui était attendu, indiquant une transmission normale du paquet sans attaque détectée.

g. « Ecrire ("Il y a une attaque") » : Si la condition ACK.nb_hop ≠ nb. saut est vérifiée, cela signifie qu'une attaque a été détectée, et le message "Il y a une attaque" est affiché ou écrit pour signaler cette situation.

h. Répétez ces étapes pour chaque nœud du réseau de capteurs sans fil afin d'implémenter la détection de sinkhole dans l'ensemble du réseau.

i. Si réception alors (Routeur) : Cette condition vérifie si le nœud en question est un routeur et a reçu un paquet. Cela permet de différencier le comportement d'un routeur de celui d'un nœud destinataire final.

j. Recevoir(paquet) : Le routeur utilise la fonction "Recevoir" pour capturer le paquet qui lui est destiné. Le paquet contient les données à transmettre ainsi que d'autres informations telles que le nombre de sauts (nb_hop) déjà effectués par le paquet.

k. Paquet.nb_hop <- paquet.nb_hop + 1: Après avoir reçu le paquet, le routeur incrémente le nombre de sauts (nb_hop) dans le paquet de 1. Cela permet de mettre à jour le nombre de sauts effectués par le paquet, indiquant qu'il a traversé un nœud supplémentaire.

l. Envoyer (paquet) ; : Une fois que le nombre de sauts a été mis à jour, le routeur utilise la fonction "envoyer" pour transmettre le paquet au prochain routeur ou à la destination finale du paquet. L'envoi du paquet permet de le faire progresser dans le réseau vers sa destination prévue.

m. Sinon Rien ; : Si le nœud ne correspond pas à la condition "Si réception alors (Routeur)" (c'est-à-dire s'il n'est pas un routeur ou s'il n'a pas reçu de paquet), alors aucune action supplémentaire n'est requise.

Planifiez l'exécution périodique de l'algorithme de détection de l'attaque de sinkhole.

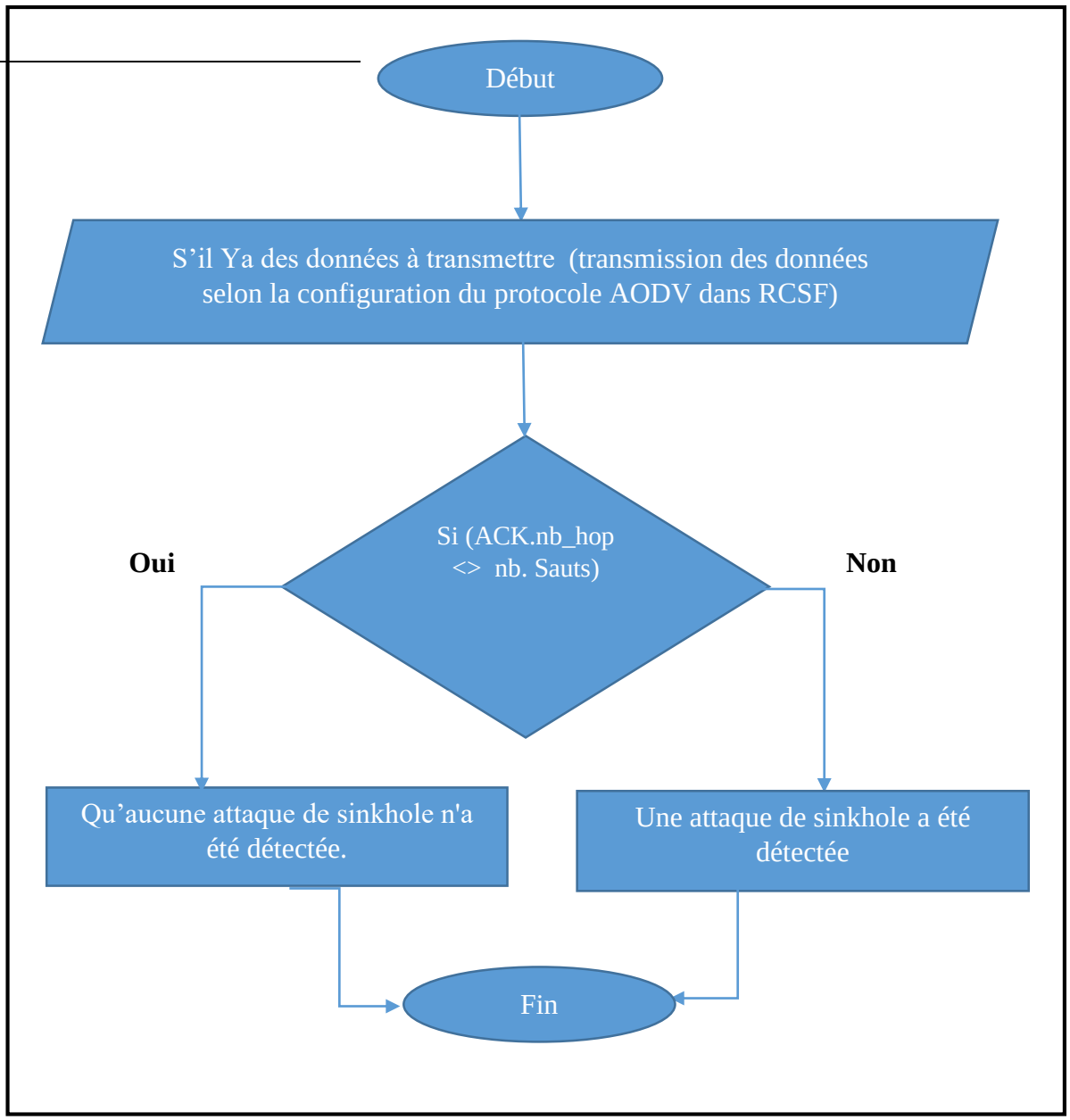


Figure 13:*logigramme de la fonction de détection de l'attaque sinkhole.*

- Ce logigramme illustre les étapes nécessaires pour détecter une attaque de sinkhole.
- Les nœuds du réseau sont parcourus un par un, et pour chaque nœud,
- Le nombre de sauts actuel du protocole AODV est récupéré et stocké dans une structure de données.
- Ensuite, il est vérifié s'il y a une variation du nombre de sauts entre les nœuds.
- Si tous les nœuds ont le même nombre de sauts, un message indiquant qu'aucune attaque de sinkhole n'a été détectée est affiché.
- Sinon, un message indiquant qu'une attaque a été détectée est affiché, suivi de la variation du nombre de sauts pour chaque nœud concerné.

6. Conception

On va modélisée notre Algorithme en modèle UML (Le Langage de Modélisation Unifié, de l'anglais Unified Modeling Language, est un langage de modélisation graphique) (diagramme de cas d'utilisation, diagramme de classes) et nous avons utilisé pour cela (l'outil StarUML) :

StarUML est un ***outil*** spécialisé dans la modélisation UML pratique dans le domaine du développement d'applications.

StarUml

Diagramme de classe :

Un nœud de capteur comprend certains composants de base qui sont organisés comme indiqué dans la Figure2 du chapitre1.

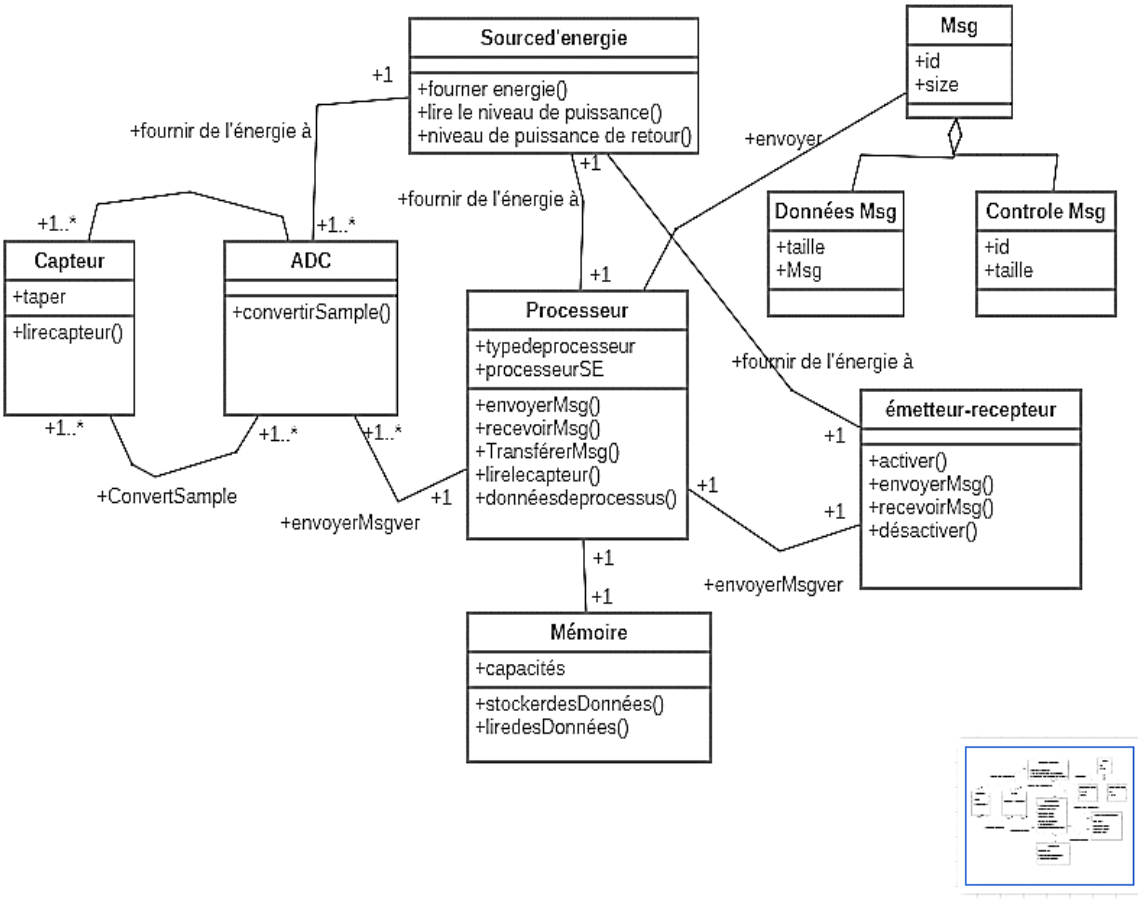


Figure 14:*Diagramme de classe d'un nœud de capteur.*

Diagramme de cas d’utilisation :

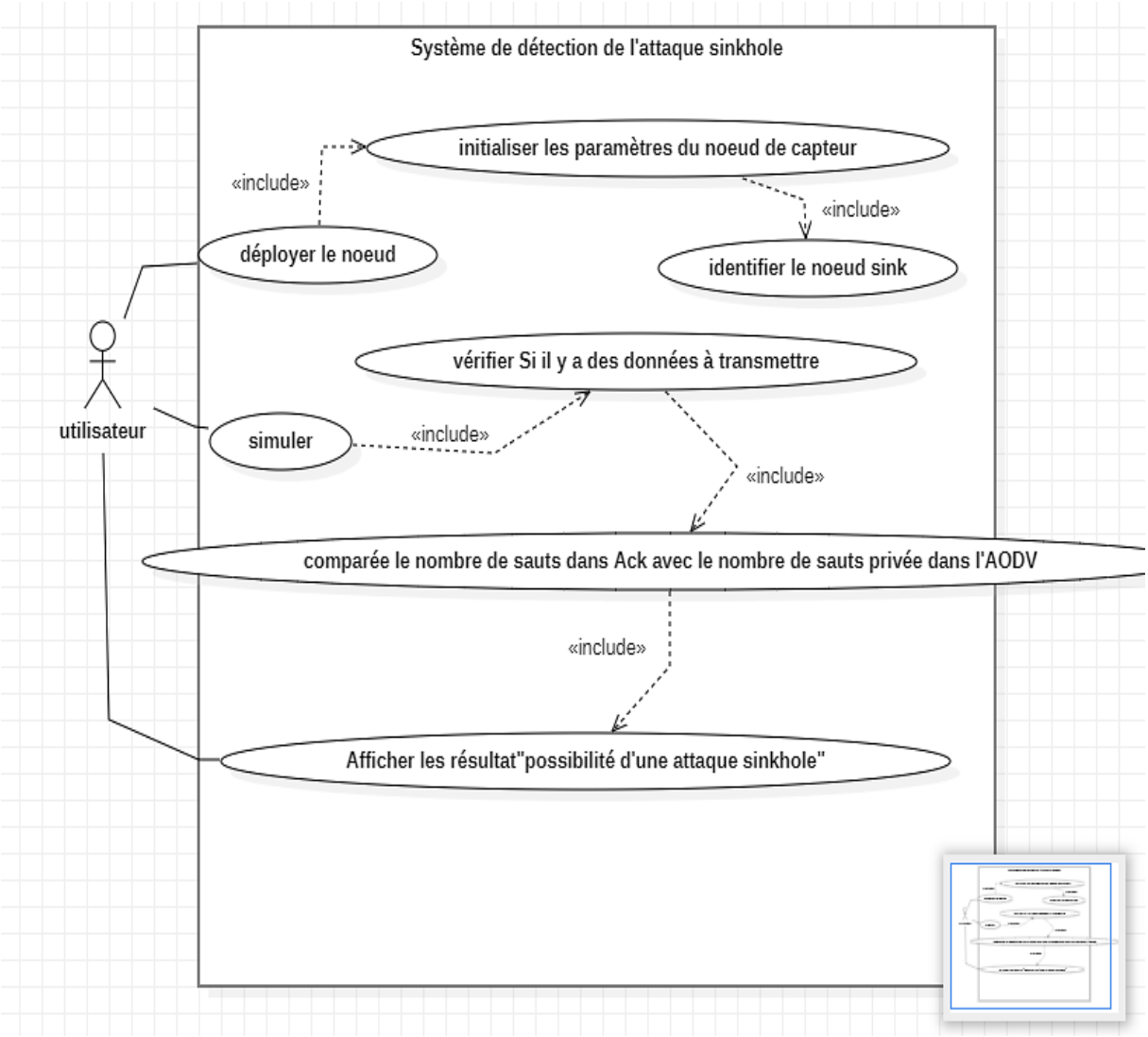


Figure 15:*Diagramme de cas d’utilisation du système de détection d’une attaque sinkhole dans un RCSF sous AODV.*

Les diagrammes de cas d'utilisation présentent les exigences du système d'utilisation.

Dans ce schéma, nous voudrais présenter les cas d'utilisation pour un scénario de simulation, dans ce cas, nous pouvons voir que la simulation a un acteur (utilisateur) qui fournit certaines actions au scénario externe.

Cas d’utilisation :

Déployer le nœud : installation et à la configuration d'un nœud informatique dans un réseau de capteur sans fil.

Simuler : création d'un environnement virtuel qui permet de modéliser et d'analyser le comportement du réseau de capteurs sans fil sans avoir besoin de déployer physiquement les capteurs. Cela permet de tester différentes configurations, protocoles et stratégies de déploiement dans un environnement contrôlé.

7. Conclusion

Dans ce chapitre nous avons présentés une étude sur le fonctionnement du protocole AODV dans les réseaux de capteur sans fil, le mécanisme de l’attaque sinkhole dans ce protocole et la solution proposé pour détecter cette attaque dans les RCSFs.

Il est important de noter que cette méthode de détection (l’algorithme proposée) fournit des indications potentielles d'une attaque de « sinkhole », mais elles ne garantissent pas une détection à 100 %.

La faible puissance du capteur, en particulier leur énergie limitée, nous obligions toujours de rechercher des solutions qui peuvent concéder la sécurité, la vie et la vitesse d'exécution.

1.Introduction

Dans l'ensemble, un RCSF opérant avec le protocole AODV ou tout autre protocole de communication, se compose de plusieurs nœuds de capteurs tout autour et partageant le médium de communication sans fil.
Parmi les techniques proposées pour spécifier et vérifier des systèmes dans lesquels
Le temps apparaît comme paramètre, qui sont largement utilisées : les Réseaux de
Petri Temporels (ou Time Petri Nets).
Après avoir proposée et expliquer notre approche dans le chapitre III, dans ce quatrième chapitre, nous allons faire la modélisation et l'analyse de notre approche sous l'outil Tina (**T**ime **P**etri **N**et **A**nalyzer).

2.Mise en œuvre, l'environnement Tina

Tina (Time Petri Net Analyzer)[8] est un environnement logiciel permettant l'édition et l'analyse de réseaux de Petri et réseaux temporels. Les différents outils constituant l'environnement peuvent être utilisés de façon combinée ou indépendante. Ces outils incluent :

nd (NetDraw) : est un outil d'édition de réseaux temporels et d'automates, sous forme graphique ou textuelle. Aussi, il intègre un simulateur « pas à pas » (graphique ou textuel) pour les réseaux temporels et permet d'invoquer les outils ci-dessous sans sortir de l'éditeur.

Tina : cet outil construit des représentations de l'espace d'états d'un réseau de Petri, temporel ou non. Aux constructions classiques (graphe de marquages, arbre de couverture), tina ajoute la construction d'espaces d'états abstraits, basés sur les techniques d'ordre partiel, préservant certaines classes de propriétés, comme l'absence de blocage, les propriétés de certaines logiques, ou les équivalences de test.

Tina(tina-2.10.0) **nd**

3.Modélisation formel du protocole AODV

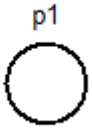
Pour modéliser formellement le protocole AODV[9] dans les réseaux de capteurs sans fil à l'aide de l'outil TINA (Time Petri Net Analyzer), nous utilisant les réseaux de Petri temporels (Timed Petri Nets) pour représenter le comportement du protocole.

• **Un réseau de Petri (RdP)** est un graphe biparti constitué de 2 sortes de nœuds :

Les places (représentées par des ronds).

[8] https://projects.laas.fr/tina/index.php
[9] Protocole de routage est peu gourmand en énergie et ne nécessite pas de grande puissance de calcul, il est donc facile à installer sur de petits équipements mobiles (nœud de capteur).

Les transitions (représentées par des barres).



Place **transition**

Le graphe est orienté : Des *arcs* vont d'une sorte de nœuds à l'autre (jamais de places à Places, ou de transitions à transitions directement).

• Graphe formé de

- ensemble de places P = {P1, P2, P3,….}

- ensemble de transition T= {T1, T2, T3,….}

- marquage initial M= {m1, m2, m3,….}

❖ Dans La figure16 on va représenter une version simplifiée du protocole AODV sans retransmission ni détection d'attaque sinkhole. Elle montre trois variantes : l'émetteur à gauche, le récepteur à droite et le réseau au milieu, qui représente le voisinage des nœuds communicants.

✓ Les nœuds (émetteurs : sont ceux qui initient la communication.
✓ Les nœuds (récepteurs) : sont ceux qui reçoivent les données transmises.
✓ Le « sink » : représente le nœud qui joue le rôle de point central pour collecter les données du réseau.
✓ Les autres nœuds forment le reste du réseau.

Description des transitions du modèle RDPT (Réseau de petri) pour le protocole AODV

Le protocole AODV, réduit le nombre de diffusions de messages, et cela, en créant les routes lors du besoin.

Ces transitions représentent les principales étapes du protocole AODV dans un modèle de réseau de Petri adapté aux réseaux de capteurs sans fil.

Nœud source :

T1 : la source diffuse le paquet RREQ pendant la découverte de la route.

T2 : Réception de l'ACK par l'émetteur.

T3 : à la réception du paquet RREQ par la destination répond par un paquet RREP contenant la route arriver à destination.

Nœud Destination :

T4 : les nœuds intermédiaires peuvent également envoyer un paquet RREP à la source s'ils ont une route vers la destination dans leur table de routage.

T5 : Débuter une nouvelle communication.

T6 : Les nœuds voisins reçoivent RREQ et vérifient si le nœud destination est connu ou s'ils ont déjà une route valide vers ce nœud.

T8 : Le message RREP suit le chemin inverse emprunté par la demande de route et est transmis aux nœuds intermédiaires jusqu'à atteindre le nœud source.

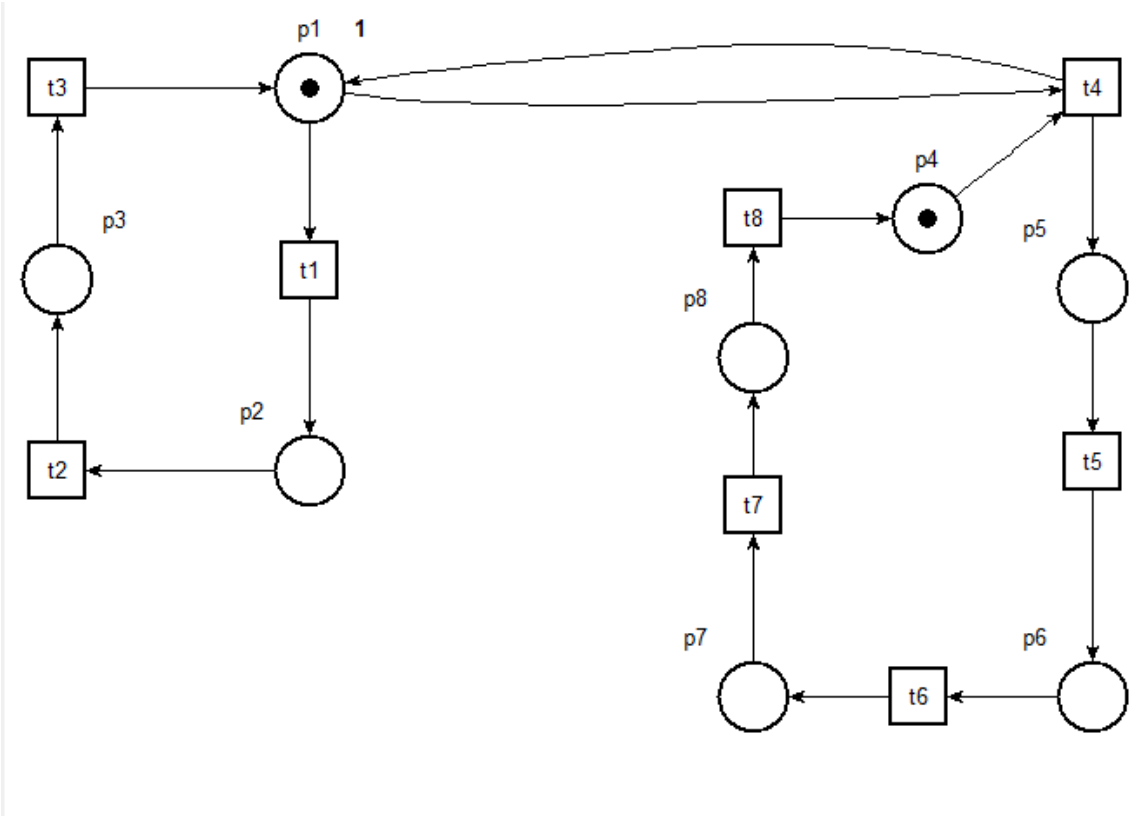


Figure 16:*RDP-T du modèle réduit du protocole AODV.*

La figure 16 trace la version sécurisée du protocole AODV représentée par un modèle de réseau de Petri Temporel (RDP-T).

Le RDP-T modélise dans la figure17 le processus de détection de l'attaque Sinkhole. Avec le marquage initial M0, nous avons ajouté une partie matérialisant la variable timer. Cette dernière, formée de : transition t12, t13, et t14 et la place p0, nous permettra de conclure qu'il y a des intrus dans le voisinage.

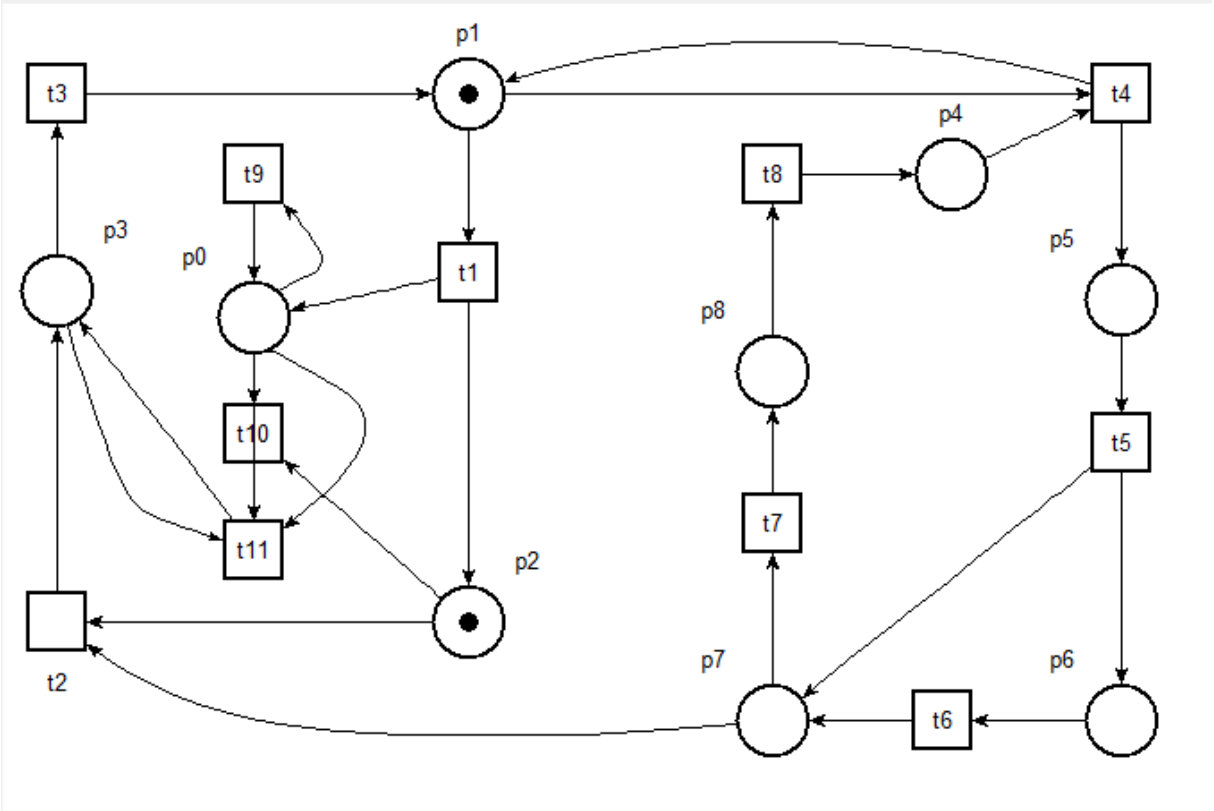


Figure 17:*RDP-T du modèle réduit du protocole AODV face à l'attaque sinkhole.*

Description des transitions du modèle RDPT (Réseau de petri) pour le protocole AODV face à l'attaque sinkhole

T1 : la source diffuse le paquet RREQ pendant la découverte de la route.

T2 : Réception de l'ACK par l'émetteur.

T3 : à la réception du paquet RREQ par la destination répond par un paquet RREP contenant la route arriver à destination.

T9 : Incrémentation de la valeur de la variable nbhop après chaque unité de temps (time slot)

T10 : Détection de l'attaque Sinkhole

T11 : Initialisation de la variable nbhop quand l'attaque n'a pas eu lieu ou elle n'a pas été détectée.

T9,T10,T11 : Mécanisme de détection de l'attaque sinkhole

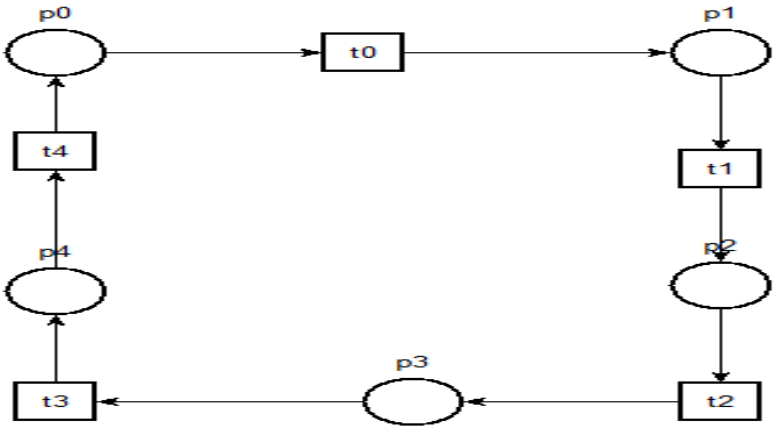
T4 : les nœuds intermédiaires peuvent également envoyer un paquet RREP à la source s'ils ont une route vers la destination dans leur table de routage.

T5 : Débuter une nouvelle communication.

T6 : Les nœuds voisins reçoivent RREQ et vérifient si le nœud destination est connu ou s'ils ont déjà une route valide vers ce nœud.

❖ Nous supposons, dans cette partie, qu'il y a une attaque de type sinkhole organisée par un nœud malicieux bien implanté dans le réseau. Ce nœud malicieux se présente comme un nœud favori sur le chemin de routage (dans le modèle RDP-T présenté c'est le nœud récepteur qui jouera le rôle du sinkhole). Alors, l'arc liant la transition "*t*5" à la place "*p*7", sur la figure 17, lorsqu'il est ôté, il simulera la fonction d'une attaque sinkhole passive (obsorption des paquets). Dans ce cas, nous avons modélisé ce comportement par la variable *nbhop*. Cette variable fonctionne comme un compteur. Elle est incrémentée après chaque changement de place (c'est ACk.nbhop <> nb. Sauts) nombre de sauts dans la place à laquelle le paquet arrivera et comparée la variable nb. Sauts dans notre algorithme (chapitre3 ligne9), cette variable *nbhop* est imagée par la place "*p*0". La transition "*t*9"incrémente la variable *nbhop*. Après chaque unité de temps, "*p*0" sera incrémentée par un jeton, la transition "*t*10"modélise la fonction detectsinkhole (), elle compare le contenu de la variable *nbhop* (nombre de jetons dans la place "*p*0") avec la valeur nbsauts Sur le modèle présenté par la figure 17, Si la transition "*t*11" est tirée, celà expliquera que le paquet RREP n'a pas reçu d'échos (aucune réponse n'a été donnée par les voisins), et comme dans notre cas, l'attaque sinkhole est détectée après avoir. La transition "*t*11", quand le réseau opère dans l'absence d'une attaque, met à zero le compteur *nbhop* pour permettre au nœud de continuer de fonctionner.

Description des transitions du graphe (figure17)



La figure si dessus visualise le comportement opérationel d'une manière globale d'un système de noeuds de capteurs. Supposons que le nœud "*A*" possède des données à communiquer au nœud "*B*". Noeud "*A*" initialise le processus par l'envoi d'une requète (*RREQ*) au nœud "*B*". La destination "*B*"répond par un paquet (*RREP*). Dès la réception du *ACK*, le nœud "*A*" envoie son paquet de données. Si le paquet est bien reçu, le noeud "*B*" informe son interlocuteur, le

noeud "*A*", par un message de confirmation sous forme d'un acquitement (*ACK*). Si le nœud "*A*"a un message de données fragmenté en plusieurs fragments, il attend durant des intervalles aléatoires après chaque fragment transféré avec succès.

4. Conclusion

Dans ce chapitre nous avons présentés une Modélisation formèle du protocole AODV dans les réseaux de capteur sans fil et le protocole face une attaque sinkhole,le mécanisme de la solution proposé pour détecter cette attaque dans les RCSFs.

Conclusion générale

Les réseaux de capteurs sans fil peuvent s'apparenter aux réseaux ad hoc sans fil, mais ils se différencient par plusieurs limitations, ce qui ne permet pas d'appliquer directement les solutions de sécurité existantes dans les réseaux Ad hoc dans les RCSFs.

Pour pouvoir développer des solutions de sécurité adaptées à ces réseaux, il faut bien comprendre leurs contraintes. En effet, le manque de ressources de tels réseaux les rend particulièrement vulnérables aux menaces de sécurité compromettant leur disponibilité.

Cependant, Les services de sécurité du protocole AODV dans les RCSFs ne protégeront pas contre une attaque sinkhole.

Par conséquent, dans ce mémoire, nous présentons un mécanisme de vérification pour nous défendre efficacement et de manière fiable contre les attaques sinkhole dans le protocole AODV.

Nous avons développé une solution algorithmique apte à satisfaire les besoins de sécurité. Le travail que j'ai mené mon permis de découvrir le domaine des RCSFs une vaste connaissance non seulement sur ses réseaux à faible puissance mais aussi sur le protocole de routage pour les réseaux à faible puissance tel que le protocole AODV et j'ai apprendre l'outil de modélisation Tina (time petri net analyzer) qui est un nouveauté pour moi.

Perspectives

Plusieurs perspectives de recherche futures peuvent être envisagées sur la base de la solution présentée dans ce mémoire.

De plus, je souhaite prochainement ajouter des nœuds mobiles dans la topologie de simulation, pour que l'attaquant puisse se déplacer.

Bibliographie

[1] M. Kaur, “Détection and Mitigation of Sinkhole Attack in Wireless Sensor network,” pp. 218–222, 2016.

[2] M. M. Zanjireh, A. Shahrabi et H. Larijani, “ANCH : A New Clustering Algorithm for Wireless Sensor Networks”,2013.

[3] S. Chettibi, “Protocole de routage avec prise en compte de la consommation

D’énergie pour les réseaux mobiles ad-hoc ”,2009.

[4] F. Nack, “An overview on wireless sensor networks technology”, pp. 1–8, 2010.

[5] N. Nejah, K. Abdennaceur, “Etude et proposition d’une méthode de géolocalisation et de suivi de patients en milieu médicalisé”, Novembre 2019.

[6] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary: Wireless Sensor Network Security: A Survey. Security in Distributed, Grid, and Pervasive Computing, Editor: Yang Xiao, Chapter 17, Auerbach Publications, CRC Press, 2006.

[7] D. Martins, H. Guyennet, D. Martins, H. Guyennet, and É. De, “État de l ’ art - Sécurité dans les réseaux de capteurs sans fil To cite this version : HAL Id : hal-00661898 Etat de l ’ art Sécurité dans les réseaux de capteurs sans fil,” 2012.

[8] Germano Guimara˜es, Eduardo Souto, Djamel Sadok, and Judith Kelner. Evaluation of security mechanisms in wireless sensor networks. IEEE Proceedings of the 2005 Systems Communications (ICW’05), 2005.

[9] S. M. Hedetniemi, S. H. Hedetniemi, and A. Liestman,«A Survey of Gossiping and Broadcasting in Communication Networks», Networks, vol. 18, 1988.

[10] W. Drira, C. Bekara, and M. Laurent, “Sécurité dans les réseaux de capteurs sans fil : conception et implémentation,” pp. 1–56, 2016.

[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):370–380, 2006.

[12] E. C. Ngai, J. Liu, and M. R. Lyu, “On the intruder detection for sinkhole attack in wireless sensor networks” in 2006 IEEE International Conference on Communications, 2006, pp. 33833389.

[14] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, “Journal of Computer and System Sciences Detection and mitigation of sinkhole attacks in wireless sensor networks,” J. Comput. Syst. Sci., vol. 80, no. 3, pp. 644–653, 2014, doi: 10.1016/j.jcss.2013.06.016.

[15] S. Roy, S. Singh, S. Choudhury, N. Debnath, Countering sinkhole and black hole attacks on sensor networks using dynamic trust management, in: Proceedings of IEEE Symposium on Computers and Communications, 2008, pp. 537–542.

[16] B. Choi, E. Cho, J. Kim, C. Hong, J. Kim, A sinkhole attack detection mechanism for LQI based mesh routing in WSN, in: Proceedings of International Conference on Information Networking, 2009, pp. 1–5.

[17] Chris Karlof and David Wagner. Secure routing in Wireless sensor networks: attacks and countermeasures. Ad Hoc Networks, 1(2-3) :293–315, 2003.

[18] I. D. Chokers and E. M. Belding-Royer, “AODV routing protocol implementation.

[19] p. Maidamwar and N. Chavhan,"A Survey on Security Isssue To Detect Wormhole Attack In WSN,"International Journal On Adhoc Networking Systems, vol.2,no. 4,pp.37-50,2012.

[20]George W. Kibirige,"A Survey on Detection of Sinkhole Attack in Wireless Sensor Network",Department of Informatics Sokoine University of Agriculture, SUAMorogoro, Tanzania

Annexes

Attaque du trou gris (grey hole attack) : L'attaque du trou gris est une variante améliorée de l'attaque du trou noir. Contrairement au trou noir, le trou gris relaye certaines informations. Par exemple, le trou gris va relayer toutes les informations concernant le routage, sauf pour des informations critiques. Ce type d'attaque est ainsi plus difficile à détecter que l'attaque du trou noir, le capteur malicieux tant qu'il se comporte de manière normale ne peut être détecté. [7]

Attaque brouillage radio : Un attaquant va envoyer des ondes sur la même fréquence que le réseau de capteurs sans fil. Ainsi les nœuds ne pourront plus communiquer car le médium est saturé par le brouillage radio. [15]

Attaque flooding : L'attaquant utilisera un appareil spécifique avec un ou plusieurs nœuds malveillants ou une forte puissance de lancement pour envoyer le message au réseau régulièrement pour le saturer (une attaque active qui est de même type que les attaques de type déni de service). [15]

Attaque par inondation avec le message Hello (Hello flooding) : Les protocoles de découvertes sur les réseaux ad-hoc utilisent ce qu'on appelle des messages de type HELLO pour s'insérer dans un réseau et pour découvrir ses nœuds voisins. Dans une attaque dite de HELLO Flooding, un attaquant va utiliser ce mécanisme pour saturer le réseau et consommer son énergie. [14]

Un nœud malicieux X avec une connexion puissante qui lui permet d'envoyer à un grand nombre de nœuds des messages de type HELLO, de manière continue. Les nœuds voisins V vont alors essayer de lui répondre, même s'ils sont situés à des distances qui ne permettent pas d'atteindre le nœud malicieux. A force de tenter de répondre à ces messages ils vont petit à petit consommer l'intégralité de leur énergie. [14]

Attaque Usurpation d'identités (Sybil attack) : Dans ce type d'attaques, le nœud malveillant prend un grand nombre d'identités qui peuvent être volés ou imaginaires. Cette attaque peut être utilisée contre les protocoles de routage. [9]