République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de Fin d'études

En vue de l'obtention du diplôme de Master en Informatique

Option : Réseau et sécurité

Thème

Confidentialité d'emplacement simultané d'un nœud source et d'une station de base dans les réseaux de capteurs sans fil

Présenté par :

BENAI DIHIA & ZAIDI AMIRA

Devant le jury composé de :

Président :	Dr. M. SADI	M.C.B U.A/Mira Béjaia
Examinateur :	Dr. F.BOUCHEBAH	M.C.B U.A/Mira Béjaia
Examinateur :	Doctorant. A. BERAZA	U.A/Mira Béjaia
Promoteur :	Dr. L.KHENOUS	M.C.B U.A/Mira Béjaia

Année Universitaire : 2022/2023

Remerciements

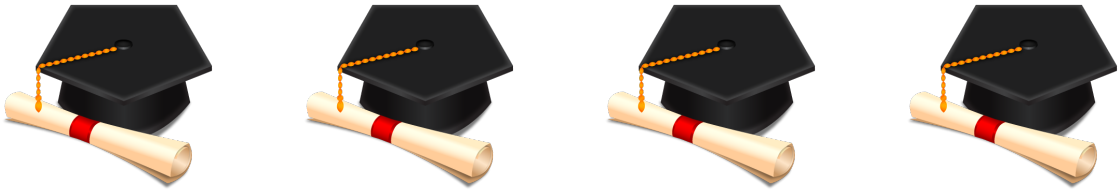
Tout d'abord, nous tenons à remercier ***Dieu****, de nous avoir donné la santé, la volonté et la patience à terme notre formation de master et pouvoir réaliser ce travail.*

Nous tenons à remercier notre promoteur Mr ***KHENOUS Lachemi*** *pour la confiance et l'intérêt qu'il nous a témoigné durant toute la période de travail, pour son aide, ses précieux conseils, sa patience .*

Nous sommes très honorées de la participation de Mr ***SADI Mustapha*** *, Mr* ***BOUCHEBAH Fatah*** *et doctorant* ***BERAZA Abd Rahmane*** *dans notre jury de soutenance. On les remercions vivement pour avoir accepté de juger ce travail.*

Nous tenons à remercier tous nos enseignantes qu'on a eu le plaisir de côtoyer pendant la période de notre formation à l'université de Béjaia.

Un grande merci à nos familles pour leurs soutiens aussi bien moral que financier et pour leurs sacrifices.



Dédicace

C'est avec une grande modestie et un immense plaisir que je dédie ce modeste travail :

A l'homme, mon précieux offre de dieu, ma source de courage ma réussite et tout mon respect, mon chère papa ***Mohammed*** *qui représente mon guide et le symbole de la bonté.*

A la femme, ma source de patience, de tendresse, et d'amour, ma chère et adorable mère ***Houria*** *pour tous ses sacrifices et ses encagements.*

A mes chères et belles ***sœurs****, ainsi mon* ***frère*** *pour leurs présence à mes côtés et leurs soutiens moraux*

A mon chère et mon petit neveu ***Mastinas****.*

A ma chère binôme ***Amira*** *pour tous les moments qu'on a passé ensemble.*

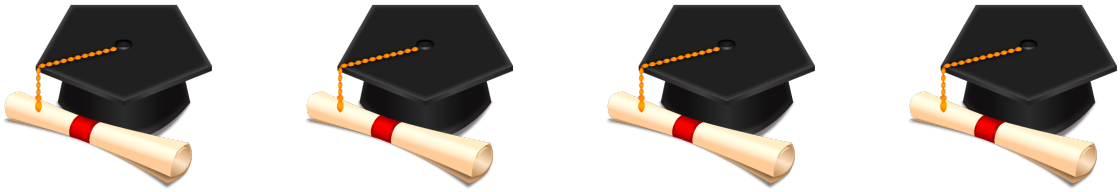
A ma copine de chambre ***Amira*** *pour tout son soutien.*

A mes chères amies ***Imane, Kenza, Aicha, Ouradia et Rayel, Zehra***

A tous mes amis de promotion de ***2 -ème année master réseau et sécurité****, en particulier* ***Lynda, Mayelisse*** *et* ***Hadir****.*

Merci à tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire.

DIHIA



Dédicace

dédie ce modeste travail à :

A mon très cher père Mohamed .

A ma très chère mère Nacera.

En reconnaissance de tous vos sacrifices, de votre soutien inconditionnel, De vos encouragements et de votre amour qui ont été la clé de ma réussite, Je prie pour que Dieu vous accorde une bonne santé et une longue vie.

A mes frères Amar et Seif Eddine et ma sœur Chahinaz

Pour leur disponibilité à entendre mes frustrations et les sources de mon stress. Avec mes souhaits de bonheur, santé, et de réussite dans leur vie.

A mes grands parents et ma famille, mes proches.

Qui me donne de l'amour et de la vivacité.

A tous mes amis Dihia, Yasmine, Hadir, Meissa

Qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

A tous ceux que j'aime et qu'ils m'aiment

Qu'ils trouvent dans ce travail l'expression de mes sentiments les plus affectueux.

AMIRA

Table des matières

Liste des tableaux

Table des figures

List of Algorithms

Liste des abréviations

BT *Bidirectional Tree*

CEM *Cyclic Entrapment Method*

DBT *Dynamic Bidirectional Tree*

FRW *Forward Random Walk*

GROW *Greedy Random Walk*

LPR *Location Privacy Roating*

MPR *Multi-Parent Routing*

RCSF *Reseaux de Capteurs Sans Fil*

RW *Random Walk*

SB *Station de Base*

TTL *Time To Live*

ZBT *Zigzag Bidirectional Tree*

Introduction générale

Au fil des années, les réseaux de capteurs sans fil (RCSF) ont acquis une importance considérable dans divers domaines. Ces réseaux sont composés de multiples nœuds capteurs qui s'activent pour collecter et transmettre des données à une station de base centrale. Ces capteurs sont déployés de manière hétérogène, que ce soit sur une zone géographique ou sur des objets spécifiques ; sans qu'une position préalablement déterminée soit nécessaire.

Les réseaux de capteurs sans fil connaissent une popularité croissante et leur utilisation se développe chaque jour dans divers domaines. Ils sont utilisés pour l'acquisition d'informations environnementales dans de nombreux secteurs. Les avancées dans les technologies de communication sans fil, la miniaturisation des capteurs, leur coût réduit et l'expansion de la gamme des capteurs disponibles (tels que les capteurs thermiques, d'humidité, optiques, de vibrations, etc.) ont considérablement élargi les possibilités d'application de ces réseaux de capteurs. Ils permettent ainsi la collecte et le traitement d'informations complexes provenant de l'environnement, telles que la météorologie, l'étude des courants, l'acidification des océans, la dispersion de polluants, et bien d'autres encore.

Le déploiement croissant des réseaux de capteurs a fait émerger la confidentialité comme l'un des problèmes majeurs à résoudre pour assurer leur succès. La confidentialité dans les réseaux de capteurs peut être classée en deux classes : la confidentialité axée sur le contenu et la confidentialité contextuelle [34]. La confidentialité axée sur le contenu concerne la capacité des adversaires à connaître le contenu des transmissions dans les réseaux de capteurs [34]. Cependant, malgré le mécanisme de chiffrement [35] des données, les supports de communication sans fil exposent toujours des informations contextuelles sur le trafic transporté sur le réseau. La confidentialité contextuelle considère la capacité des adversaires à déduire des informations à partir d'observations de capteurs et de communications sans avoir accès au contenu des messages. Les comportements des capteurs, tels que les modèles de communication et le chemin de routage d'un message, peuvent donner aux adversaires des indices pour déduire des informations sur le réseau, telles que l'emplacement de la source d'un message ou l'emplacement de la station de base.

La protection de l'emplacement de la source dans les RCSF devient un problème très

important lorsqu'un réseau de capteurs est utilisé pour surveiller des cibles précieuses ou que la source est un objet sensible. Par exemple, les paquets de navigation Web sortant d'une maison dans un réseau permettent à un espion d'analyser les habitudes de navigation d'une famille si l'emplacement source de ces paquets peut être déterminé, grâce à l'analyse du trafic.

De même, un adversaire peut détruire une station de base une fois découverte, rendant l'ensemble du réseau de capteurs inopérant, car la station de base est un point central de collecte de données et donc de défaillance.

Dans ce mémoire, nous nous focalisons sur le problème de préservation de la confidentialité, simultané, d'un nœud source et d'un récepteur dans le réseau. Nous explorons quelques principales techniques, protocoles et mécanismes de protection qui peuvent être utilisés pour prévenir la divulgation de l'emplacement des nœuds et des stations de base dans un environnement sans fil. L'objectif de ce travail est de proposer une solution efficace qui assure une forte protection de la confidentialité d'emplacement dans les RCSF qui soit plus performante en termes de coût énergétique et de latence.

Le présent travail s'articule autour de quatre chapitres :

- Le chapitre 1, intitulé "Notions de bases sur les réseaux de capteurs sans fil ", présente des informations générales sur les réseaux de capteur sans fil, ainsi que les différentes techniques, caractéristiques et domaines d'applications des RCSF.
- Le chapitre 2, intitulé " Etat de l'art sur la confidentialité d'emplacement de la source et de la station de base dans les réseaux de capteur ", présente quelques principales existantes solutions pour protéger la confidentialité d'emplacement de la source et de la station de base dans les RCSF.
- Le chapitre 3, intitulé "Solution proposée ", explique notre solution proposée pour assurer la confidentialité d'emplacement, simultané, de la source et de la station de base.
- chapitre 4, intitulé " Evaluation de performances ", montre l'évaluation analytique et par simulation de notre solution sous MATLEB.

Nous terminons ce mémoire par une conclusion générale et quelques perspectives qui pourraient contribuer à l'amélioration du système à l'avenir.

Chapitre 1

Notions de bases sur les RCSF

1.1 Introduction

Les réseaux de capteurs sans fil (RCSF) ont récemment suscité un grand intérêt au sein de la communauté des chercheurs, en raison de leurs large éventail d'applications. Ces réseaux sont composés d'un grand nombre des nœuds capteurs qui communiquent entre eux pour transmettre des données collectées à partir de l'environnement. [16] Malheureusement, en raison de leurs nature distribuée et de leur déploiement dans des zones reculées, ces réseaux sont vulnérables à de nombreuses menaces de sécurité qui compromettent leur bon fonctionnement. Dans ce qui suit, nous étudierons les réseaux de capteurs sans fil, en abordant les caractéristiques, les différents domaines d'application, l'architecture ainsi que les facteurs influençant la conception des réseaux de capteurs. Nous présenterons, également, la sécurité dans les réseaux de capteurs et les différentes attaques possibles dans ce domaine.

1.2 Définition d'un capteur

Un capteur également appelé senseur, est un système conçu pour détecter un phénomène physique et le convertir en signal électrique représentatif. Les capteurs sont des dispositifs alimentés par des batteries qui ont la capacité de communiquer entre eux et de détecter des évènements dans leur zone de détection. Ils peuvent être utilisés dans une grande variété d'applications environnementales telles que, la mesure de la température, l'humidité, de la pression, etc. Les capteurs sont également équipés de matériel permettant d'effectuer des communications sans fil par ondes radio. [1]

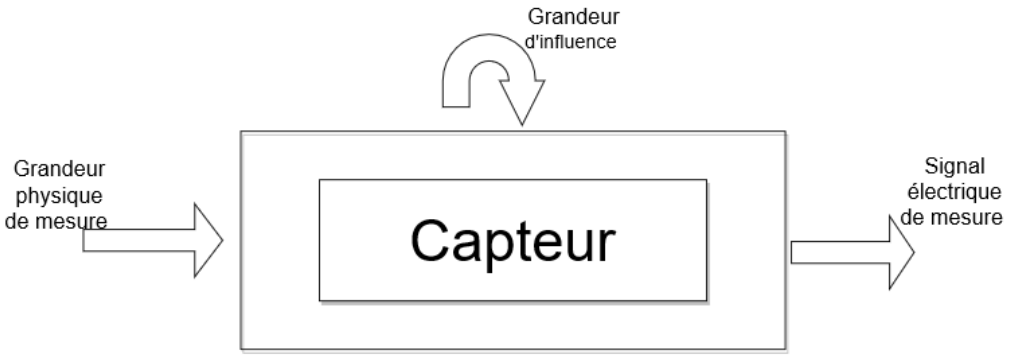


FIGURE 1.1 – Fonctionnement d'un capteur [1]

1.3 Réseau de capteurs sans fil (RCSF)

Un réseau de capteurs est considéré comme un type de réseau ad hoc, en raison de l'absence d'une infrastructure fixe de communication et d'administration centralisée. Il est composé d'un grand nombre de nœuds de capteurs, qui sont déployé de manière dense à l'intérieur d'un phénomène. [17] Ces nœuds sont des capteurs intelligents, également appelés‘’smart sensors", qui jouent à la fois le rôle d'hôtes et de routeurs, permettant ainsi aux données de se propager dans le réseau via la communication multi-saut. Les données collectées par les nœuds capteurs sont traitées et transmises à une station de base pour une analyse spécifiques où une transmission ultérieure à des systèmes externes. [2]

1.4 Caractéristiques des réseaux de capteurs sans fil

Les RCSF possédent plusieurs caractéristiques. Voici quelques-unes des leurs principales caractéristiques des RCSF : [3]

1.4.1 Scalabilité

La scalabilité, c'est-à-dire la capacité à évoluer à grande échelle, est un aspect critique pour les réseaux de capteurs, afin de gérer efficacement des millions de nœuds sans compromettre les performances globales du réseau.

1.4.2 Grande densité de capteurs

Les réseaux de capteurs sont généralement déployés dans un environnement très dense. Cette densité permet une collecte de données plus élevée et une surveillance plus précise.

1.4.3 Communication sans fil

Les réseaux de capteurs utilisent la communication sans fil, ce qui permet un déploiement facile et économique, sans avoir besoin d'une infrastructure filaire coûteuse.

1.4.4 Faible consommation d'énergie

Les capteurs sont alimentés par des batteries, qui ont une durée de vie limitée. Par conséquent, les capteurs doivent être conçus pour minimiser leur consommation d'énergie et prolonger la durée de vie de la batterie.

1.4.5 Application diverse

Les réseaux de capteurs peuvent être utilisés dans différents domaines d'application, tels que la surveillance de l'environnement, la surveillance de la santé, le Contrôle de la circulation, etc.

1.5 Domaines d'application des RCSF

Les RCSF sont utilisés dans divers domaines, tels que le militaire, l'environnemental, le sanitaire et autres domaines commerciaux. Ils peuvent également être utilisés dans des catégories supplémentaires telles que l'exploration spatiale, le traitement chimique et les secours en cas de catastrophe. [2]

1.5.1 Domaine militaire

Les RCSF peuvent faire partie des systèmes militaires de commandement, de renseignement, de surveillance, de reconnaissance et de ciblage (C4ISRT). Ils permettent aux chefs et aux commandants de surveiller en permanence l'état des troupes, des équipements et des munitions sur le champ de bataille grâce à l'utilisation de réseaux de capteurs. Chaque troupe, véhicule, équipement et munition peut être équipé de petits capteurs qui signalent son état. Ces rapports sont collectées dans des nœuds de collecte et envoyées aux chefs de troupe. Les données peuvent également être transmises aux niveaux supérieurs de la hiérarchie de commandement tout en étant agrégées avec les données provenant d'autres unités à chaque niveau. Les réseaux de capteurs sont utilisés pour la détection des attaques nucléaires, biologiques et chimiques, et servent de système d'alerte chimique ou biologique qui permet aux forces de réagir rapidement et de réduire le nombre de victimes.

1.5.2 Domaines environnementaux

Les réseaux de capteurs peuvent être utilisés dans diverses applications environnementales, telles que le suivi des mouvements des oiseaux, des petits animaux et des insectes, la sur-

veillance des conditions environnementales impactant les cultures et le bétail, la détection chimique/biologique, l'agriculture de précision et la détection des incendies de forêt. Par exemple, le déploiement de capteurs thermiques dans une forêt peut aider à détecter l'origine exacte du feu aux utilisateurs finaux avant que le feu ne se propage de manière incontrôlable. De même, leur déploiement dans des environnements urbains et chimiques peut aider à détecter la pollution et analyser la qualité de l'aire.

1.5.3 Domaines médicaux

Parmi les utilisations sanitaires des réseaux de capteur est la surveillance intégrée des patients, l'administration de médicaments dans les hôpitaux et la surveillance des médecins et des patients à l'intérieur d'un établissement de santé. [4,5]. Chaque capteur a une tâche spécifique, par exemple, un capteur peut détecte la fréquence cardiaque tandis qu'un autre capteur détecte la pression sanguine. De plus, ces capteurs peuvent détecter les mouvements anormaux (chutes, cris, etc.) de personnes particulières (personnes handicapées, personne âgées, etc.).

1.5.4 Domaines commerciaux

Les réseaux de capteurs sont de plus en plus utilisés dans le domaine commercial pour améliorer l'efficacité, la sécurité et la qualité des opérations. Par exemple, dans le suivi des stocks, chaque capteur peut être attaché à un article dans un entrepôt, ce qui permet aux utilisateurs de connaître l'emplacement exact de l'article et de compter le nombre d'articles de la même catégorie, contrôle de la qualité, et aussi la gestion des bâtiments qui peuvent être utilisés pour surveiller les systèmes de chauffage, de ventilation et de climatisation, afin d'optimiser l'utilisation de l'énergie et de réduire les coûts d'exploitation.

1.6 Comparaison réseaux de capteurs et réseaux ad hoc

Le tableau suivant illustre la différence entre RCSF et réseau ad hoc : [33]

Réseau de capteur sans fil	**Ad hoc**
Nœuds collaborent pour remplir un objectif	Chaque nœud a son propre objectif
Flot de données tous vers un (Many-to-one)	Flot tous vers tous (Any-to-any)
Très grand nombre de nœuds n'ayant pas tous un identificateur	Notion d'ID
Énergie est un facteur déterminant, nœud capteur sujet aux pannes	Débit est majeur
Objectif ciblé	Générique / communication

TABLE 1.1 – Comparaison réseau de capteur / ad hoc

1.7 Les facteurs influençant la conception des réseaux de capteurs

La conception d'un réseau de capteurs peut être influencée par différents facteurs, notamment la tolérance aux pannes, la scalabilité, les coûts de production, la topologie du réseau de capteurs, les contraintes matérielles, les supports de transmission et la consommation d'énergie. Ces facteurs peuvent être utilisés pour comparer plusieurs schémas de réseau de capteurs sans fil.

1.7.1 Tolérances en panne

Ensemble des techniques de conception des systèmes qui continuent à fonctionner même en présence de pannes. Ces pannes peuvent être causées par le manque d'énergie, des dommages physiques ou des interférences environnementales. La défaillance de ces nœuds ne doit pas affecter le fonctionnement global du réseau de capteurs. Autrement dit, la tolérance aux pannes est la capacité à maintenir les fonctionnalités du réseau de capteurs sans interruption due aux pannes des nœuds de capteurs [6].

1.7.2 Scalabilité

Pour étudier un phénomène, il est possible d'employer des centaines à des milliers de nœuds de capteurs. Les nouveaux systèmes doivent donc fonctionner avec ces nœuds et avoir la capacité de gérer efficacement une augmentation du nombre de capteurs dans le réseau de capteurs, sans compromettre la fiabilité où la consommation d'énergie.

1.7.3 Coût de production

Les réseaux de capteurs contiennent plusieurs nœuds de capteurs. Le coût d'un seul nœud est très important pour justifier le coût global du réseau. Si ce dernier est plus élevé que celui du déploiement dans un capteur ordinaire, alors le système n'est pas rentable. Par conséquent, le coût d'un nœud doit être faible. [7]

1.7.4 Topologie du réseau de capteurs

La disparition d'un nœud de capteur ainsi que le déploiement d'un nouveau nœud rendent la topologie du réseau instable. Tout cela nécessite une gestion minutieuse de la maintenance de la topologie.

1.7.5 Consommation d'énergie

Dans les réseaux de capteurs, la consommation d'énergie est un facteur de conception important, mais pas une considération principale, car elle influence la durée de vie du réseau. Cette énergie est consommée par différents capteurs pour les opérations de captage, de traitement des données et de communication.

1.8 Architecteur d'un réseau de capteurs sans fil

Un réseau de capteurs se compose de plusieurs nœuds de capteurs qui utilisent la communication multi-saut pour se communiquer. A l'aide de cette architecteur multi-saut, un RCSF transmet les données collectées à un nœud SB. (Voire la figure 1.2) ; ce dernier agit comme une passerelle pour les réseaux de capteurs. Ce nœud a également d'autre capacité de traitement de l'information pour une transformation ultérieure, s'il y a lieu. [8]

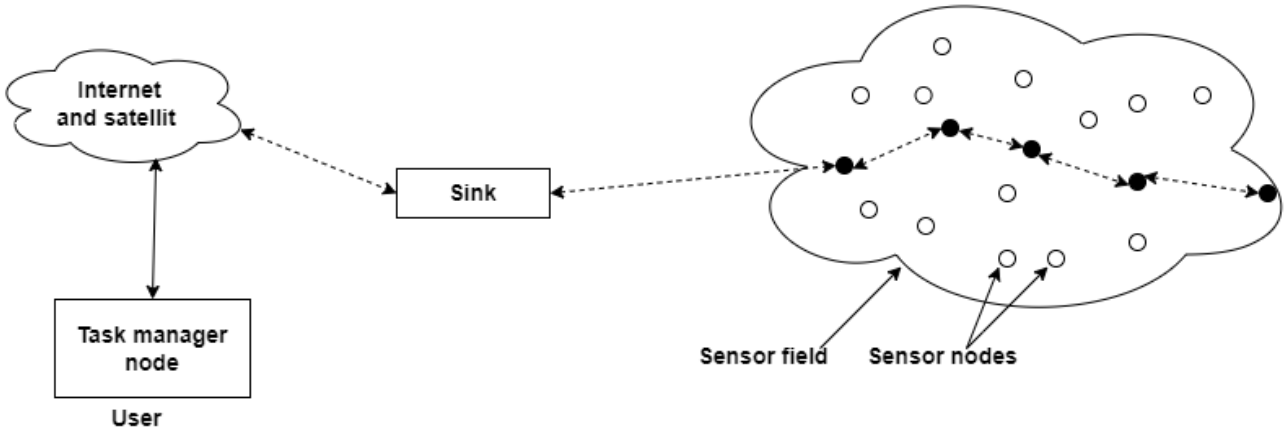


FIGURE 1.2 – Architecture d'un réseau de capteurs sans-fil. [3]

Il existe deux types d'architecture pour les réseaux de capteurs sans fil : l'architecture plate et hiérarchique. Dans l'architecture plat, les capteurs peuvent communiquer directement avec la station de base via un mode multi-saut. Alors que l'architecture hiérarchique est proposée pour réduire la complexité de la plupart des nœuds de capteurs, où les nœuds représentent des clusters appelés Cluster-Head qui transmettent directement les données à la station de base via un mode multi-saut entre les Clusters-Heads. [3]

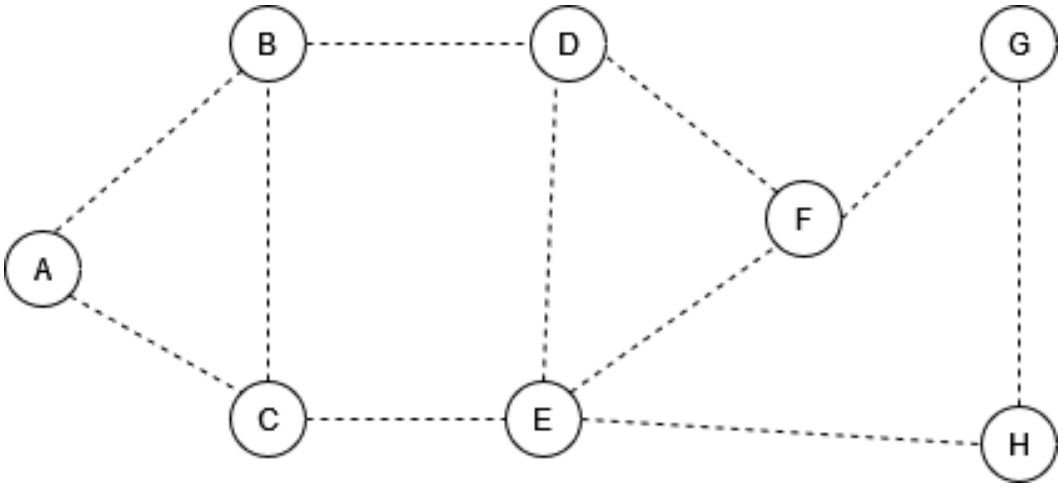


FIGURE 1.3 – Exemple de topologie plate. [3]

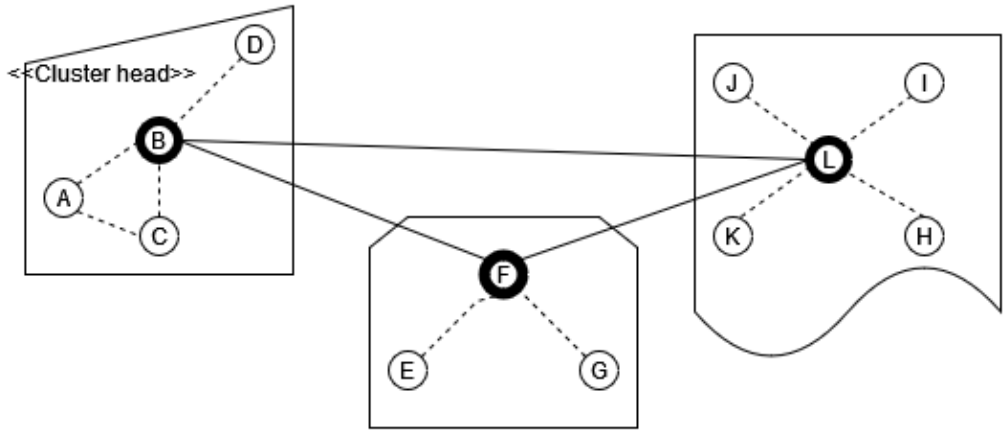


FIGURE 1.4 – Exemple de topologie hiérarchique. [3]

1.9 Sécurité dans les réseaux de capteurs

1.9.1 Objectif de la sécurité

Quelle que soit le réseau, sa politique de sécurité vise à satisfaire les propretés suivantes : [9]

1 . La confidentialité

La confidentialité est une exigence importante qui consiste à rendre l'information inaccessible pour les entités non autorisées.

2 . L'intégrité

L'intégrité vise à garantir que le message reçus n'est pas modifié en cours de route par un adversaire.

3 . L'authentification

Il s'agit de s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être. Les utilisateurs doivent être authentifiés avant de pouvoir accéder aux informations ou aux ressources. [15]

4 . Non-répudiation

Mécanisme permettant de garantir qu'aucun des émetteurs ou récepteurs ne peuvent nier l'envoi ou la réception d'un message. En satisfaisant ces propriétés, on peut aider à protéger les informations et les ressources d'un réseau contre les attaques potentielles.

1.9.2 Les attaques dans les RCSF

En raison de la communication ouverte dans les réseaux de capteurs sans fil, les attaquants peuvent accéder facilement aux communications entre les nœuds de capteurs. Les attaques de sécurité dans les réseaux de capteurs peuvent être de différentes types :

1 . Attaques interne

Une attaque interne est une intrusion malveillante qui est effectuée par une personne autorisée à accéder aux systèmes ou aux données d'une organisation, ou en utilisent t des systèmes informatiques de l'entreprise à des fins malveillantes. Les attaques internes peuvent être intentionnelles ou accidentelles et peuvent causer des dommages considérables à l'entreprise en termes de perte de données, de perte de productivité et de perturbation des activités de l'entreprise. Les attaques internes peuvent être plus difficiles à détecter que les attaques externes car les attaquants internes ont souvent une connaissance approfondie des systèmes, des réseaux et des politiques de sécurité de l'entreprise. Ils peuvent utiliser leur accès privilégié pour accéder à des informations sensibles et éviter les mécanismes de sécurité qui pourraient alerter les systèmes de détection. [36]

2 . Attaques externe

Une attaque externe est une intrusion malveillante dans un système ou un réseau qui provient de l'extérieur de l'organisation. Cette attaque se produit lorsqu'un individu ou un groupe extérieur à l'organisation tente de s'approprier ou d'accéder de manière non autorisée à des informations de localisation sensibles appartenant à l'entreprise ou à ses employés et tout ça se produit à travers plusieurs méthodes, notamment la surveillance de la communication sans fil, l'utilisation de logiciels malveillants pour accéder aux appareils mobiles des employés ou l'interception de données

de localisation en transit, souvent via Internet, en utilisant des techniques comme l'usurpation d'identité. Les attaques externes peuvent être prévenues en mettant en place des mesures de sécurité telles que des pares-feux, systèmes de détection d'intrusion, logiciels antivirus, systèmes de protection contre les dénis de service et des politiques de sécurité strictes. [37]

3 . Attaques local

L'attaque locale est une attaque où un attaquant tente de découvrir l'emplacement physique d'un utilisateur à partir de son appareil local, tel qu'un smartphone ou un ordinateur portable. L'attaquant peut utiliser des techniques telles que la triangulation de signal sans fil ou la surveillance du trafic réseau pour essayer de déterminer la position de l'utilisateur. Les attaques locales peuvent être particulièrement efficaces dans les environnements où l'attaque a un accès physique à l'appareil de l'utilisateur, tel que dans un lieu public où l'utilisateur utilise son appareil. [38]

4 . Attaques global

Une attaque globale veut dire une attaque qui vise à compromettre un grand nombre de systèmes ou d'utilisateurs à travers le monde. Elle tente à suivre la position d'un utilisateur sur une période prolongée en utilisant des données de localisation collectées à partir de sources multiples, telles que des capteurs GPS, des réseaux sans fil et des données de localisation des applications. L'attaquant peut utiliser des techniques de corrélation pour lier les données de localisation à l'identité de l'utilisateur et ainsi suivre ses déplacements. Les attaques globales peuvent être menées par des agences gouvernementales, des entreprises ou des pirates informatiques. [38]

5 . Attaques passives

L'attaque passive est une technique d'attaque qui se produit lorsque les données sensibles sont interceptées ou captées par une personne non autorisée sans être modifiées. Elle se produit lorsqu'un nœud non-autorisé obtient un accès à une ressource sans modifier les données ou perturber le fonctionnement du réseau. Une fois l'attaquant a acquis suffisamment d'informations, il peut produire une attaque contre le réseau, ce qui transforme l'attaque passive en une attaque active. [10]

6 . Attaques actives

Cette attaque peut se produire lorsque les données sensibles sur l'emplacement sont modifiées ou altérées par une personne non autorisée. Par exemple, analyse de trafic, traçage de paquet, l'usurpation d'adresse IP, le phishing. Elle se produit lorsqu'un nœud non autorisé obtient un accès à une ressource en apportant des modifications aux données ou en perturbant le bon fonctionnement du réseau. [11]

7 . Attaque sur le contenu

L'ttaque sur le contenu est une technique d'attaque informatique qui cible directement le contenu d'un fichier, d'un message ou d'une communication, plutôt que les protocoles ou les systèmes qui les transportent. Une attaque sur le contenu fait référence à une méthode d'interception de données sans perturber la communication ou le contenu en cours. Cela peut inclure l'écoute clandestine de conversations ou la collecte de données sans que l'utilisateur ne s'en rende compte ou l'injection de code malveillant dans un site web, la modification de données en transit ou la falsification de paquets de données pour tromper un utilisateur ou un système. Ces types d'attaques peuvent être utilisés à des fins malveillantes, comme le vol de données personnelles, la fraude, ou l'espionnage industriel [12] .

8 . Attaque d'analyse de trafic

L'attaque d'analyse de trafic est une attaque passive qui consiste à surveiller et à analyser le trafic réseau pour intercepter des informations confidentielles telles que des identifiants de connexion, des mots de passe, des données de carte de crédit, des e-mails et des fichiers. Cette technique est souvent utilisée par les cybercriminels pour espionner des connexions réseau non sécurisées ou mal sécurisées. [13]

9 . Injection de nœuds malveillants

Les attaquants peuvent ajouter des nœuds malveillants dans le réseau de différente manière. Ces nœuds malveillants peuvent être conçus pour intercepter, modifier ou même supprimer des données, ce qui peut avoir des conséquences graves sur la fiabilité et la sécurité du réseau.

10 . Compromissions des nœuds malveillants

Les attaquants peuvent ajouter des nœuds malveillants dans le réseau de différente manière. Ces nœuds malveillants peuvent être conçus pour intercepter, modifier ou même supprimer des données, ce qui peut avoir des conséquences graves sur la fiabilité et la sécurité du réseau. [14]

1.10 Conclusion

Dans ce chapitre, on a découvert les réseaux de capteur sans fil, et leur application, ainsi les architectures d'un réseau de capteur sans fil. Ensuite nous avons présenté les différents objectifs de sécurité qui sont nécessaire dans les réseaux de capteur. L'utilisation des réseaux de capteur a des avantages considérables comme le faible coût, grande flexibilité, facilité de déploiement, et une faible consommation d'énergie. Dans le chapitre suivant, on donnera un état de l'art des principales solutions existantes pour assurer la confidentialité de l'emplacement d'une source et d'une station de base.

Chapitre 2

État de l'art sur la confidentialité d'emplacement de la source et de station de base dans les réseaux de capteur

2.1 Introduction

La protection de la confidentialité est l'un des défis les plus importants qui menace le déploiement réussi des systèmes de capteurs. Bien que de nombreux problèmes liés à la protection de la confidentialité puissent être résolus par des mécanismes de sécurité, il existe un problème de protection de la confidentialité dans les réseaux de capteurs qui ne peut pas être résolu de manière adéquate par la sécurité du réseau : la protection de l'emplacement de la source et de la station de base. Dans ce chapitre on présente les travaux antérieur réalisés par un ensemble d'auteurs pour préserver la confidentialité de l'emplacement de la source et du station de base dans les réseaux de capteurs, puis on conclut par une comparaison des travaux présentés en se basant sur les critères suivants : période de sécurité, latence et consommation d'énergie.

2.2 Travaux antérieurs

Cette partie présente les travaux d'un ensemble d'auteurs qui ont proposées un ensemble des solutions pour garantir la confidentialité de l'emplacement de la source et de la station de base.

De nombreux réseaux de capteurs ont utilisé des méthodes de routage basées sur l'inondation et le routage à chemin unique pour assurer la confidentialité de l'emplacement de la source et de la station de base.

Dans [18, 19], la méthode d'inondation a été utilisée, basée sur la diffusion des données et des messages de contrôle. L'émetteur d'un message transmet son message à chacun de ses voisins, qui le retransmettent à leur tour à chacun de leurs voisins.

En revanche, la méthode de chemin unique repose sur le principe de transmettre des paquets uniquement à l'un de ses voisins. Dans [20] , Karp et al ont proposé d'utiliser les informations

de l'emplacement d'un nœud et de ses voisins, ainsi que la destination, pour calculer un chemin de routage unique. Dans [21], Niculescu et al ont proposé un routage basé sur la trajectoire, qui utilise les informations d'emplacement associées à un nœud et à ses voisins pour créer un chemin de routage le long d'une trajectoire spécifiée. Dans le protocole de routage à chemin unique de base, dès que la source génère un nouveau paquet, elle le transmet au voisin ayant le gradient le plus élevé par le chemin le plus court.

La méthode de l'inondation (flooding) et du routage à chemin unique ne peuvent pas assurer la protection de la confidentialité, car un adversaire peut facilement identifier le chemin le plus court entre la source et le SB. Cela soulève la nécessité d'une nouvelle approche qui réduirait le risque de violation de la confidentialité de l'emplacement de la source. Une approche proposée est l'injection de fausses sources et de faux messages dans le réseau. Pour démontrer l'efficacité des faux messages, il est essentiel qu'ils aient la même longueur que les vrais messages et qu'ils soient également cryptés, afin que l'adversaire ne puisse pas faire la différence entre un faux message et un vrai.

Cependant, les études réalisées sur ces méthodes ont révélé leur inefficacité pour protéger la confidentialité de l'emplacement des sources. Par conséquent, plusieurs autres méthodes ont été proposées, que nous examinerons ci-dessous.

2.3 Confidentialité d'emplacement d'un noeud source

2.3.1 Solution kamat-P et all

Kamat.P et al dans [22] ont apporté des modifications à la méthode de l'inondation (flooding) et au routage à chemin unique. Ils ont ainsi créé une nouvelle méthode appelée routage fantôme, qui consiste en deux phases : dans la première phase les messages sont routés vers une source fantôme en utilisant la marche aléatoire, et dans la deuxième phase les messages sont inondé dans le réseaux vers la station de base.. Le routage fantôme est une technique améliorée visant à protéger la confidentialité de l'emplacement. Son objectif est d'éloigner un adversaire de la source réelle et de le diriger vers une source fantôme en utilisant une marche aléatoire (voir Figure 2.1)

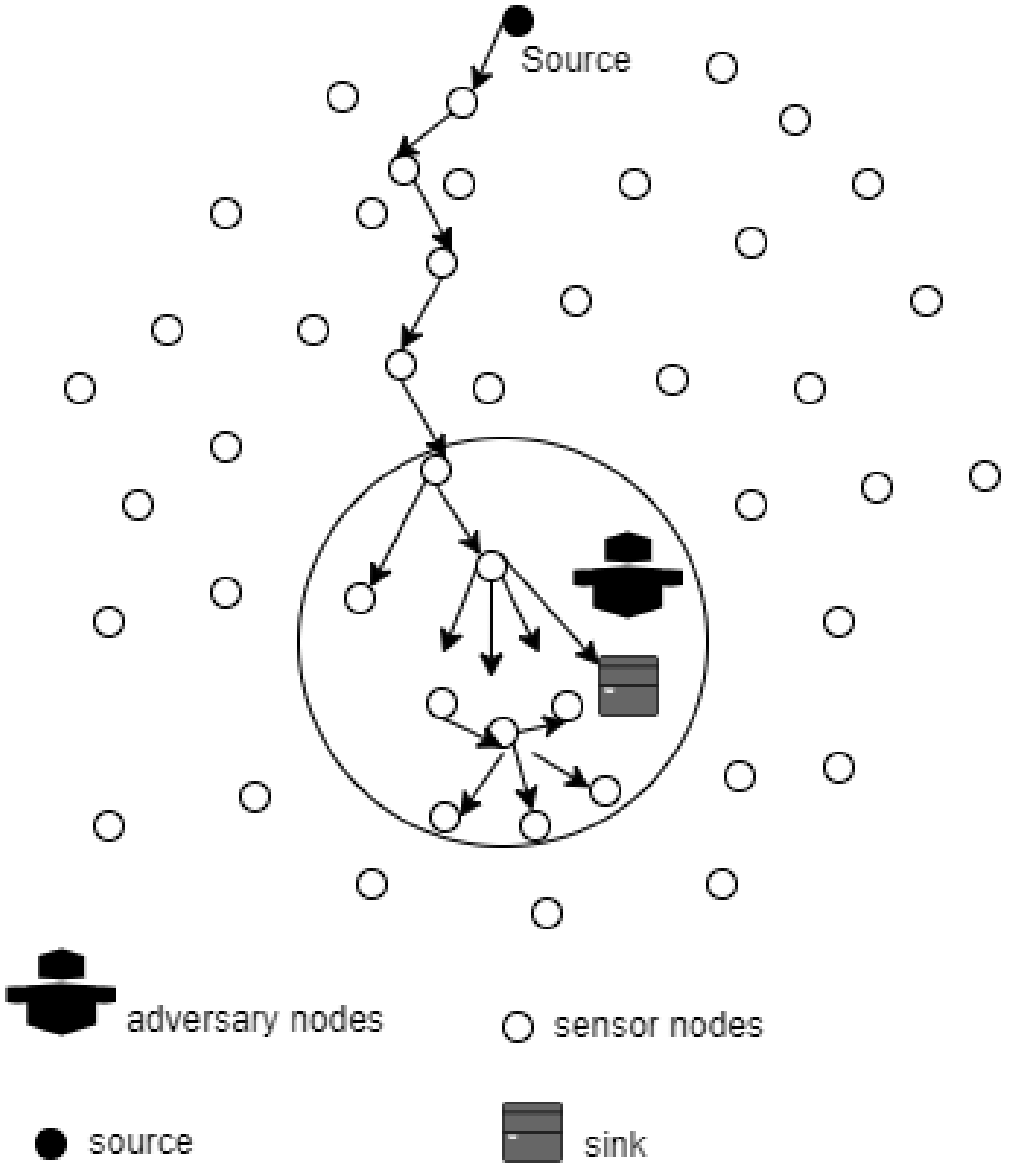


FIGURE 2.1 – Illustration du Phantom Flooding [22]]

2.3.2 Solution de Ouyang-Y et all

La méthode de piégeage cyclique CEM(cyclic entrapment method) [27] est proposée par Ouyang.Y et all tente de fournir la confidentialité d'un noeud source en assurant une période de sécurité élevée. L'approche consiste à générer un faux trafic sous forme de boucle dès le déploiement du réseau de capteurs. Chaque boucle est composée d'un nœud de capteur et d'une séquence de nœuds qui sont disposés de manière séquentielle et à portée les uns des autres. Lorsqu'un adversaire tente de tracer (backtracking) les messages transmet par une source vers un récepteur, quand il arrive sur un noeud activant une boucle, il doit faire un choix du chemin à

suivre ; et s'il fait un mauvais choix alors se retrouve piégé dans cette boucle, ce qui va conduire à parcourir toute la boucle inutilement. En répétant le mauvais choix plusieurs fois, augmentera la période de sécurité.

2.4 Confidentialité d'emplacement d'un noeud récepteur (station de base)

2.4.1 Solution Jian, Y et all

Dans [26] , Jian-Y et al. ont proposé un protocole de routage pour garantir la confidentialité de l'emplacement du récepteur, appelé LPR (Location Privacy Routing). Ce protocole vise à randomiser les chemins de routage afin que la direction des paquets ne soit pas toujours dirigée vers le destinataire. LPR utilise des faux paquets pour rendre les paquets interceptés indéchiffrables pour les adversaires.

Dans ce protocole, chaque nœud capteur divise ses voisins en deux listes : une liste "plus proche" composée des voisins les plus proches du récepteur, et une liste "plus éloignée" composée des voisins les plus éloignés (ou à une distance équivalente) de la station de base. Ces deux listes peuvent être facilement construites en utilisant les distances euclidiennes entre les noeuds, à condition que chaque noeud connaisse sa propre position. Si ce n'est pas le cas, chaque fois que la station de base se déplace vers une nouvelle position, il émet un paquet de balise dans le réseau. Ce paquet contient un nombre de saut initialisé à Zéro. Lorsqu'un capteur reçoit la balise pour la première fois, il incrémente le nombre de sauts du paquet de un, et enregistre le nombre de sauts, puis transmet le paquet à ses voisins. Une fois que la diffusion de la balise est terminée, les voisins échangent les nombres de sauts enregistrés, sur la base desquels ils établissent leurs listes de proximité et d'éloignement. Tout d'abord, cela ne se produit qu'une fois après que le receveur a atteint une nouvelle position. Un adversaire ne peut effectuer qu'un seul mouvement basé sur cette diffusion.

Dans le protocole LPR, le prochain saut d'un capteur vers le récepteur n'est pas fixe. Parfois, le saut suivant ne pointe même pas vers le récepteur, ce qui rend plus difficile pour une attaque de traçage de paquets de réussir.

2.4.2 Contre-mesures pour protéger la station de base contre les attaques d'analyse de trafic

Plusieurs contre-mesures ont été proposées dans [28] pour contrer les attaques d'analyse de trafic visant à dissimuler l'emplacement d'une station de base. ces techniques sont : routage multi-parent (MPR), marche aléatoire (RW), propagation fractale (DF).

1) Schéma de routage multi-parents

Chaque noeud qui désire transmettre un paquet de données vers la station de base. Nous appelons ce schéma le routage multi-parents (MPR). Deux méthodes sont proposées pour configurer des parents multiples pour chaque nœud. Dans la première méthode, le message de balise envoyé par la station de base contient un champ de niveau fixé à niveau 0. Lorsqu'un nœud transmet ce message, il incrémente le niveau de 1. Cette valeur de niveau représente le nombre de sauts qu'un nœud effectue par rapport à la station de base le long d'un chemin particulier. Un nœud de capteur S sélectionne tous les nœuds voisins dont la valeur de niveau est inférieure à celle de S comme nœuds parents. En revanche, dans la deuxième méthode, un nœud surveille tous les messages de balise qu'il reçoit avant de transmettre le premier message de balise. Ainsi, un nœud doit attendre un certain temps avant de transmettre un message de balise. Il sélectionne tous les nœuds dont il reçoit un message de balise en attendant de transmettre le premier message de balise reçu comme ses nœuds parents.

2) Marche aléatoire

La marche aléatoire permet de diversifier le routage afin de réduire l'effet des attaques de surveillance du débit. Dans RW, lorsqu'un nœud reçoit un paquet, il transmet le paquet à l'un de ses nœuds parents avec une probabilité (pr), et il transmet le paquet à un de ses voisins avec une probabilité (1-pr). (Voir la figure 2.6(c)). La technique de marche aléatoire fait en sorte que certains paquets traversent un chemin plus long pour atteindre la station de base que le chemin le plus court. Cela signifie que la technique de marche aléatoire consommera en moyenne plus d'énergie par nœud.

3) Propagation fractale

La possibilité dans MPR et RW qu'un nœud transmette un paquet à son nœud parent est plus élevée que la possibilité qu'il le transmette à l'un de ses autres voisins. Pour cette raison, un adversaire peut exploiter cette situation pour lancer une attaque par corrélation temporelle, soit en injectant des données de rapport anormales, soit en effectuant une surveillance sur une longue période. Afin de remédier aux lacunes du MPR et du RW, une nouvelle technique appelée propagation fractale a été proposée dans [28].

Dans cette technique, plusieurs faux paquets sont créés et propagés dans le réseau afin d'introduire plus de hasard dans le modèle de communication. Lorsqu'un nœud apprend que son voisin transmet un paquet à la station de base, il crée un faux paquet avec une probabilité pc et le transmet à l'un de ses voisins. Pour contrôler la portée de propagation du faux paquet, chaque faux paquet nouvellement généré contient un paramètre TTL (Time To Live) de valeur K. K est une constante connue de tous les nœuds, de sorte qu'un adversaire ne peut pas bloquer le réseau entier en envoyant des faux paquets dont le paramètre TTL est supérieur à K.

Lorsqu'un nœud reçoit un faux paquet, il décrément le TTL de 1. Si la valeur du TTL est supérieure à zéro, le faux paquet est transmis aux nœuds voisins (pas nécessairement en direction de la station de base). Si la valeur du TTL est égale à zéro, le nœud cesse de transmettre le faux paquet. De plus, lorsqu'un nœud apprend que son voisin transmet un faux paquet à quelqu'un d'autre avec une valeur TTL k ($k < K$), il génère et transmet un autre faux paquet avec une probabilité pc et une valeur TTL k-1. Ces faux paquets se répandent dans le réseau, et leurs chemins de transmission forment un arbre (voir figure 4(d)).

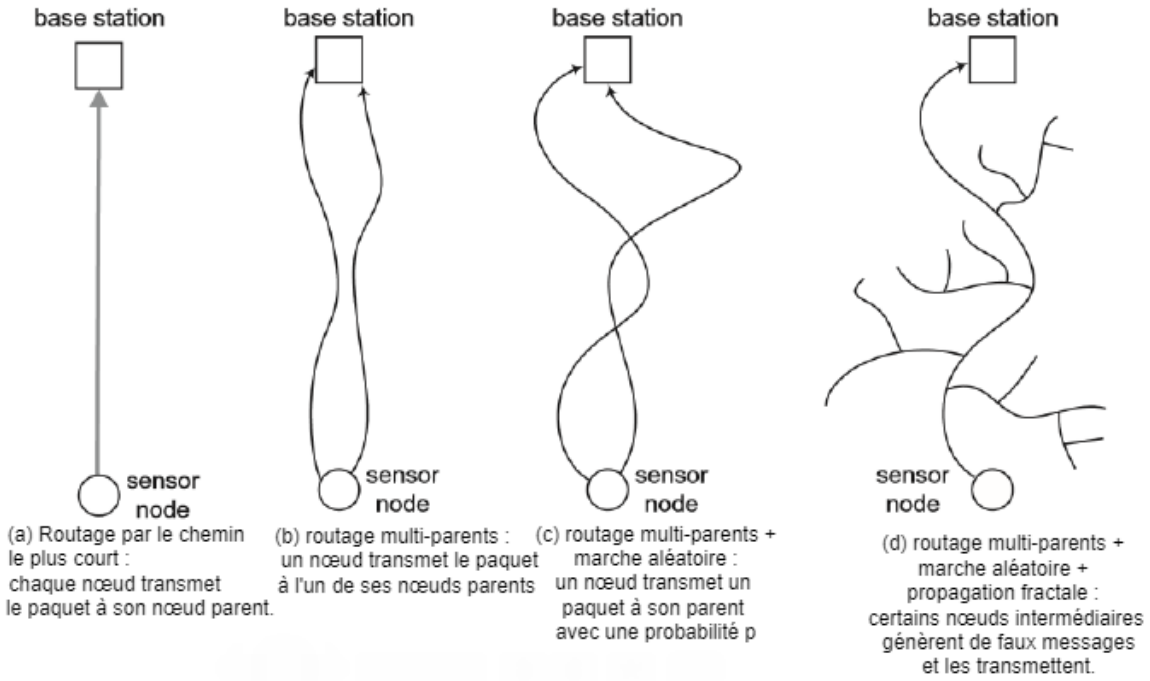


FIGURE 2.2 – Techniques pour contrer l'analyse de trafic. [28]

2.5 Confidentialité d'emplacement des noeuds source et récepteur

2.5.1 Solution Shi-W et all

Dans l'étude réalisée dans [23], les auteurs ont constaté qu'une attaque est possible contre le routage fantôme basé sur l'inondation. Par conséquent, les auteurs ont proposé une méthode alternative appelée GROW. Cette dernière, utilise une marche aléatoire basée sur la source et la station de base pour réduire considérablement le risque de détection des paquets.

Cette méthode repose sur le principe de la diffusion locale et utilise un filtre de Bloom [24] pour stocker tous les voisins actuels dans le paquet de transmission. Chaque fois qu'un capteur transmet un paquet, il enregistre le dernier saut à partir duquel le paquet est arrivé et le prochain saut auquel il transmettra le paquet. Lorsque la marche aléatoire revient vers un capteur, elle choisit

un voisin qui n'a jamais transmis le paquet auparavant. Cette approche permet de maximiser la couverture pour une longueur de chemin donnée.

2.5.2 Solution Chen-H et all

Dans l'étude menée par Chen-H et al dans [25], quatre solutions ont été proposées pour assurer la transmission sécurisée des messages de la source au récepteur : la marche aléatoire vers l'avant (FRW), l'arbre bidirectionnel (BT), l'arbre bidirectionnel dynamique (DBT) et l'arbre bidirectionnel en zigzag (ZBT).

La première solution, la marche aléatoire vers l'avant (FRW : Forward Random Walk), consiste à effectuer une marche aléatoire. Chaque nœud doit connaître le nombre de sauts vers la station de base (Hi) ainsi que le nombre de ses voisins (Ni). Ensuite, chaque nœud divise ses voisins en trois ensembles : les plus proches (CLi), les plus éloignés (FLi) et la liste équivalente (ELi). Un nœud est classé dans la liste des plus proches si son nombre de sauts est inférieur à Hi, dans la liste des plus éloignés s'il est supérieur à Hi, et dans la liste équivalente s'il est égal à Hi. Lorsqu'un nœud détecte un événement, il agit comme un nœud source et choisit aléatoirement un voisin de la liste d'envoi (FRLi) qui est l'union de CLi et ELi pour envoyer son paquet. Ce schéma protège la confidentialité de l'emplacement, mais il augmente la latence en raison de la marche aléatoire. FRW ne relaie les paquets qu'aux voisins de la liste d'envoi (FRLi), ce qui réduit la période de sécurité. Par conséquent, une autre solution consiste à utiliser des messages factices (dummy) dans le réseau pour détourner l'adversaire du véritable chemin de livraison.

La deuxième solution, l'arbre bidirectionnel (BT : Bidirectional Tree), repose sur le principe de cacher la source et le récepteur dans les branches d'une topologie arborescente formée par le flux des paquets transmis. Les messages réels sont transmis par le chemin le plus court entre la source et la station de base. Par conséquent, nous utilisons la topologie arborescente au long du chemin le plus court du côté de la source pour protéger la confidentialité de la localisation de bout en bout.La figure2.4 montre le schéma principal du schéma BT. Dans ce schéma BT les messages factices sont transmis des nœuds de tige aux nœuds de feuille.

La troisième solution, le schéma de l'arbre bidirectionnel dynamique (DBT : Dynamic Bidirectional Tree), combine le schéma FRW et BT, ce qui rend le chemin de livraison des messages réels variable dans le temps, augmentant ainsi la difficulté de traçage.

Dans la dernière méthode, l'arbre bidirectionnel en zigzag (ZBT), des proxys sont utilisés, un pour protéger la source et un autre pour protéger le récepteur. Les messages dans ce schéma sont transférés en zigzag. Le proxy peut masquer l'adresse IP ou l'identifiant unique de la source réelle en utilisant son propre identifiant. Ainsi, lorsqu'un message est transmis à travers le proxy, l'adversaire ne peut pas directement identifier la véritable source. Ce protocole comprend trois

segments : de la source au proxy de la source, du proxy source au proxy SB, et du proxy SB au noeud SB. Pour garantir l'efficacité de ZBT, plusieurs proxys sont générés pour une meilleure protection de l'emplacement de la source et du récepteur.

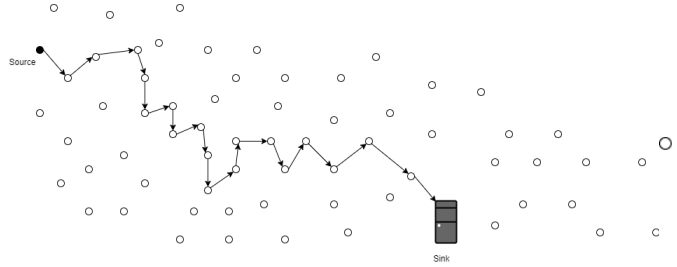


FIGURE 2.3 – a) Le scénario de schéma marche aléatoire vers l'avant (FRW) [25]

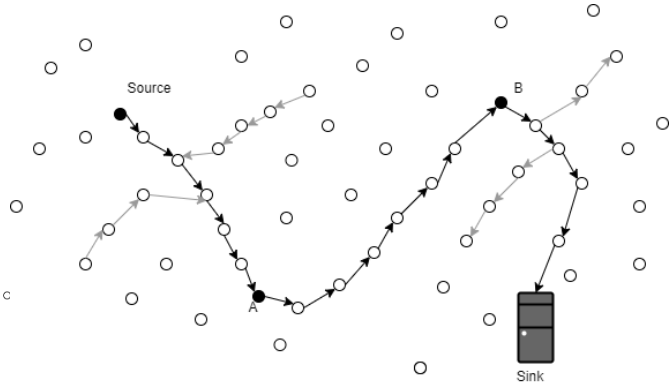


FIGURE 2.4 – b) Le scénario de schéma arbre bidirectionnel (BT) [25]

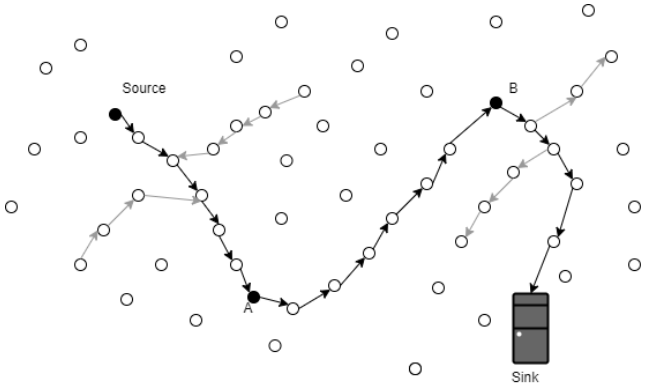


FIGURE 2.5 – c) Le scénario de schéma arbre bidirectionnel dynamique (DBT) [25]

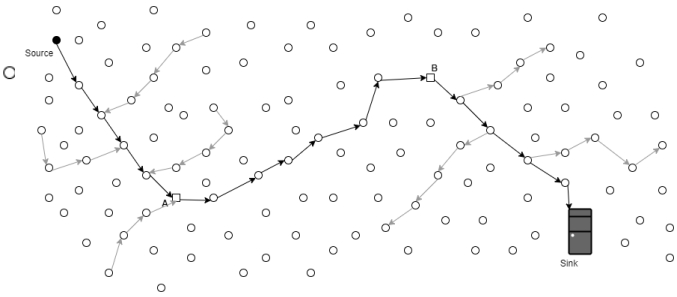


FIGURE 2.6 – d) Le scénario de schéma arbre bidirectionnel en zigzag (ZBT) [25]

2.6 Les critères d'évaluation des solutions existantes

Pour évaluer les méthodes de protection de l'emplacement de la source et de la station de base, nous nous intéressons aux critères suivants : période de sécurité (Safety period), latence et consommation d'énergie. [25]

2.6.1 Période de sécurité(Safty period)

Les recherches sur le problème de la protection d'emplacement d'une source (resp. station de base) dans les réseaux de capteurs n'ont pas encore abouti à un moyen d'empêcher absolument

un adversaire de trouver une source (resp. station de base) ; au lieu de cela, la protection fournie est généralement mesurée en fonction de la période de sécurité attendue.

La période de sécurité est mesurée comme étant le nombre de sauts où l'adversaire lance le traçage, c'est-à-dire lorsqu'il écoute le premier paquet de données émis par la source, et se termine lorsque l'adversaire capture la source ou la station de base.

2.6.2 Latence

La latence désigne le temps entre le départ d'un message de la source et son arrivée à la destination à travers un réseau. Elle est mesurée en fonction du nombre de paquets transmis dans le réseau pendant une période de temps donnée.

2.6.3 Consommation d'énergie

La consommation d'énergie par un nœud de capteur est due essentiellement aux opérations suivantes : capture, traitement et communication. Chaque transmission de paquets nécessite une certaine quantité d'énergie, et la consommation d'énergie totale est mesurée en fonction du nombre de paquets transmis dans le réseau pendant une période de temps donnée.

2.7 Étude comparative

Nous présentons une comparaison entre les méthodes de protection d'emplacement de la source et de la station de base, en se basent sur les critères cités précédemment.

2.7.1 Méthode de routage fantôme (Kamat-P et al.)

Période de sécurité : La méthode de routage fantôme assure un temps de sécurité considérable en rendant difficile pour un adversaire de suivre le mouvement des paquets.

Latence : La latence peut être plus longue en raison de la marche aléatoire effectuée par chaque paquet avant d'atteindre la SB.

Consommation d'énergie : La méthode de routage fantôme augmente la consommation d'énergie marginalement, car elle n'ajoute qu'une communication supplémentaire minimale, tout en améliorant significativement la confidentialité.

2.7.2 Méthode des boucles CEM (Ouyang-Y et al)

Période de sécurité : La méthode basée sur les boucles offre une période de sécurité améliorée par rapport à d'autres méthodes, en raison de l'utilisation de boucles dans le réseau.

Latence : Elle maintient une latence minimale pour les messages.

Consommation d'énergie : La consommation d'énergie dépend de la longueur des boucles utilisées. Une augmentation de la longueur des boucles peut entraîner une consommation d'énergie plus élevée.

2.7.3 Méthode LPR

Période de sécurité : La méthode de routage probabiliste fournit un temps de sécurité plus long que les autres solutions, mais cela vient avec un coût élevé en raison de l'injection de faux paquets.

Latence : La latence dépendra de la topologie du réseau et de la marche aléatoire des paquets.

Consommation d'énergie : La consommation d'énergie est influencée par l'injection de faux paquets, ce qui peut entraîner une consommation d'énergie plus élevée.

2.7.4 Méthode GROW (Shi-W et al)

Période de sécurité : La méthode de marche aléatoire offre une période de sécurité plus élevée en obligeant l'adversaire à utiliser des stratégies de retour en arrière pour retrouver la source.

Latence : La latence peut être légèrement plus longue en raison de la marche aléatoire des paquets.

Consommation d'énergie : La consommation d'énergie est inférieure à la moitié de celle de la méthode de routage fantôme.

2.7.5 Méthodes FRW,BT,DBT, ZBT (Chen-H et al.)

Période de sécurité : Le schéma ZBT offre une période de sécurité plus élevée par rapport aux autres schémas, ce qui est favorable. La période de sécurité augmente rapidement dans schéma BT lorsque nombre de saut augment. Par contre ce dernier est faible dans les schémas DBT et FRW.

Latence : La latence dépendra de la topologie et du nombre de sauts nécessaires. Elle peut varier.

Consommation d'énergie : Le schéma ZBT consomme plus d'énergie en raison de l'utilisation de proxys et de messages fictifs par rapport aux autres.

En résumé, chaque méthode présente ses avantages et ses inconvénients en ce qui concerne la période de sécurité, la latence et la consommation d'énergie.

2.8 Comparaison

L'étude comparative des solutions citées ci-dessus, selon les trois métriques suivantes : période de sécurité, énergie et latence. Nous a permis de dresser le table comparatif suivant :

Méthode	**Période de sécurité**	**Consommation d'énergie**	**Latence**
Routage fantôme [22]	Forte	marginale	élevée
Marche aléatoire (FRW) [25, 28]	Forte	Faible	élevée
Arbre bidirectionnel (BT) [25]	Moyenne	Moyenne	Légèrement plus longue
Arbre bidirectionnel dynamique(DBT) [25]	Faible	élevée	Très élevée
Arbre bidirectionnel en zigzag (ZBT) [25]	Forte	élevée	variable
Piegeage cyclique (CEM) [27]	Forte	Variable : dépend de la longueur des boucles	Faible
Méthode LPR [26]	Très forte	élevée	Variable : dépend de la topologie
Méthode GROW [23]	Forte	Variable : dépend de la topologie	élevée Latence

TABLE 2.1 – Comparaison des méthodes de préservation de la confidentialité d'emplacement de la source et de station de base dans les RCSF

2.9 Conclusion

Dans ce chapitre, nous avons présenté les critères pertinents pour évaluer la confidentialité de l'emplacement de la source et de la station de base dans les réseaux de capteurs sans fil : la période de sécurité (Safety period), la latence et la consommation d'énergie. Nous avons également passé en revue les solutions existantes ainsi que les contre-mesures contre les attaques d'analyse de trafic dans ces réseaux. Ensuite, nous avons comparé ces solutions en fonction des critères choisis.

Dans l'ensemble, nous avons examiné différentes approches telles que le routage fantôme, la marche aléatoire, le schéma ZBT, l'emplacement basée sur les boucles, le routage probabiliste et GROW. Chaque méthode présente ses avantages et ses inconvénients en termes de période de sécurité, de latence et de consommation d'énergie.

Cette comparaison nous a permis d'identifier les forces et les faiblesses de chaque méthode, ce qui peut aider à prendre des décisions éclairées lors de la conception et de la mise en œuvre de solutions de confidentialité d'emplacement dans les réseaux de capteurs sans fil.

Chapitre 3

Solution proposée

3.1 Introduction

La technique de génération de faux trafic sous forme de faux paquets est utilisée dans une solution précédente pour fournir la confidentialité d'emplacement, que ce soit de la source ou de la station de base séparément. La figure 3.1 montre un faux trafic généré sous forme de faux chemins du coté de la source et du coté de la station de base pour protéger respectivement l'emplacement de la source et de la station de base.

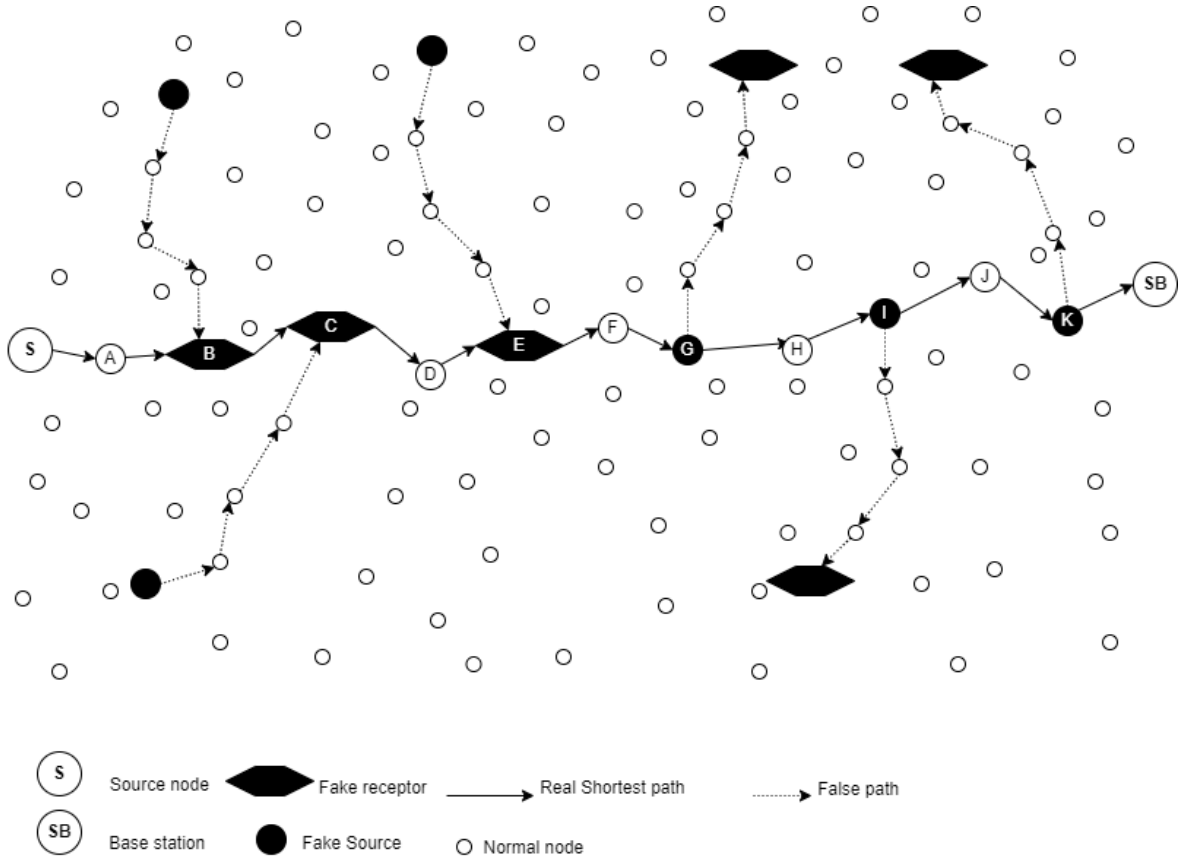


FIGURE 3.1 – Confidentialité de l'emplacement de bout en bout en utilisant de faux chemins séparément [25]

Cependant, cette méthode présente plusieurs lacunes en termes de période de sécurité et de consommation d'énergie qui sont donnés ci-dessous :

- L'émission du faux trafic du coté de la fausse source n'est pas garantie de commencer juste au moment du lancement du vrai trafic (données) vers la station de base, puisque les nœuds initiant le faux trafic ne sont pas sur le chemin réel pour qu'ils soient activés implicitement lorsque le vrai trafic commence. Ainsi, une activation explicite est nécessaire, mais elle nécessite une consommation supplémentaire d'énergie. Sinon, l'émission d'un faux trafic consommerait une énergie précieuse des nœuds capteur, bien qu'il n'y ait pas de données à communiquer. De même, il est nécessaire d'arrêter explicitement l'émission du faux trafic lorsque la source arrête l'émission des données vers la station de base.
- A quelle fréquence le faux trafic devrait-il être injecté afin qu'il soit similaire à la fréquence d'envoi du vrai trafic, rendant ainsi difficile pour un adversaire utilisant l'attaque d'analyse de trafic de distinguer le vrai du faux trafic. Ainsi, augmenter la période de sûreté.

3.2 Aperçu de la solution proposée

Pour assurer la confidentialité de la source et de la station de base au même temps, notre idée consiste à utiliser des faux chemin qui assurent la protection de la source et de la station de base simultanément, en combinant les faux chemins dédiés pour protéger la source avec ceux dédies pour protéger la station de base, comme montre la figure 3.2. Pour que notre solution agisse efficacement contre un adversaire en l'éloignant de la source et la station de base avec un moindre coût énergétique, a génération du faux trafic doit vérifier les critères suivants :

- L'émission d'un faux trafic doit être activé (respectivement désactivé) quand la source lance (respectivement , arrête) l'émission d'un vrai trafic. Ainsi, un nœud transmet d'envoyer un faux trafic quand il y a uniquement une communication des données entre la source et la SB., ce qui économise sa consommation d'énergie et augmente sa durée de vie. Par conséquent, la durée de vie du RCSF est prolongée.
- La fréquence d'émission du vrai trafic soit le même que la fréquence d'émission du vrai trafic.

Pour réaliser ces deux conditions dans notre solution, les nœuds initiant l'envoi du faux trafic sont choisit aléatoirement parmi les nœuds du chemin de livraison des données (chemin réel) qui sont du coté de la station de base et ayant une distance en saut entre L/2 et L/4 de la station de base. Un adversaire qui trace en avant (suivre) les paquets de données, lorsqu'il arrive sur ces nœuds, doit choisir la direction du paquet à suivre. S'il fait un mauvais choix, c'est-à-dire s'il choisit de suivre le faux paquet, il sera conduit loin de la station de base.

De même, les nœuds recevant le faux trafic sont choisit aléatoirement parmi les nœuds du chemin réel qui sont du coté de la source, et ayant une distance en saut entre L/2 et 3L/4 de

la station de base. Un adversaire qui trace en arrière (backtraking) les paquets de données, en arrivant sur ces nœuds, doit choisir la direction du paquet à tracer en arrière. S'il se trompe et choisit de tracer en arrière le faux paquet, il sera conduit loin de la source.

On appel les nœuds initiant l'envoi du faux trafic et les nœuds recevant le faux trafic respectivement fausse-source et fausse-sink.

Notre solution permet d'améliorer la période de sécurité et d'énergie comme suit :

- Le faux trafic à générer et à transmettre est réduit de moitie, car chaque faux chemin est au même temps un faux chemin entrant du coté de la source et comme un faux chemin sortant du coté de la station de base. Ce qui réduit la consommation d'énergie de moitie.
- Aucun mécanisme n'est utilisé pour l'activation et la désactivation d'un faux trafic, puisque les nœuds initiant la transmission sont sur le chemin réel et s'activent implicitement quand ils reçoivent le vrai trafic et se désactivent implicitement quand le nœud source arrête l'envoi des données à la station de base.
- Une même fréquence d'émersion est utilisée du faux trafic et les données.

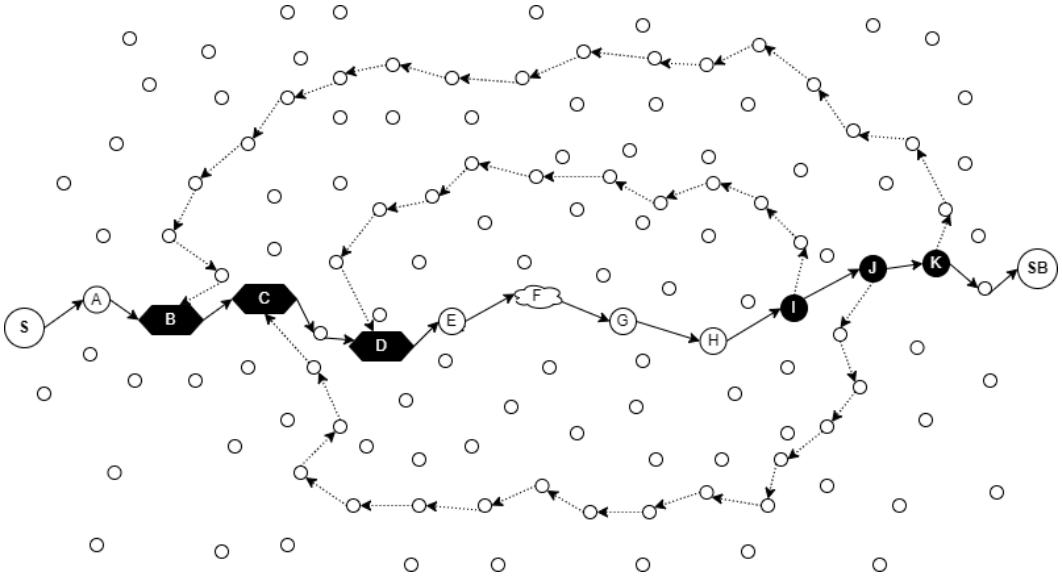


FIGURE 3.2 – Faux chemins pour préserver la confidentialité d'emplacement d'une source et d'une station de base au même temps

La figure 3.2 montre un ensemble de faux chemins qui sont activés lorsque une communication est initiée entre une source et une station de base. Ces faux chemins assurent deux fonctions au même temps : Le flux entrant vers le (resp. sortant du) chemin réel permet de piéger un adversaire qui tente de tracer en arrière (resp. en avant (suivre)), saut-par-saut le vrai trafic pour atteindre la source (resp. station de base).

3.3 Spécification des faux chemins

La création des faux chemins se produit quand un nœud source a des données à communiquer à la station de base. Un faux chemin est créé entre deux nœuds choisis au hasard du vrai chemin. Le nœud initiant la création d'un faux chemin est choisi parmi les nœuds qui se trouvent sur la moitie du chemin réel qui est du coté de la station de base (les nœuds I, J, K de la figure 3.2) et agit comme fausse-source. Le nœud destinataire d'un faux chemin est choisi parmi les nœuds qui se trouvent sur la moitié du chemin réel qui est du coté de la source (les nœuds D, C, B sur la figure 3.2) et agit comme une fausse-sink.

3.4 Procédure d'établissement d'un faux chemin

Le nœud source transmet un message de découverte de route REQ-R sur le plus court chemin le plus court vers la Sink. La requête enregistre chaque nœud visité et le stocke dans le champ Set-of-Fake-Sink du REQ-R jusqu'à ce qu'il atteigne le milieu du chemin réel, c'est-à-dire : $Nombre-de-Sauts \leq Shortest-Path-length/2$. Lorsque la requête soit après le nœud médian du chemin réel, chaque nœud visité décide, avec probabilité Pf, de devenir une fausse-source en initiant la procédure de création de faux-chemin (voir section 4.2) entre lui-même et un nœud choisi au hasard parmi le Set-of-fake-Sink, qui fait agit comme faux-BS. Le format du message REQ-R est représenté sur le tableau 3.1.

Sink-Node	Set-of-Fake-Sink	Hop-count	Shortest-path-length	Request-type

TABLE 3.1 – Format du message REQ-R

La procédure exécutée en chaque nœud lors de la réception d'un REQ-R est donnée par l'algorithme1.

Algorithm 1 Algorithm 1 : Génération des faux chemins

/ *le nœud source envoi la requête REQ-R pour générer des faux chemins. / * Cet algorithme est exécuté par chaque nœud visité X sur le chemin réel, quand il reçoit la requête REQ-R* /

Begin

Hop-count++

if ($\frac{\text{path-length}}{4} \leq$ hop-count $< \frac{\text{path-length}}{2}$) **then**

/* le nœud est stocké dans le champ fake-sink-list de la requête REQ-R avec une probabilité Pf*/

Générer un nombre aléatoire Q

if ($Q >$ Pf) **then** le nœud ajoute son (id) dans le champ Fake-Sink-Set

Endif

ElseIf($\frac{\text{path-length}}{2} <$ hop-count $\leq \frac{3\times\text{path-length}}{4}$) /*le nœud génère un faux chemin avec la même probabilité Pf*/

Then

Générer un nombre aléatoire Q ; /* le nœud peut initier la création d'un faux chemin*/

if ($Q >$ Pf) **then** /* le nœud devient une fausse-source et génère un faux chemin*/

Choisir un voisin Y qui n'est pas sur le chemin réel ;

Choisir aléatoirement un nœud Z depuis Fake-Sink-Set comme fausse-sink ;

Transmettre le message de création d'un faux chemin REQ-FP (Y, Z,set-of-ordered-nodes, REQ-FP).

Endif.

if |fake-sink-set| ≥ 1 **then**

Supprimer un nœud choisi aléatoirement de Fake-Sink-Set ;

Endif

Endif

Transmettre REQ-R dans le réseau en utilisant le protocole de routage du plus court chemin

End.

3.5 Génération de faux chemins

En s'insérant de [27], un noeud X qui décide de créer un faux chemin devient fausse-source, et choisit d'abord un noeud comme fausse-sink depuis le champ Set-of-Fake-Sink. Ensuite, il initialise les champs Set-of-ordred-Nodes et Type respectivement à "vide" et "REQ-F-Path". Enfin, il transmet la requête REQ-F-Path à un nœud Y qu'il sélectionne aléatoirement parmi ces voisins qui ne sont pas sur le chemin réel (plus court chemin) vers la station de base. La requête fait une marche aléatoire pour L sauts et enregistre tous les nœuds visités dans le champ Set-of-Ordered-Nodes, jusqu'à ce qu'elle atteigne le noeud fausse-sink. Le nœud fausse-sink extrait les nœuds stockés et construit la réponse RES-F-Path en mettant dans les champs Reverse-Ordered-of-Nodes les nœuds stockés dans l'ordre inverse, et met le champ Type à RES-F-Path puis il transmet le message RES-F-Path au nœud fausse-source. Le message passe par tous les nœuds

stockés dans l'ordre inverse jusqu'à ce qu'il atteigne la fausse-source, et le faux-chemin serait créé. Les formats des messages REQ-F-Path et RES-F-Path sont montrés respectivement sur les tableaux 3.2 et 3.3 .

Fake source	Fake sink	Set-of-Ordered-nodes	type

TABLE 3.2 – Format de la requête message REQ-FP

Fake source	Fake sink	Reverse-Order-of -nodes	type

TABLE 3.3 – Format de la requête message RES-FP

Lorsque le nœud source estime que le REQ-R a atteint la station de bases, par exemple en attendant un laps de temps entre l'envoi du paquet REQ-R et le début de la communication pour s'assurer que les faux chemins sont crée, il lance la communication des données à la station de base. Quand un nœud reçoit un paquet de données, il vérifie s'il est une fausse-source ; si s'est oui, il active le faux chemin correspondant en envoyant un faux message le long de ce faux chemin au nœud faux-sink. L'envoi de faux paquets se poursuit tant que le nœud source a des données à envoyer à la station de base. Ainsi, les faux paquets et les paquets de données sont transmets de manière uniforme et l' arrêt de la transmission est implicite, puisque les faux paquets sont transmit quand il existe des données cours en transmission. Donc, avec la supposition que les faux paquets sont de même longueur qu'un message de données et sont cryptés, un adversaire ne pourra pas distinguer entre un faux paquet et un message de données.

La figure 3.3 montre un exemple de faux chemins qui sont crées entre une fausse-source et un fausse-SB qui sont représentées respectivement par des cercles et des hexagones pleins.

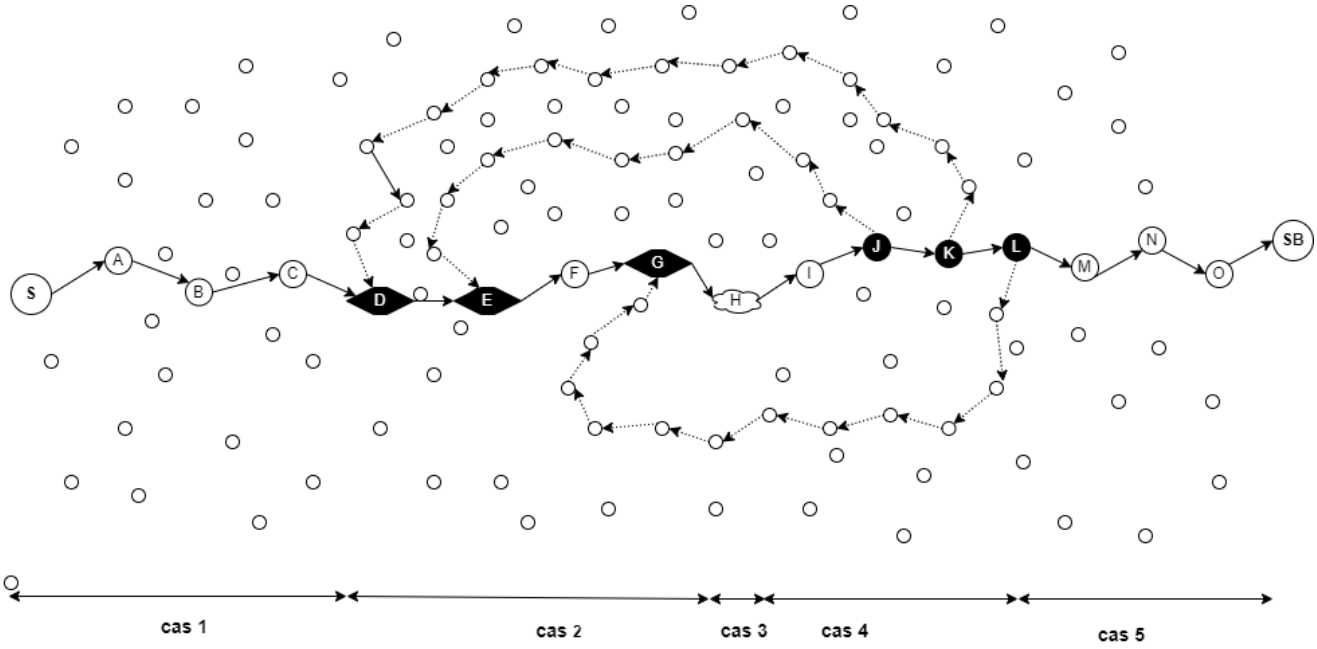


FIGURE 3.3 – Exemple de faux chemins pour préserver simultanément la confidentialité d'emplacement d'une source et d'une station de base

L'explication détaillé par un exemple de distance de 16 sauts entre la source et la station de base, comme illustré sur la figure 3.3 est la suivante :

Initialement, le nœud source prépare le message de demande REQ-R en initialisant les champs : Set-of-Fake-Sink, Hop-count, Path-length et Type respectivement à, vide, 0, 16 et REQ-R. Puis il transmet la requête REQ-R à la station de base sur le plus court chemin. La requête REQ-R est traitée de cinq manières différentes, selon la distance du nœud visité à la station de base, comme suit :

Cas 1 : la requête n'a pas encore parcourue le quart du chemin réel

Le nœud a son hop-count entre 0 et (path-length/4). Le nœud juste incrémente le champ hop-count et transmit la requête à son nœud voisin. Dans l'exemple de la figure3.3, les nœuds A, B, C ont leurs hop-count respectivement 1, 2, 3 qui sont supérieurs à 0 et inferieurs à 4 (16/4).

Cas 2 : la requête a parcourue entre le quart et le milieu du chemin réel

Le nœud a son hop-count dans l'intervalle [path-length/4 .. path-length/2 [. Le nœud visité incrémente le hop-count, puis avec une probabilité Pf, il devient fausse-sink et ajoute son identifiant dans le champ Set-of-fake-sink. Dans l'exemple de la figure 3.3, les nœuds D, E, F, G ont leurs hop-count dans l'intervalle [4.. 8[. Parmi eux, les nœuds D, E,G sont ajoutés dans le champ Set-of-fake-sink peuvent devenir des fausse-sink.

Cas 3 : la requête est au nœud qui est au milieu du chemin réel

Le nœud a son hop-count = path-length/2. Le nœud juste incrémente le champ hop-count et transmit la requête à son nœud voisin. Dans l'exemple de la figure 3.3, le nœud H a son hop-count = 8 (16/4).

Cas 4 : la requête a parcourue la distance entre la moitie et trois quarts du chemin réel.

Le nœud incrémente et ajoute son identifiant dans le champ hop-count puis, il décide, avec une probabilité Pf, de créer un faux chemin et devenir fausse-source. Un nœud qui décide de créer un faux chemin choisit aléatoirement un nœud parmi ceux stockés dans le champ Set-of-fake-sink comme fausse-sink, puis exécute les instructions 6 à 11 ne figurent pas sur l'algorithme1. Ensuite, il supprime le nœud fausse-sink du champ Set-of-fake-sink. Enfin, le nœud transmet la requête à son voisin sur le plus court chemin. Dans l'exemple de la figure 3.3, les nœuds I, J, k, L ont leurs hop-count dans l'intervalle [8.. 12[. Parmi eux, les nœuds J, K, L ont décidé de créer des faux chemins vers respectivement les nœuds E, D, G et sont devenus des fausse-sources.

Cas 5 : la requête dépasse la distance de trois quarts du chemin réel

Le nœud a son hop-count dans l'intervalle [3/4 *path-length .. path-length [.Comme le cas 1, le nœud juste incrémente le champ hop-count et transmit la requête à son nœud voisin. Dans l'exemple de la figure 3.3, les nœuds M, N, O ont leurs hop-count respectivement 13, 14, 15 qui sont supérieur à 12 ((3*16)/4) et inférieur à 16.

Afin que le nombre de noeuds stockés dans le champ Set-of-fake-source devient réduit ou vide, quand la requête REQ-R atteint la station de base, on a supposé que la probabilité pour qu'un nœud devient fausse-source soit la même pour devenir fausse-sink. Ainsi, le nombre de fausse-source sera approximativement égal au nombre de fausse-sink ; et chaque fois qu'un faux chemin est crée, le nœud fausse-sink correspondant est supprimé du champ Set-of-fake-sink s'il n'est pas le dernier.

3.6 Conclusion

Dans ce chapitre, nous avons proposé une méthode pour protéger la confidentialité d'emplacement simultanément de la source et de la station de base dans les réseaux de capteur sans fil. En premier, nous avons décrit les Inconvénients d'une existante méthode, ensuite notre solution, et enfin un exemple pour bien comprendre notre méthode. Dans le chapitre suivant, nous présentons les résultats de simulations.

Chapitre 4

Evaluation de performances

4.1 Introduction

Dans ce chapitre, nous présenterons l'évaluation de notre méthode de protection de la confidentialité de l'emplacement simultané de la source et de station de base dans les RCSF en nous basant sur les critères période de sécurité et l'énergie consommée. Nous examinerons plusieurs scénarios de simulation décrivant l'environnement de simulation que nous avons utilisé, puis nous discuterons en détail les résultats obtenus par simulation de ce protocole de routage.

4.2 Environnement de simulation

4.2.1 Définition de MATLAB

MATLAB est un environnement de calcul numérique et un langage de programmation de haut niveau développé par MathWorks, basé sur la représentation matricielle des données. Il offre une interface pratique pour effectuer des calculs mathématiques complexes, créer des visualisations et développer des algorithmes. MATLAB comprend un grand nombre de fonctions mathématiques intégrées et de boîtes à outils, qui permettent aux utilisateurs d'effectuer rapidement et facilement une grande variété de tâches, de l'analyse de données et du traitement de signaux à la conception de systèmes de contrôle et à l'apprentissage. La simulation du protocole étudié requiert l'utilisation et la manipulation des vecteurs, des tableaux et des matrices. Le côté évaluation des performances quant à lui, requiert la génération des graphes, et donc l'utilisation des outils de traçage qu'offre MATLAB. Ce dernier est largement utilisé dans des domaines tels que l'ingénierie, la physique, les mathématiques et la finance, et est connu pour ses capacités puissantes d'analyse de données et sa facilité d'utilisation. [29]

Dans notre simulation on a utilisé la version R2009b de MATLAB.

4.2.2 Choix MATLAB

Nous avons choisi le langage de programmation MATLAB pour plusieurs raisons :

- MATLAB est un langage de programmation de haut niveau spécialement conçu pour l'informatique scientifique et technique.
- Il permet une programmation plus rapide et plus efficace pour les calculs et la présentation des résultats.
- Offre un environnement de développement qui facilite la gestion du code, des fichiers et des données.
- Le logiciel comprend des fonctions graphiques personnalises, et il offre également des fonctions pour l'analyse et le traitement de donnes, adaptées aux besoins spécifiques de nombreux ingénieurs et scientifique.
- Il propose des applications personnalisées pour des tâches spécialisées telles que l'ajustement de courbes, la classification de données et l'analyse de signaux. [30]
- La fenêtre "Workspace" : le répertorie de l'ensemble des variables existantes, avec leurs types et leurs valeurs.
- La fenêtre "Command History" : elle enregistre l'historique de toutes les commandes entrées par l'utilisateur.
- La fenêtre "Command Window" : sert à formuler des expressions et à interagir avec MATLAB. Cette dernière est utilisée tout au long du chapitre.

4.2.3 Environnement de MATLAB

Au lancement de MATLAB, différentes fenêtres apparaissent en fonction de la version utilisée. Parmi celles-ci, on peut retrouver : [32]

- La fenêtre ''Current Folder" : permet d'afficher le répertoire courant ainsi que les fichiers existants.
- La fenêtre "Workspace" : le répertorie de l'ensemble des variables existantes, avec leurs types et leurs valeurs.
- La fenêtre "Command History" : elle enregistre l'historique de toutes les commandes entrées par l'utilisateur.
- La fenêtre "Command Window" : sert à formuler des expressions et à interagir avec MATLAB.
  Cette dernière est utilisée tout au long du chapitre.

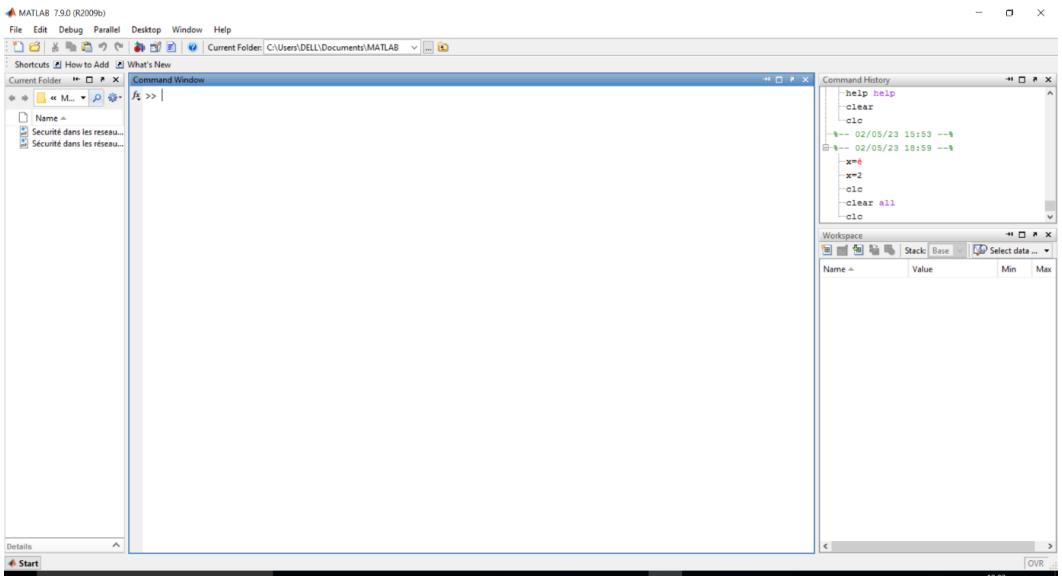


FIGURE 4.1 – Environnement MATLAB

4.3 Simulation

La simulation est un outil utilisé par les chercheurs, les ingénieurs, les militaires et d'autres professionnels pour étudier les résultats d'une action sur un élément sans avoir besoin de réaliser l'expérience sur l'élément réel. Elle se déroule dans un environnement simulé plutôt que dans le monde réel. Bien que certains simulateurs soient plus complets que d'autre dans leurs résultats de simulation, tous permettent d'étudier le comportement d'un réseau ayant une topologie et des caractéristiques spécifiques. La simulation présente un grand intérêt pour créer la topologie d'un réseau avant de le mettre en place dans le monde réel. Les simulateurs intègrent en effet de nombreux outils permettant de réaliser des simulations très réalistes. Par ailleurs, il est possible d'utiliser un simulateur pour tester un nouveau protocole (la facilité de l'intégration dépendant du simulateur utilisé) avant de l'implémenter dans un réseau réel, comme c'est le cas pour un protocole de réseau de capteur sans fil. [31]

4.4 Evaluation

Afin d'évaluer les performances de la méthode d'utilisation des faux chemins dans les RCSF, on doit déterminer la formule pour estimer chaque paramètre. Safety periode et l'énergie consommée.

La formule pour déterminer safety periode est comme suit :

a) Un nœud appartenant au chemin de livraison des données peut activer un faux chemin avec une probabilité (P). Ce paramètre permet d'augmenter ou diminuer le nombre de faux chemins activés selon le niveau de confidentialité désiré.

b) Un nœud qui est sur le chemin de communication de données peut activer au plus

un faux chemin. Donc, un adversaire a une probabilité optimale Q = $\frac{1}{2}$ de sélectionner correctement un vrai chemin et a une probabilité (1-Q) de faire un mauvais choix.
c) La distance (n) entre la station de base et la source est fixée dans cette simulation à 80 sauts.
d) Un adversaire se place au milieu entre la source et la station de base et tente de tracer les paquets entendus dans le sens de la source ou de la station de base. Donc, en moyenne, un adversaire parcourt une distance de n/2.
e) Si un adversaire fait un mauvais choix en tançant le faux chemin alors il parcourt une distance de (L) sauts.

D'après les observations a) b) c), d) et e), on peut calculer la période de sécurité avec l'équation suivante :

$$Safetyperiod = n/2 + (Q * P * L + Q * P * L... * Q * P * L), sommede(n/2)termes \quad (4.1)$$

En remplaçant Q par sa valeur on obtient :

$$Safetyperiod = n/2 + 1/2(P * L + P * L...P * L) \quad (4.2)$$

Après réduction, la formule devient :

$$\text{Safety period} = \frac{n}{2} + \frac{1}{2}\sum_{i=1}^{\frac{n}{2}} P \cdot L \quad (4.3)$$

4.5 Paramètres de simulation utilisés

Nous avons effectué plusieurs simulations. Les principaux paramètres de simulation sont résumés dans le tableau 4.1

Il convient de noter que nos résultats sont basés sur la simulation d'un réseau spécifique composé de 200 nœuds, dont les emplacements sont générés de manières aléatoires dans une zone de 100 m2. La portée radio de chaque nœud est de 100m. Les positions de la station de base et de la source sont fixée respectivement aux coordonnées (0.1 ; 0.5) et (0.9 ; 0.1).

Paramètres	**Valeurs**	**Unité de mesure**
La surface du réseau	(100*100)	(m*m)
Nombre des nœuds	200	/
La portée radio d'un nœud.	100	Mètre
Emplacement de la station de base	(0.1 ; 0.5)	Mètre
Emplacement de la source	(0.9 ; 0.1)	Mètre
Consommation d'énergie à l'émission	50*0.000000001	Joule
Consommation d'énergie à la réception	50*0.000000001	Joule
Distance en saut entre la source et la station de base	80	/

TABLE 4.1 – Paramètres de simulation

4.6 Fonctionnement de simulateur

Le fonctionnement de base de notre simulateur est indiqué par le l'organigramme de la figure suivante :

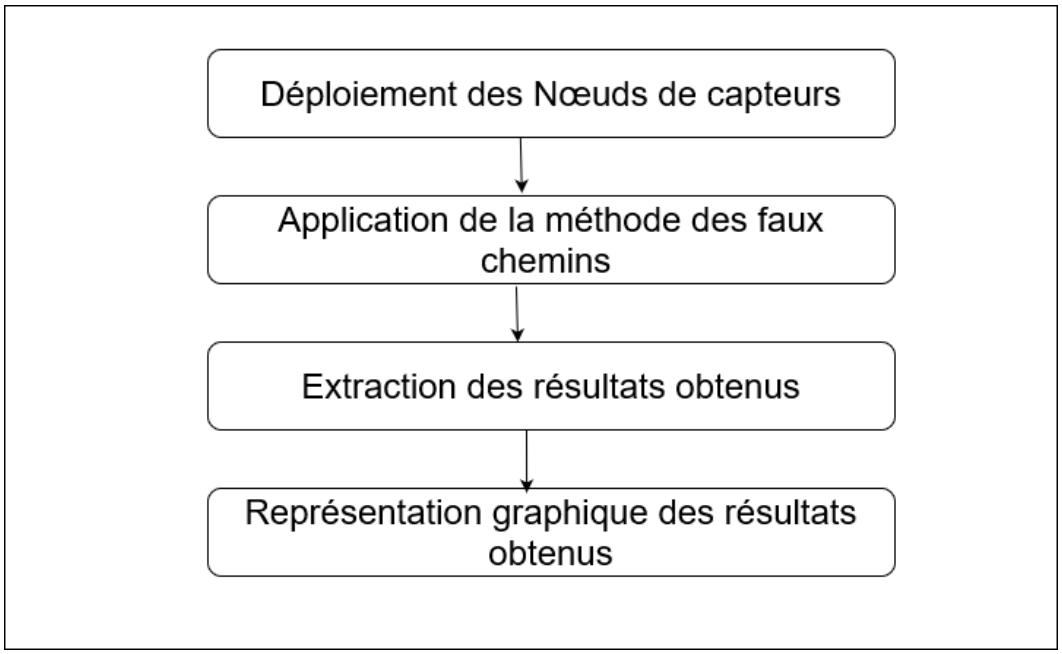


FIGURE 4.2 – Fonctionnement de la simulation réalisée.

4.6.1 Déploiements des nœuds de capteurs

Nous avons déployé 200 nœuds de capteurs sans fil dans un espace à deux dimensions d'une manière aléatoire sur une zone de 100 m2 (voir la figure 4.3) ; on se basant sur une fonction aléatoire qui génère à chaque fois un emplacement différent de l'emplacement précédent. Au début chaque nœud possède son emplacement sur deux positions. La station de base et la source

sont positionnées initialement aux coordonnées (0.1, 0.5) et (0.9, 0.1 respectivement.

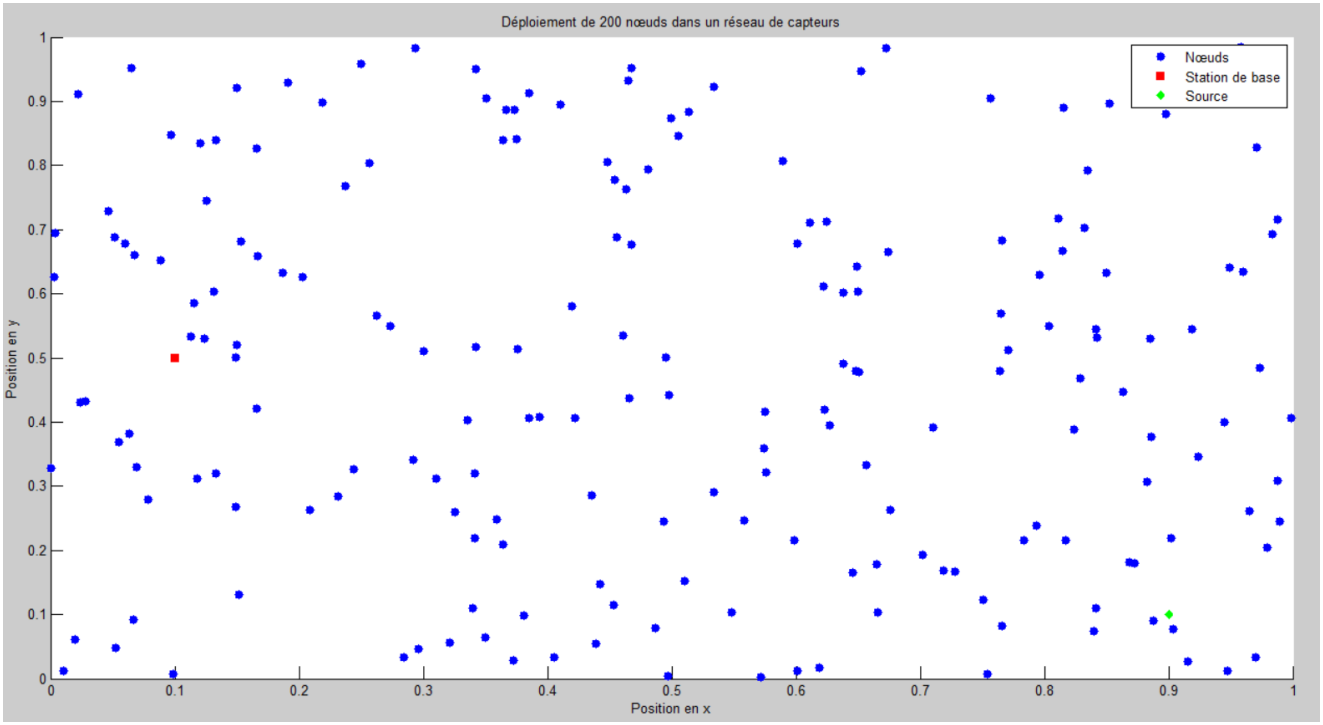


FIGURE 4.3 – Déploiement aléatoire de 200 nœuds de capteur.

Lorsqu'il s'agit de déployer des nœuds de capteurs sans fil dans un espace donné, un positionnement aléatoire peut souvent être la meilleure option, car il permet de répartir les nœuds de manière uniforme sur l'ensemble de la zone, ce qui peut aider à assurer une couverture efficace et à maximiser la collecte de données. Dans le cas présent, la figure 4.3 montre le déploiement de 200 nœuds de capteurs sans fil est effectué sur une zone de 100 m2. Nous avons utilisé une fonction pour générer aléatoirement chaque positionnement sur l'ensemble de la zone de déploiement afin de garantir que le positionnement des nœuds est différent à chaque fois. Il est également important de noter que chaque nœud possède une position initiale en deux dimensions. Cela permet de suivre la position de chaque nœud et de s'assurer qu'il reste dans la zone de déploiement prévue. La station de base et la source sont également positionnées initialement aux coordonnées (0.1 ; 0.5) et (0.9 ; 0.1) respectivement. Cela peut aider à définir une structure de base pour le déploiement et à garantir que les nœuds sont positionnés de manière à maximiser la couverture de la zone.

4.6.2 Résultats et discussion

La figure 4.4 montre comment la période de sécurité varie en fonction de la longueur de faux chemin L pour différentes valeurs de la probabilité d'activation de faux chemins. On peut observer que toutes les courbes croissent quand la longueur de faux chemin augmente. Cela indique que la période de sécurité augmente quand la longueur L augmente. Cependant, on peut également

remarquer que les courbes ne croissent pas de manière uniforme pour toutes les valeurs de P ; en particulier, la courbe correspondant à P = 0.9 présente une croissance plus rapide que les autres courbes pour de faibles valeurs de la longueur L, tandis que les courbes correspondant à P = 0.1 et P= 0.3 ont une croissance plus lente pour les mêmes valeurs de la longueur L. Nous pouvons observer aussi que la période de sécurité augmente quand le nombre de faux chemins activé augmente c.à.d. la probabilité d'activation de faux chemins P, augmente.

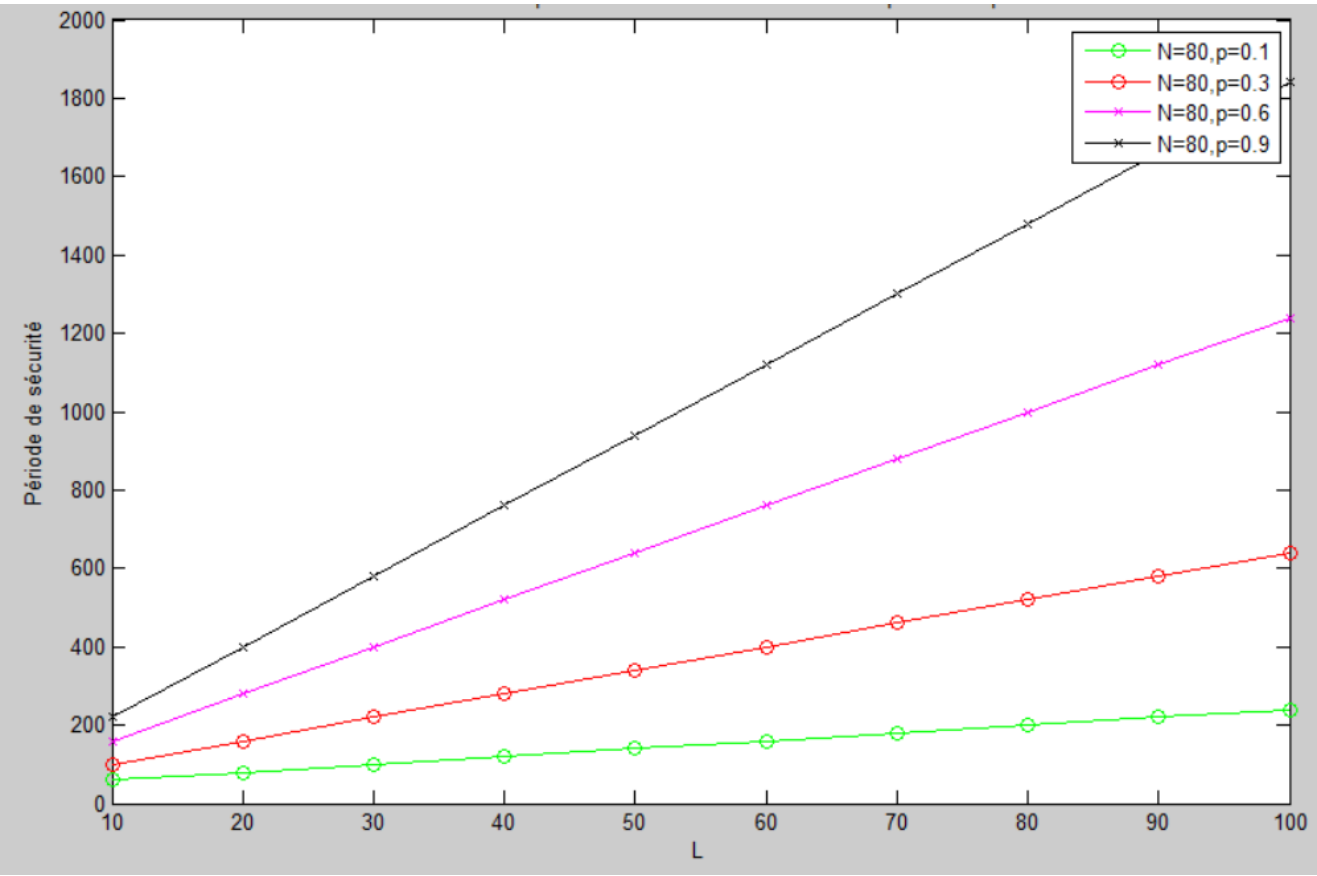


FIGURE 4.4 – Période de sécurité en fonction de la longueur de faux chemin (L) pour différentes probabilités (P) d'activation d'un faux chemin.

La figure 4.5 montre la période de sécurité en fonction de la probabilité qu'un nœud active un faux chemin pour différentes valeurs de L. On peut observer que la période de sécurité augmente quand la probabilité d'activation de faux chemins augmente, pour toutes les longueurs de faux chemin représentées dans la figure. En outre, on peut également observer que la croissance de la période de sécurité est plus rapide pour les valeurs plus élevées de L qui est représenté dans ce schéma par L=100. Lorsque la longueur d'un faux chemin est accrue, la période de sécurité également augmente. Cela implique que si un attaquant se trouve sur un faux chemin de grande longueur, il perdra beaucoup de temps pour quitter et essayer une deuxième fois pour trouver le bon chemin.

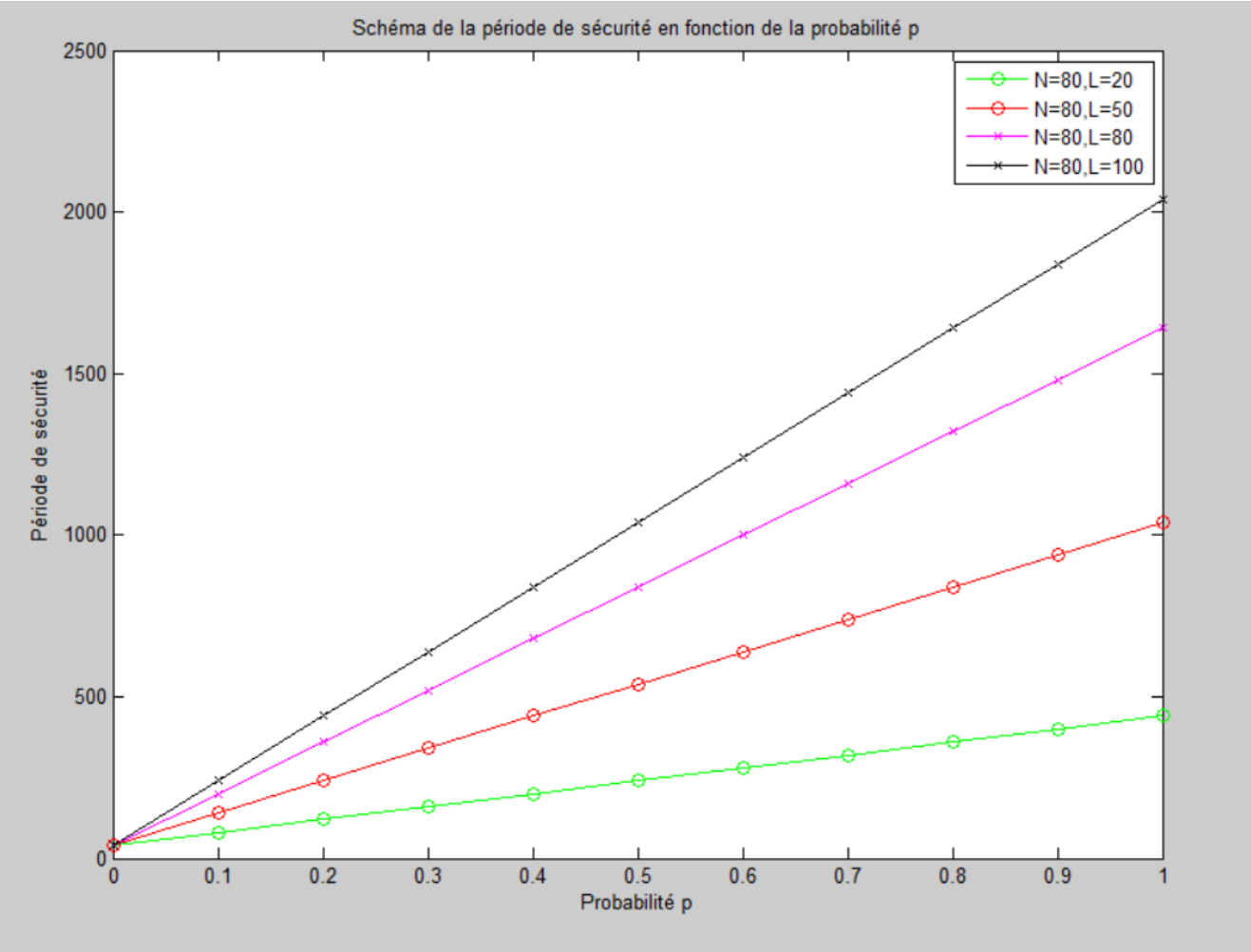


FIGURE 4.5 – Période de sécurité en fonction de la probabilité (P) qu'un nœud crée un faux chemin p pour différentes valeurs de L.

La figure 4.6 montre la période de sécurité en fonction de la distance (n) en sauts entre la source et station de base pour différentes longueurs de faux chemin (L). La probabilité de création de faux chemins est fixée à P = 0,4 pour toutes les courbes représentées dans la figure. En examinant la figure, on peut observer que la période de sécurité augmente lorsque n augmente, pour toutes les valeurs de L représentées. De plus, on peut également observer que la période de sécurité est élevée pour les longueurs de faux chemin élevées. Par exemple, pour L = 80, la période de sécurité est plus grande pour N = 80 que pour N = 20.

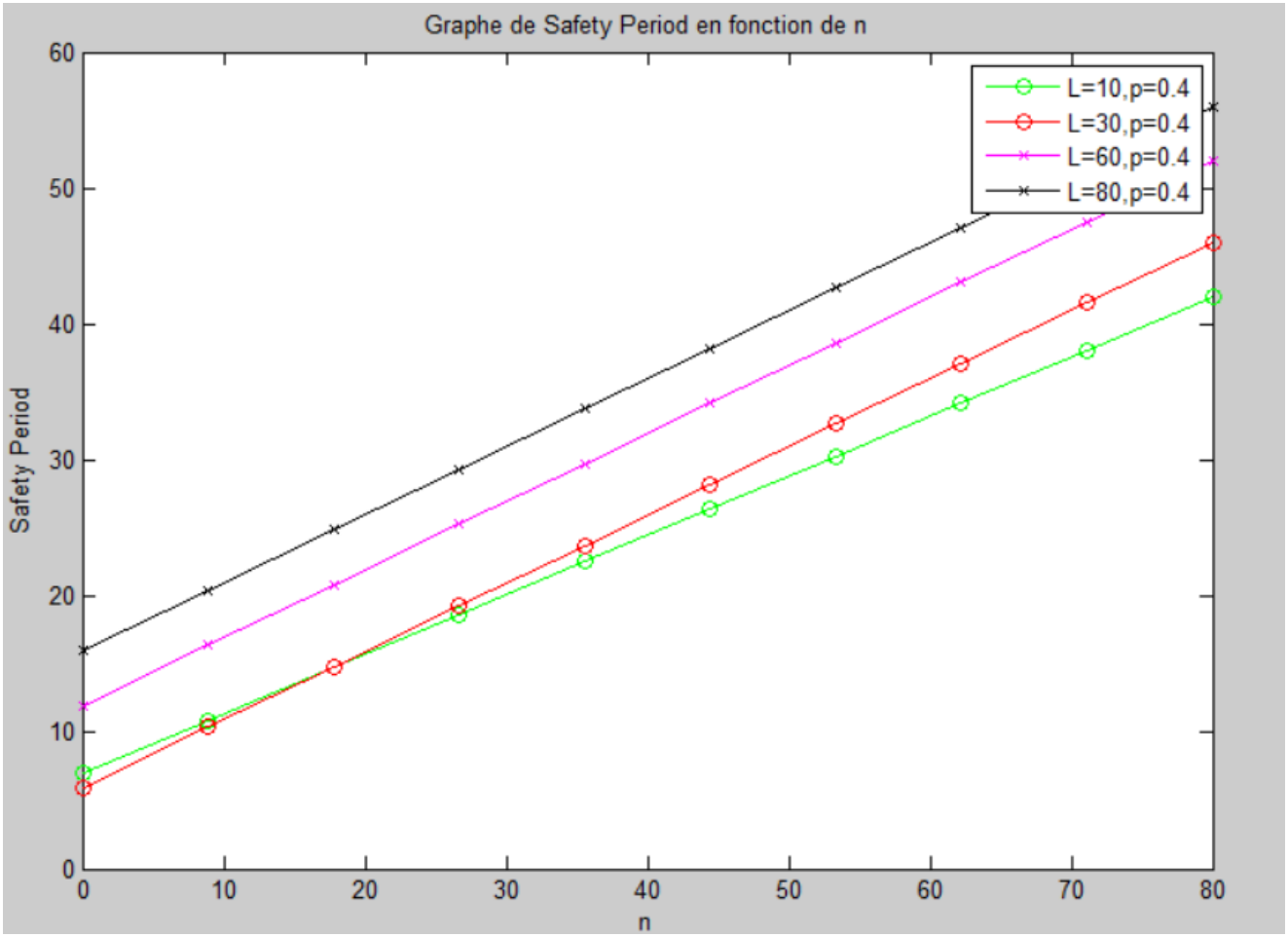


FIGURE 4.6 – période de sécurité en fonction de la distance n entre la source et la station de base, pour différentes valeurs de L.

La Figure 4.7 montre la période de sécurité en fonction de la distance en sauts n entre la station de base et source pour différentes valeurs de la probabilité d'activation d'un faux chemin P et une longueur de faux chemin fixée à L = 60. On peut observer que la période de sécurité augmente de manière significative lorsque P augmente. En examinant la figure, on peut observer que la période de sécurité augmente lorsque la probabilité P augmente pour toutes les valeurs de N représentées.

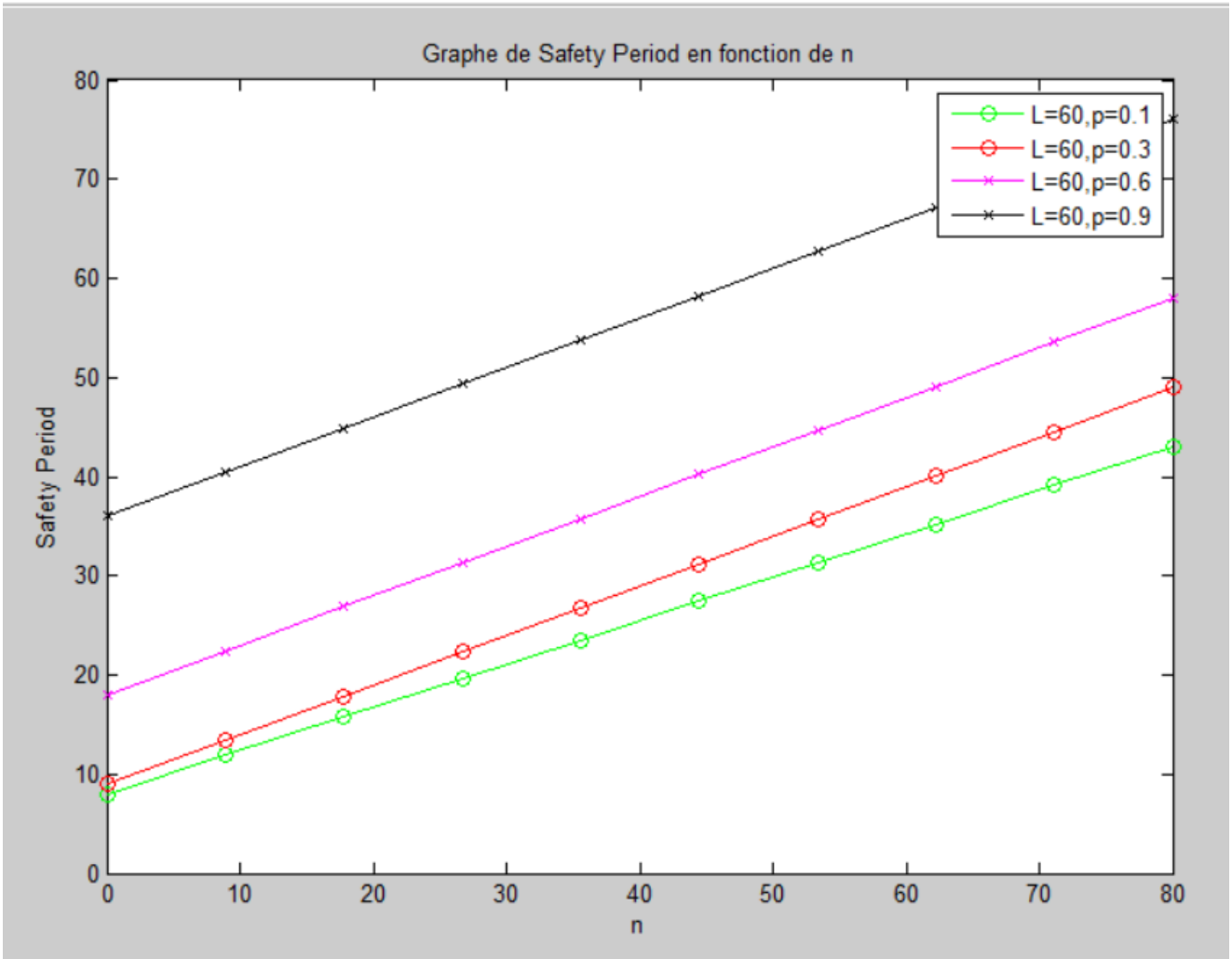


FIGURE 4.7 – période de sécurité en fonction de la distance n pour différentes valeurs de la probabilité P.

4.7 Comparaison de notre solution avec la solution existante

Dans cette section, nous allons comparer analytiquement notre solution avec la méthode existante décrite dans [25], en nous basant sur deux critères : la période de sécurité et le coût d'énergie. La comparaison est effectuée dans les mêmes conditions : les faux chemins ont la même longueur et le même protocole de routage est utilisé pour envoyer un message de données de la source vers la station de base. Nous supposons qu'un adversaire se place au milieu, entre la source et la station de base, et tente de suivre la trace (backtrack) en direction de la source ou de suivre la trace (forward) en direction de la station de base.

1) Période de sécurité (safety period)

- Dans notre solution, la distance en saut prévisible qu'un adversaire doit parcourir pour

atteindre la source (S) ou la station de base (SB) est donnée par l'équation suivante :

$$\text{Safety period} = \frac{n}{2} + \frac{1}{2}\sum_{i=1}^{\frac{n}{2}} Pi \cdot L \tag{4.4}$$

- Dans la solution existence, la distance en sauts prévisible qu'un adversaire doit parcourir pour atteindre une source (S) est donnée par l'équation suivante :

$$\text{Safety period} = \frac{n}{2} + \frac{1}{2}\sum_{i=1}^{\frac{n}{2}} Pi \cdot L \tag{4.5}$$

Où **n/2** est la distance entre le milieu du chemin réel et la source, **Pi** est la probabilité d'activation d'un faux chemin par le nœud i et **L** la longueur du faux chemin. De même, la distance prévisible qu'un adversaire doit parcourir pour atteindre la station de base (SB) est donnée par l'équation (4.5) ci-dessus.
D'après ces résultats, on remarque que la période de sécurité dans notre solution est identique à celle de la solution existante. Cela est dû au fait que dans les deux méthodes, un faux chemin est activé avec la même probabilité (Pi). De plus, si un adversaire choisit un mauvais chemin, il parcourt la même distance (L) et se trouve à une distance de (n/2) de la source ou de la station de base.

2) Coût énergétique

La consommation d'énergie est un paramètre important pour les réseaux de capteurs. Nous avons évalué le coût énergétique de notre solution en comparant les coûts énergétiques par rapport à la solution existante.

Dans notre solution, l'énergie totale est obtenue comme suit :

$$E = \mathbf{k} \cdot (E_{\text{send}} + E_{\text{receive}}) \tag{4.6}$$

Où E_{send} est l'énergie nécessaire à un nœud pour envoyer un message,E_{receive} est l'énergie nécessaire à un nœud pour recevoir un message et **k** est le nombre d'émissions et réceptions d'un vrai ou un faux paquet.

Étant donné que l'énergie d'émission d'un nœud $E_{\mathbf{send}}$ est généralement supérieure à l'énergie de réceptions d'un nœud E_{receive} [27], on néglige E_{receive} . Donc, le coût d'énergie est égal au coût de l'énergie d'émission, et l'équation (1) devient :

$$E = \mathbf{k} \cdot E_{\text{send}} \tag{4.7}$$

On peut trouver le nombre total de vrai et fausses émission k en fonction de **L**, $P_{\mathbf{i}}$ et **n** comme suit :

a) Nombre de vraies émissions effectuées quand un vrai paquet est émet

Un vrai paquet est transmet de la source vers la station de base sur le plus court chemin. Donc, le nombre d'émissions qui va effectuer est égal à la distance en sauts (n) entre la source et la station de base.

b) Nombre de fausses émissions nécessaires quand un vrai paquet est émet

Quand un vrai paquet est émit, la confidentialité de l'emplacement de la source et de la station de base est fournie simultanément par l'activation des faux chemins qui se trouvent entre le milieu du chemin de données et la station de base. Le nombre de fausses transmissions est égal au nombre de nœuds qui se trouvent entre le milieu du chemin de données et la station de base (n/2), multiplié par la probabilité (Pi) qu'un nœud active un faux chemin, multiplié par le nombre de nœuds dans un faux chemin (L). Ceci donne :

$$\sum_{i=1}^{\frac{n}{2}} Pi \cdot L \tag{4.8}$$

Donc, (a) et (b), on obtient k est :

$$\mathbf{k} = (\sum_{i=1}^{\frac{n}{2}} Pi \cdot L) + n \tag{4.9}$$

• Dans la solution de Chen-H et all [27] , les fausses sources ne sont pas sur le chemin de données, il est nécessaire d'être activées explicitement par le nœud source au début de la communication et être désactivées à la fin de la communication ; contrairement aux fausses stations de bases.

Soit $Emsg\_act\_désact\_fs$ le nombre d'émissions qu'il faut pour leur activation et désactivation. Donc, la formule de calcul de l'énergie totale est obtenue comme suit :

$$E = \mathbf{k} \cdot (E_{\text{send}} + E_{\text{receive}}) + E_{msg\_act\_désact\_fs} \tag{4.10}$$

c) L'activation/désactivation des fausses sources sont réalisées uniquement une seule fois. Donc, on peut ignorer $\mathrm{E}_{msg\_act\_désact\_fs}$.

d) Nombre de fausses émissions nécessaires quand un vrai paquet est émet

Quand un vrai paquet est émet, la confidentialité de l'emplacement de la source est fournie par l'activation des faux chemins qui sont entre la source et le milieu du chemin de données (c'est-à-dire, le faux trafic du côté de la source). On note par $E_{\text{send(S)}}$ ce nombre de faux trafic. De même, quand un vrai paquet est émet, la confidentialité de l'emplacement de la station de base est fournie par l'activation des faut chemins qui sont entre la station de base

et le milieu du chemin de données (c'est-à-dire, le faux trafic du côté de la station de base). On note par $E_{\text{send(SB)}}$ ce nombre de faux trafic. Pour assurer la confidentialité d'emplacement simultanément de la source et la station de base, tous les faux chemins entre la source et la station de base doivent être activés. Donc, ce faux trafic est égale la somme des deux : $E_{\text{send(S)}} + E_{\text{send(SB)}}$.

Étant donné que l'adversaire est supposé être au milieu, la protection fournie pour assurer la confidentialité d'emplacement d'une source est identique à celle fourni pour assurer la confidentialité de la station de base. on a alors $E_{\text{send(S)}} = E_{\text{send(SB)}}$.

Donc, on peut simplifier $E_{\text{send(S)}} + E_{\text{send(SB)}}$ par :

$$2 \cdot E_{\text{send(S)}} \tag{4.11}$$

Comme la même manière que précédemment, on peut trouver le faux trafic en fonction de **L**, **Pi** et **n** comme suit :

$$2 \sum_{i=1}^{\frac{n}{2}} Pi \cdot L \tag{4.12}$$

Donc, de (a), (c) et (d) le trafic total k (vrai et faux) est :

$$\mathbf{k} = 2 * (\sum_{i=1}^{\frac{n}{2}} Pi \cdot L) + n \tag{4.13}$$

La comparaison analytique montre que le coût énergétique dans notre solution est réduit presque à la moitie par rapport à la solution existante, cela est prouvé par les équations (4.14) et (4.10).

La raison est que dans notre solution le faux trafic généré est réduit à la moitié, un faux chemin dans notre solution est équivalent à deux faux chemins dans la solution existante.

Pour confirmer les résultats obtenus on a réalisé une petite simulation sous MATLAB pour comparer l'énergie consommée dans notre solution et la solution existante.
La figure 4.8 montre l'énergie consommée en fonction de la distance entre la source et la station de base dans les deux méthodes citées précédemment. D'après le schéma, on remarque que notre méthode consomme moins d'énergie par apport à la solution existante. On prend l'exemple lorsque la distance entre la source et la station de base est de 16, nous observons une différence significative en termes de consommation d'énergie entre la solution existante (48) et notre méthode (28). Cette diminution est considérable et démontre l'efficacité de notre approche. On constate aussi que la distance entre la source et la station de base n'influence pas vraiment sur la consommation d'énergie et l'augmentation est linéaire à cette distance.

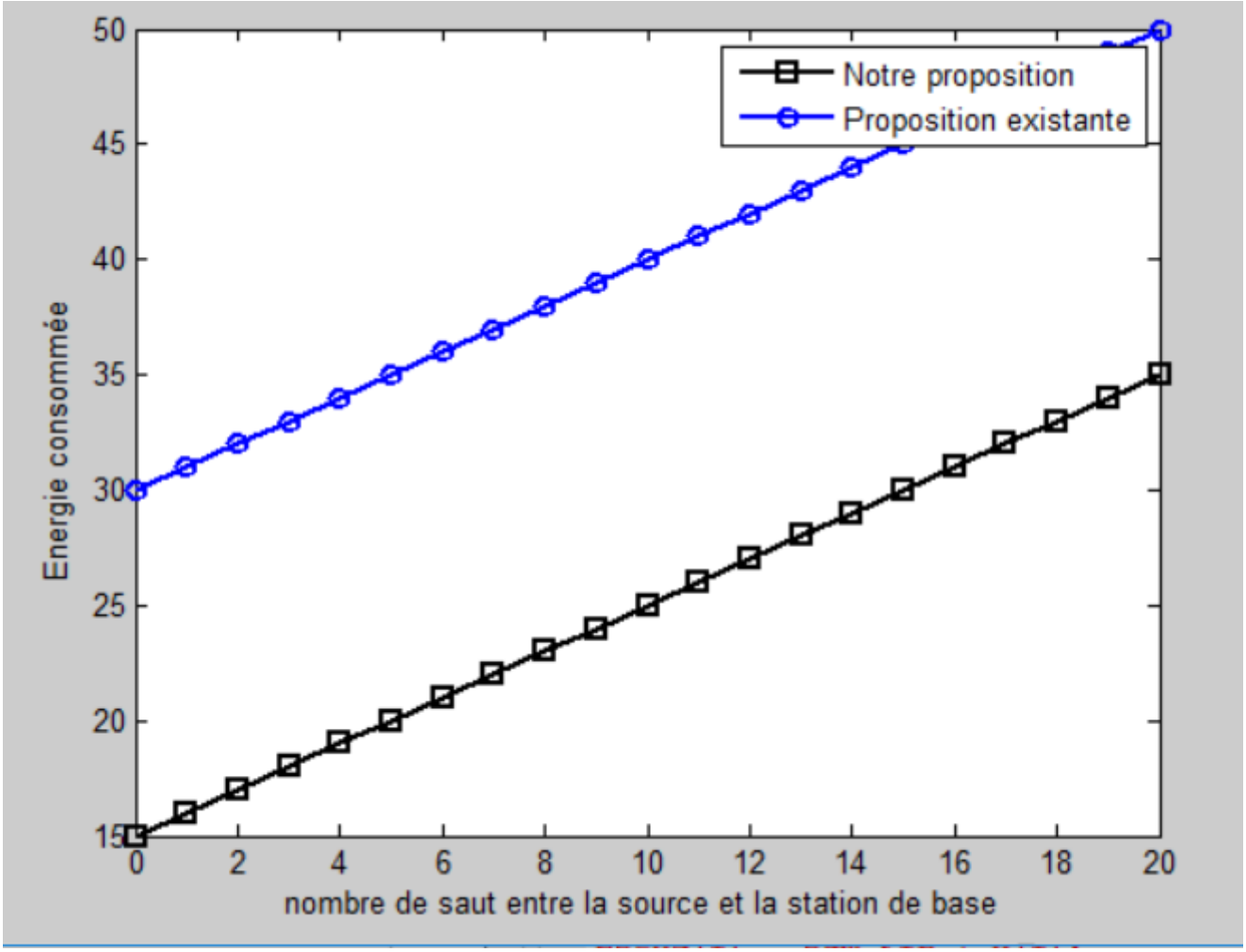


FIGURE 4.8 – Énergie consommée en fonction de la distance entre la source et la station de base dans les deux méthodes.

4.8 Conclusion

Dans ce chapitre, nous avons abordé les aspects pratiques liés à la réalisation de notre projet, à savoir l'outil de développement nécessaires et le langage de programmation. Nous avons présenté aussi les paramètres nécessaires pour la simulation. Par la suite, nous avons exposé quelques captures d'écran montrons les résultats de simulations pour la période et sécurité et l'énergie consommée. Enfin on a fait une petite comparaison entre notre la solution existante pour confirmer l'efficacité de cette dernière.

Conclusion générale et perspectives

Les RCSF peuvent être déployé pour surveiller certains événements et repérer leurs emplacements, les informations d'emplacement sont destinées uniquement aux utilisateurs légitimes. Cependant, un adversaire peut être en mesure de retracer les chemins de routage des messages jusqu'à la source/destination de l'événement, ce qui peut constituer une violation de la confidentialité pour certaine situation. Ainsi, la protection de la confidentialité d'emplacement est essentielle pour un déploiement réussi.

Dans ce mémoire, nous avons d'abord abordé des notions de base des RCSF. Ensuit Nous avons examiné diverses méthodes existantes qui fournissent la confidentialité d'emplacement d'un noeud source ou d'un noeud récepteur. Parmi celles-ci, nous avons étudié les approches telles que le routage fantôme, la méthode des boucles, GROW et LPR.
Enfin, nous avons proposé une solution qui permet de préserver, simultanément, l'emplacement d'un noeud source et d'une station de base. Notre solution permet d'améliorer une méthode existante, en terme du coût énergétique, en réduisant presque de moitie la consommation d'énergie ; à notre connaissance, c'est l'unique méthode dans la littérature qui a abordée la confidentialité de bout en bout. Nous avons évalué analytiquement et par simulation extensive en se basant sur deux critères : période de sécurité et le coût énergétique. Les résultats montrent que notre solution permet d'améliorer le coût énergétique comparativement à la solution existante.

Cependant, malgré les améliorations apportées, la sécurité du système reste préservée. Certaines critiques pourraient considérer que la réduction de moitié de la consommation d'énergie par rapport à la solution existante n'est pas suffisamment significative, nécessitant ainsi des recherches supplémentaires pour explorer des approches permettant une réduction encore plus marquée de la consommation d´énergie. Il est donc essentiel de continuer à développer des solutions robustes et fiables pour préserver la confidentialité de l'emplacement dans les réseaux de capteurs sans fil. Au terme de ce travail, quelques perspectives peuvent être envisagées. Il serait intéressant :

- D'étendre notre étude à un réseau de plusieurs source et plusieurs station de bases.
- D'analyser d'autres critères de performance comme la latence et d'autres attaques sur la confidentialité d'emplacement comme l'analyse de trafic.

Bibliographie

[1] M RABHI Seddik, *Optimisation des algorithmes de localisation dans les réseaux de capteurs sans fil*, Thèse de doctorat, Université FERHAT ABBAS - SETIF1,2016

[2] Mme, Gherbi Chirihane. *Algorithme de routage pour les réseaux de captures avec prise en charge de la consommation d'énergie*. 2017.

[3] Mme,Lynda TLILI. *Modèle de confiance pour sécuriser le routage dans les réseaux de capteurs sans fil*, Mémoire Master Université MOULOUD MAMMERI-TIZI-OUZOU. 2011

[4] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, *Scalable coordination for wireless sensor networks : self-configuring localization systems, International Symposium on Communication Theory and Applications* (ISCTA 2001), Ambleside, UK, July 2001

[5] J.M. Kahn, R.H. Katz, K.S.J. Pister, *Next century challenges : mobile networking for smart dust, Proceedings of the ACM MobiCom'99*, Washington, USA, 1999, pp. 271–278

[6] G. Hoblos, M. Staroswiecki, A. Aitouche, *Optimal design of fault tolerant sensor networks,* IEEE International Conference on Control Applications, Anchorage, AK, September 2000, pp. 467–472.

[7] J. Rabaey, J. Ammer, J.L. da Silva Jr., D. Patel, PicoRadio : *ad-hoc wireless networking of ubiquitous lowenergy sensor/monitor nodes, Proceedings of the IEEE Computer Society AnnualWorkshoponVLSI(WVLSI'00), Orlanda, Florida,* April 2000, pp. 9–12.

[8] M. Lehsaini, *Diffusion et couverture basées sur le Clustering dans les réseaux de capteurs : application à la domotique,* Thèse de Doctorat Université A.B Tlemcen Université de Franche-Comté, 2009.

[9] S.ATHMANI *Protocoles pour la Securité des Reseaux de Capteurs Sans Fil.*Thèse de Doctorat Université A.B Tlemcen Université de Batna, juillet 2018

[10] Cherfi Sarra,*Détection d'intrusions via des réseaux de neurones optimisés par des métaheuristiques*, Mémoire Master d, Université Mohamed Seddik Ben Yahia de Jijel.2019

[11] N. B. Priyadharshini et al.*Active and Passive Attacks in Computer Network Security". In : Advances in Intelligent Systems and Computing*, vol 1060, pp. 491-500. (2020)

[12] https ://www.techopedia.com/definition/4144/man-in-the-middle-attack-mitm Consulté le 25/04/2023.

[13] Benbrahim, S.-E. *Défense contre l'attaque d'analyse de trafic dans les réseaux de capteurs sans fil (WSN)* thèse , École Polytechnique de Montréal. PolyPublie. (2011) https ://publications.polymtl.ca/655/ Consulté le 25/04/ 2023,

[14] Carl Hartung, James Balasalle, and Richard Han. *Node compromise in sensor networks : The need for secure systems.* Technical report, Department of Computer Science University of Colorado at Boulder, January 2005.

[15] J. P. Walters, Z. Liang, W. Shi, et V. Chaudhary, *Wireless Sensor Network Security : A Survey* , in Security in Distributed, Grid, and Pervasive Computing, 2006 Auerbach Publications, CRC Press,

[16] I. F. Akyildiz, W. Su, Y.Sankarasubramaniam, and E. l. Cayirci. *"A survey on sensor networks".* IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-116, August 2002.

[17] Equipe de Get, *Capt'Ad-hoc. "Sensor networks : State of the art".* Technical Report, Telecom Paris, ENST Br, INT, INRIA, Mars 2006

[18] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smit, *"Parametric probabilistic sensor network routing,"* in Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, 2003

[19] H. Lim and C. Kim, *"Flooding in Wireless Ad-hoc Networks," in IEEE computer communications,* 2000

[20] B. Karp and H. T. Kung, "GPSR : *greedy perimeter stateless routing for wireless networks,"* in Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM), August 2000

[21] D. Niculescu and B. Nath, "Trajectory Based Forwarding and its Applications," in Proceedings of the Ninth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM), September 2003, pp. 260–272

[22] Kamat, P., Zhang, Y., Trappe, W., Ozturk, C. *Enhancing source-location privacy in sensor network routing. In 25th IEEE international conference on distributed computing systems (ICDCS'05)* (pp. 599-608). IEEE.2005, June.

[23] Shi, W Xi, Y., Schwiebert, L *Preserving source location privacy in monitoring-based wireless sensor networks. In Proceedings 20th IEEE International Parallel Distributed Processing Symposium* (pp. 8-pp). IEEE. April, 2006

[24] A. Broder and M. Mitzenmacher.*Network applications of bloom filters : A survey. In Allerton Conference*, 2002

[25] Chen, H., Lou, W. *On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. Pervasive and Mobile Computing, 36-50*,2015

[26] Jian, Y., Chen, S., Zhang, Z., Zhang, L. *Protecting receiver-location privacy in wireless sensor networks. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications* (pp. 1955-1963). IEEE (2007, May)

[27] Ouyang, Y., Le, X., Chen, G., Ford, J., Makedon, F.*Entrapping adversaries for source protection in sensor networks. In 2006 International symposium on a world of wireless, mobile and multimedia networks* (pp. 10-pp). IEEE.(2006, June).

[28] Deng, J., Han, R., Mishra, S.. *Countermeasures against traffic analysis attacks in wireless sensor networks. In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)* (pp. 113-126). IEEE. (2005, September)

[29] M. GHEBBI Sofiane*Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs sans fil* mémoire de master recherche , université A/Mira de Béjaia Faculté des Sciences Exactes, 2016.

[30] MathWorks, *"Principales fonctionnalités MATLAB"*, 2011

[31] A. Naima et R. Kheira *Simulation de la surveillance des réseaux de capteurs sans fil (RCSF) sous Omnet++* Mémoire de master université IBN KHALDOUN – TIARET , 2019

[32] H.BABA, F.ZOHRA*Le calcule scientifique applique au géné civile sous MTLAB* Polycope, Universite Mohamed boudif-Oran, 2016.

[33] https ://www.ladissertation.com/Divers/Divers/Réseaux-de-capteurs-vs-réseaux-ad-hoc-72137.html Consulté le 01/05/2023.

[34] P.Kamat,Y.Zhang,W.Trappe,C.Ozturk,*Enhancingsource-location privacy in sensor network routing,in :Proc. of IEEE ICDCS* ,2005,pp.599–608.

[35] L. Eschenaur, V. Gligor, *A key-management scheme for distributed sensor networks, in : Proc. of the 9th ACM Conference on Computer and CommunicationsSecurity,CCS* ,2002,pp.41–47.

[36] M. Cherdantseva et al. *Cybersecurity of Industrial Control Systems : A Systematic Literature Review. In : IEEE Transactions on Industrial Informatics.* (2018) pp. 2060-2069.

[37] Cherfi Sarra,. *Détection d'intrusions via des réseaux de neurones optimisés par des métaheuristiques* Mémoire Master de Recherche en Informatique, Université Mohamed Seddik Ben Yahia de Jijel. (2019/2020)

[38] G. Sindre et al *"Local and Global Security Threats to Organizations". In : Information Security : Foundations, Technologies and Applications.* (2013). pp. 433-467.

Résumé Les réseaux de capteurs sans fil (RCSF) sont composés d'un ensemble de capteurs sans fil qui collaborent pour collecter et transmettre des données environnementales. Ces réseaux ont une variété d'applications potentielles et fournissent des informations précieuses pour la surveillance et la prise de décision dans divers domaines.
La confidentialité de l'emplacement dans les RCSF est une préoccupation majeure, essentielle pour un déploiement réussi.
Dans ce mémoire, nous avons en premier lieu, examine différentes approches pour assurer la confidentialité d'emplacement d la source et de la station de base, telles que le routage fantôme, la méthode des boucles, GROW et LPR, qui ont été développées pour renforcer la confidentialité de l'emplacement.
En second lieu nous avons proposé une solution qui permet de préserver, simultanément, l'emplacement d'un nœud source et d'une station de base. Notre solution permet d'améliorer une méthode existante, en terme du coût énergétique, en réduisant presque de moitié la consommation d'énergie. En dernier lieu, nous avons évalué analytiquement et par une simulation extensive en se basant sur deux critères : période de sécurité et le coût énergétique.

Mots-clés– Réseau de capteur sans fil, confidentialité d'emplacement d'une source/station de base, MATLAB.

Abstract Wireless sensor networks (WSNs) consist of a set of wireless sensors that collaborate to collect and transmit environmental data. These networks have a variety of potential applications and provide valuable information for monitoring and decision-making in various domains.
Location privacy in WSNs is a major concern and essential for successful deployment. In this thesis, we first examine different approaches to ensure location privacy of the source and base station, such as ghost routing, loop-based methods, GROW, and LPR, which have been developed to enhance location privacy.
Secondly, we propose a solution that simultaneously preserves the location of a source node and a base station. Our solution improves an existing method in terms of energy cost by reducing energy consumption by nearly half.
Lastly, we evaluate our solution analytically and through extensive simulations based on two criteria : security period and energy cost.

Key-words– Wireless sensor network, Location privacy of a source/base station, MATLAB.