RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

**Université Abderrahmane Mira Bejaia**
**Faculté des Sciences Exactes**
**Département d'Informatique**


# Mémoire fin de cycle

**En vue de l'obtention du diplôme de master professionnel en informatique**

**Option : Administration et sécurité des réseaux**

## THÉME

# Étude de la confidentialité d'emplacement dans les réseaux de capteurs sans fil

**Réalisé par : Mr.** OUCHENE Issam

**Soutenu publiquement le** : 12/09/2023 devant le jury composé de :

| | |
|---|---|
| Président DR.SADI MUSTAPHA | MCB université A.Mira Béjaia |
| Examinateur DR.BENNAI ATHMANE YANI | MCB université A.Mira Béjaia |
| Rapporteur DR.KHENOUS LACHEMI | MCB université A.Mira Béjaia |

*Remerciements*

*Je tiens à remercier toutes les personnes qui ont contribué au succès de mon travail.*

*Tout d'abord, j'adresse mes remerciements à mon encadreur Dr KHENOUS*

*Lachemi pour son aide.*

*Je tiens à remercier les membres du jury pour m'avoir fait le plaisir d'accepter*

*d'examiner ce travail.*

*J'ai remercié aussi tous les enseignants, du primaire jusqu'à l'université, qui ont*

*affinéma formation.*

*Je tiens à remercier également ma famille et mes amies. Merci de me soutenir*

*dans cetravail*

*Dédicace*

*A mes parents ; A mes beaux-parents.*

*A mes frères et mes sœurs.*

*A mes amies*

# *Table des matières*

# *Liste des figures*

# *Liste des Tableaux*

# *La liste des abréviations*

**ACK** Accusé de réception **(**Acknowledgement)

**ADC** Convertisseur analogique-numérique

**CAS** Système d'anonymat cryptographique

**CEM** Méthode de piégeage cyclique (Cyclic Entrapement Method)

**DEFP** Propagation fractale différentielle appliquée (Differential Enfonced Fractal Propagation)

**DFP** Propagation fractale différentielle

**DOS** Déni de Service

**GROW** Retouche de groupe via sans fil (Group Rekeying Over Wireless)

**ID** Identifiant

**LPR** Routage de chemin à charge équilibrée (Load-balanced Path Routing)

**Ma** la marche aléatoire

**MPR** routage multi-parent **(**multi-parent routing)

**NBC** Nucléaires, Biologiques, Chimiques

**NMR** Anneau de mélange de réseau (Network Mixing Ring)

**Pr** probabilité de création

**P fake** faux paquet

**PF** propagation fractale

**PFS** Schéma de filtre basé sur proxy

**PRNG** Générateur de nombres pseudo-aléatoires (Pseudo Random Number Generator)

**RCSF** Réseau de capteurs sans fil

**RHIR** Randomisation de l'identifiant de hachage inversé (Reverse Hashing ID Randomisation)

**RRIN** Routage vers le nœud intermédiaire aléatoire (Routing to the Randomly Intemediate Node)

**RW** Marche aléatoire

**Network WALN** Réseau local sans fil **(**Wireless Local Area Network)

**SAS** Schéma d'anonymat simple

**SB** Station de base

**TCP/IP** Transmission Control Protocol/Internet Protocol

**TFS** Schéma de filtrage basé sur un arbre

**TTL fake** Time To Live (faux durée de vie)

**WSN** Réseau de capteurs sans fil (wireless sensor network)

# Introduction générale

Un réseau des capteurs sans fil (RSCF) se compose généralement d'un grand nombre de nœuds de capteurs aux ressources limitées [1]. Chaque nœud agit comme une source d'informations, est capable de collecter des données de son environnement physique et de les transmettre vers un récepteur via un réseau multi-sauts, danslequel chaque nœud remplit la fonction de routage.

Les RCSF ont une multitude d'applications, où les capteurs sont discrètement intégrés dans l'environnement pour effectuer des opérations telles que la surveillance d'un objet sensible, le suivi et reportage. Dans de tels scénarios, le problème de confidentialité doit être soigneusement étudié, car la simple observation du fonctionnement du réseau peut révéler de grandes quantités d'informations confidentielles à des parties non autorisées. L'un des problèmes qui retient plus l'attention dans le domaine de la confidentialité est celui de la confidentialité d'emplacement, qui vise à empêcher les attaquants d'obtenir l'emplacement de nœuds spécifiques quiles intéressent.

Par exemple, des capteurs seront déployés dans des habitats naturels pour surveiller les animaux en voie de disparition. Lorsqu'un capteur signale un objet surveillé en envoyant une série de messages via le réseau de capteurs, un attaquant peut écouter clandestinement les communications interceptées du réseau de capteurs et être enmesure de déterminer l'emplacement exact de l'objet via l'analyse du trafic. Ce type d'applications nécessite des méthodes de routages avancées avec une protection de la confidentialité d'emplacement des nœuds sources (Resp. Stations de base).

La confidentialité dans les RCSF peut être classée en deux catégories: la confidentialité du contenu et la confidentialité contextuelle. Les menaces contre la confidentialité du contenu surviennent en raison de la capacité des adversaires à observer et à manipuler le contenu des paquets envoyés via un réseau de capteurs. Ce type de menaces est contré par le chiffrement et l'authentification. Cependant, un adversaire peut toujours être en mesure d'extraire des informations contextuelles sur le trafic transporté dans 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 nature ouverte de la communication sans fil permet aux attaquants d'écouter ou d'injecter facilement des paquets de données dans un réseau de capteurs. De plus, les réseaux de capteurs sont généralement déployés dans des zones ouvertes, où les nœuds de capteurs sans surveillance manquent de protection physique. Cela signifie que les attaquants rencontreront beaucoup moins d'obstacles lorsqu'ils attaqueront un réseau de capteurs.

Pour aborder la confidentialité de l'emplacement pour les réseaux de capteurs, nous examinons les caractéristiques de confidentialité et de performances de différents protocoles de routage de capteurs proposés dans la littérature, en particulier le niveau de confidentialité fourni, la consommation d'énergie et la latence de livraison des messages.

L'objectif de notre étude est de proposer une solution qui minimise les chances d'un adversaire de trouve la cible (source ou la station de base) en peu de temps - en d'autres termes, nous voulons prolonger le temps dont dispose un adversaire pour trouver une cible. C'est ce que nous allons examiner dans l'ordre suivant :

Dans le premier chapitre, nous présenterons les généralités sur les RCSF, y compris leurs systèmes d'exploitation, ainsi que les différentes contraintes, architectures, applications et composantes des réseaux decapteurs sans fil. Nous aborderons les problèmes rencontrés et certaines solutions nécessaires pour les résoudre.

Dans le deuxième chapitre, nous examinons les différents protocoles de sécurité visant à protéger la confidentialité d'identité, d'emplacement de la source et dans le troisième chapitre la confidentialité d'identité, d'emplacement de la station de base dans les RCSF contre un adversaire cherchant à trouver la source ou la destination d'un événement.

Dans le quatrième chapitre, nous donnons notre solution de protection de la confidentialité d'emplacement dela station de base.

Dans le quatrième chapitre, nous passerons à la simulation de notre proposition afin d'évaluer son niveau de confidentialité fourni, en utilisant la métrique « période de sécurité (ρ) » pour qualifier son niveau de confidentialité. Enfin, nous terminons par une conclusion générale et des perspectives.

# I Chapitre 1

# Introduction aux réseaux de capteur sans fil

## I.1 Introduction

Un réseau de capteurs sans fil (RCSF) est un réseau de capteurs autonomes et interconnectés qui communiquent entre eux à l'aide de technologies sans fil [1]. Ils sont couramment utilisés dans les environnements de surveillance tels que les processus industriels, les applications de suivi militaire, la surveillance de l'habitat, etc. Considérés comme le successeur des réseaux ad-hoc, les RCSF ont séduit les grandes entreprises pour leur riche potentiel applicatif, mais en raison de leur faible coût et de leur déploiement dans des zones hostiles, ils sont fragiles et sujets à diverses pannes.

Un réseau de capteurs est constitué d'un grand nombre de nœuds de capteurs déployés de manière dense à l'intérieur ou très près d'un phénomène observé. Les nœuds de capteurs sont équipés d'un processeur embarqué, ce qui leur permet d'effectuer localement des calculs simples et de ne transmettre que les données requises et partiellement traitées, ce qui favorise l'effort coopératif des nœuds de capteurs.

## I.2 Architecture des RCSF

Dans [1], un réseau de capteurs est décrit, où les nœuds de capteurs sont dispersés dans une zone, capables de collecter et de transmettre des données aux stations de base et aux utilisateurs finaux. Les données sont acheminées à l'aide d'une architecture multi-sauts sans infrastructure via le récepteur. Les récepteurs peuvent communiquer avec les nœuds du gestionnaire de tâches via Internet ou des satellites. La pile de protocoles utilisée par les nœuds récepteurs et capteurs intègre des considérations d'alimentation et de routage, intègre les données aux protocoles réseau, transfère efficacement la puissance sur le support sans fil et facilite les efforts coopératifs des nœuds vers le capteur. La pile de protocoles comprend la couche application, la couche transport, la couche réseau et la couche liaison de données.

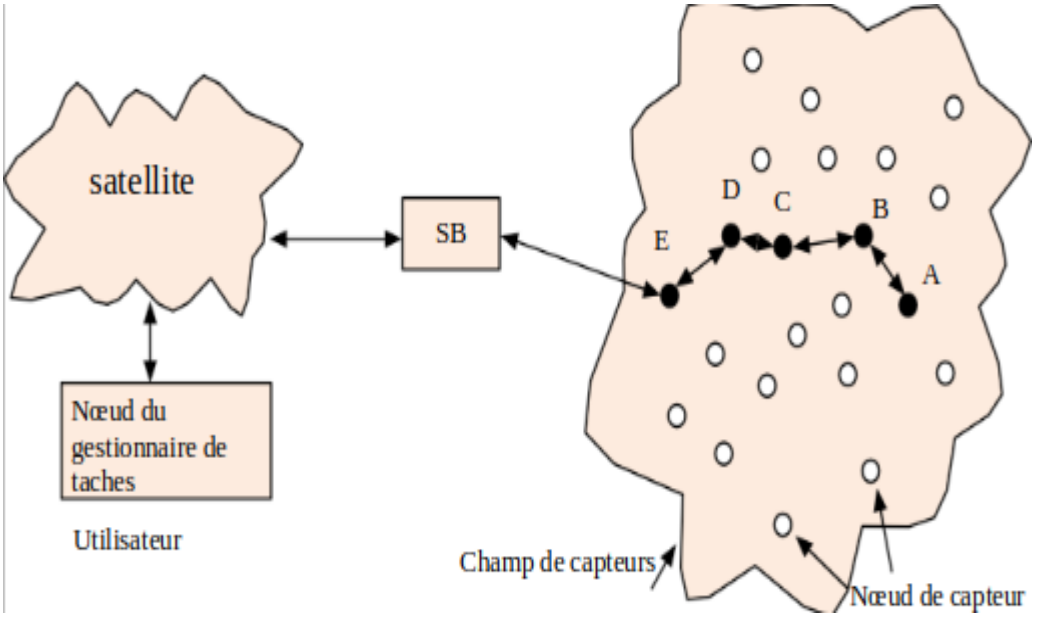


**Figure I.1Architecture des RCSF [1].**

## I.3 Domaines d'applications des RCSF

Les réseaux de capteurs sont composés de différents types de capteurs [3], notamment des capteurs sismiques, magnétiques, thermiques, visuels, infrarouges, acoustiques et radar. Ces capteurs peuvent surveiller diverses conditions ambiantes telles que la température, l'humidité, le mouvement des véhicules, l'état de la foudre, la pression, la composition du sol, les niveaux de bruit, la présence ou l'absence de certains objets et les niveaux de contrainte mécanique sur les objets attachés. Les nœuds de capteurs peuvent effectuer une détection continue, une détection d'événement, une identification d'événement, une détection d'emplacement et un contrôle local des actionneurs. La connexion sans fil de ces nœuds permet la micro-détection, ce qui promet de nombreux nouveaux domaines d'application. Ces applications peuvent être classées dans les domaines militaire, environnemental, domestique et autres domaines commerciaux. D'autres catégories potentielles comprennent l'exploration spatiale, le traitement chimique et les secours en cas de catastrophe.

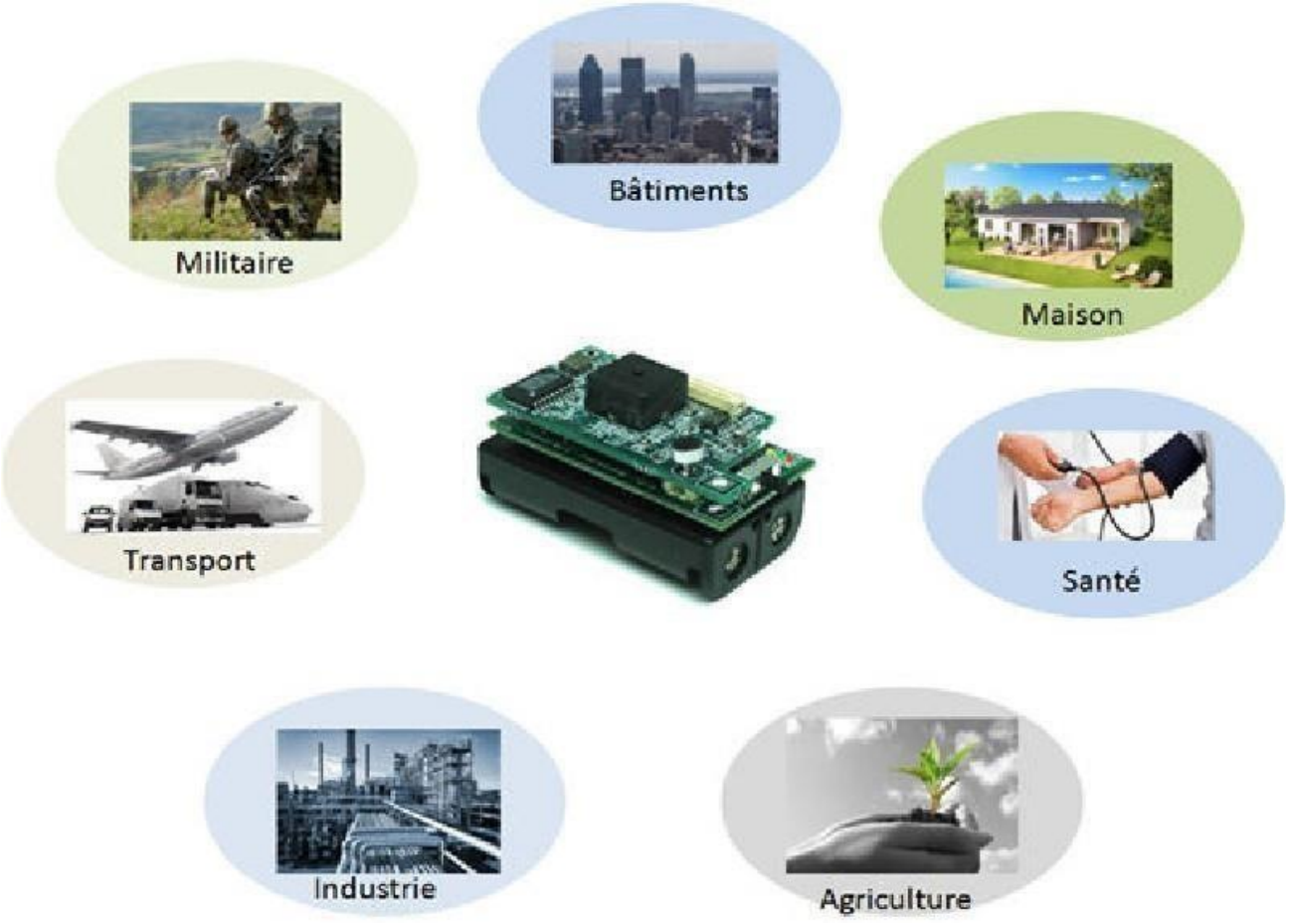


**Figure I.2 Domaines d'applications [3]**

- **Applications militaires**

Les réseaux de capteurs sans fil ont des applications potentielles dans les systèmes militaires [3] de commandement, de contrôle, de communication, d'informatique, de renseignement, de surveillance, de reconnaissance et de ciblage. Les réseaux de capteurs sont une technique de détection efficace pour les opérations militaires en raison de leurs caractéristiques de déploiement rapide, d'auto-organisation et de tolérance aux pannes. Contrairement aux capteurs traditionnels, la destruction de certains nœuds capteurs par des actions hostiles n'affecte pas autant l'opération militaire puisque les réseaux de capteurs reposent sur le déploiement dense de nœuds capteurs jetables et à faible coût.

Certaines des applications militaires des réseaux de capteurs sont la surveillance des forces, de l'équipement et des munitions amis, la surveillance du champ de bataille, la reconnaissance des forces et du terrain opposé, le ciblage, l'évaluation des dommages au combat et le nucléaire, détection et reconnaissance d'attaques biologiques et chimiques (NBC). Les réseaux de capteurs peuvent être utilisés pour surveiller l'état des troupes, des véhicules, de l'équipement et des munitions amis, couvrir des terrains critiques et surveiller de près les activités des forces opposées, recueillir des renseignements précieux sur les forces et le terrain opposés, incorporer dans des systèmes de guidage de munitions intelligentes, recueillir des données d'évaluation des dommages de combat et fournir un temps de réactioncritique pour les systèmes d'alerte chimique ou biologique en cas d'attaques NBC.

- **Applications environnementales**

Les réseaux de capteurs ont un large éventail d'applications environnementales [3], y compris le suivi des mouvements d'oiseaux, de petits animaux et d'insectes. Ces réseaux sont également utilisés pour surveiller les conditions environnementales qui affectent les cultures et le bétail, telles que l'humidité et la température du sol. De plus, ils peuvent être utilisés pour l'irrigation, ainsi que comme macro-instruments pour la surveillance de la Terre à grande échelle et l'exploration planétaire.

La détection chimique et biologique est une autre application importante des réseaux de capteurs, qui peuvent être utilisés pour détecter les polluants et autres contaminants dans l'environnement. L'agriculture de précision est un autre domaine où les réseaux de capteurs sont utilisés pour surveiller l'humidité du sol et d'autres facteurs qui affectent les rendements des cultures.

- **Applications de santé**

Les réseaux de capteurs ont diverses applications de soins de santé [3], telles que la fourniture d'interfaces pour les personnes handicapées, la surveillance intégrée des patients, les diagnostics, l'administration de médicaments hospitaliers, la surveillance des mouvements internes et des processus d'insectes ou d'autres petits animaux, la surveillance à distance, le suivi et la surveillance des données physiologiques humaines Médecins et patients à l'hôpital.

L'une des principales applications des réseaux de capteurs est la surveillance à distance des données physiologiques humaines. Les données physiologiques collectées par le réseau de capteurs peuvent être stockées longtemps pour l'exploration médicale. Le réseau de capteurs installé peut également surveiller et détecter le comportement des personnes âgées, comme les chutes, permettant aux médecins d'identifierplus tôt des symptômes prédéfinis. Les réseaux de capteurs facilitent une meilleure qualité de vie pour lessujets par rapport aux centres de traitement.

- **Application commerciale**

Diverses applications commerciales des réseaux de capteurs sont décrites dans [3]. Ces applications incluent la surveillance de la fatigue des matériaux, la construction de claviers virtuels, la gestion des stocks, la surveillance de la qualité des produits, la construction d'espaces de bureau intelligents, le contrôle des facteurs environnementaux dans les immeubles de bureaux, le guidage des robots dans les environnements de fabrication et la création de jouets interactifs et de musées, l'automatisation des processus d'usine, surveillance et intégration de nœuds de capteurs dans des structures intelligentes, diagnostic de machines, amélioration des transports, chambres de traitement de semi-conducteurs, machines tournantes, souffleries, instrumentation de chambre an échoïque, détection de vol de véhicules. Détection et surveillance, suivi de véhicules, etc.

- **Application à domicile**

La domotique [3] fait référence à l'intégration de nœuds de capteurs intelligents et d'actionneurs dans des appareils électroménagers tels que des aspirateurs, des fours à micro-ondes, des réfrigérateurs et des magnétoscopes. Ces nœuds de capteurs permettent la communication entre l'appareil lui-même et avec des réseaux externes tels qu'internet ou des satellites. Cette connectivité permet aux utilisateurs finaux de gérer facilement leurs appareils domestiques à la fois localement et à distance.

D'autre part, la conception d'environnements intelligents peut être abordée sous deux angles : centré sur l'humain et centré sur la technologie. D'un point de vue centré sur l'humain, les environnements intelligents doivent s'adapter aux besoins des utilisateurs finaux, en tenant compte des capacités d'entrée/sortie. Une perspective centrée sur la technologie se concentre sur le développement de technologies matérielles, de solutions réseau et de services middleware pour prendre en charge un environnement intelligent.

## I.4 Comparaison entre les RCSF et les réseaux sans fil classiques

Le tableau ci-dessous présente une comparaison entre les Réseaux de Capteurs sans Fil (RCSF) et les réseaux sans fil traditionnels [2], en se basant sur cinq critères : la quantité de nœuds, l'importance de la consommation énergétique, l'importance de la qualité de service et les modes de communication.

**Tableau 1 Comparaison entre les RCSF et les réseaux sans fil**

| | Réseau WLAN | Réseau cellulaire | RCSF |
|---|---|---|---|
| Quantité de nœuds | Diminué | Élevé | Très élevé |
| L'importance de la consommation d'énergie | Réduit étant donné la facilité de recharge des nœuds. | Réduit étant donné la facilité de recharge desnœuds. | Très élevé |
| Importance dela qualité de service | Élevée | Élevée | Diminué |
| Type de communication | Point à point | Du mobile vers la station de base et vice versa | broadcast, multicast, Convergecast |

## I.5 Composants d'un nœud de capteur

Un nœud de capteur est le composant de base d'un réseau de capteurs sans fil et se compose de quatre composants principaux : une unité de capteur, une unité de traitement, une unité d'émetteur- récepteur et une unité d'alimentation [1]. Des composants supplémentaires tels que des systèmes de suivi, des générateurs d'énergie et des mobilisateurs peuvent être présents en fonction des besoins spécifiques de l'application.

L'unité de capteur se compose de deux sous-unités : capteur et convertisseur analogique-numérique (ADC). Des capteurs captent et mesurent des phénomènes physiques et produisent des signaux analogiques. Ces signaux analogiques sont convertis en signaux numériques par des ADC avant d'être envoyés à l'unité de traitement.

L'unité de traitement, typiquement équipée d'une petite unité de stockage, gère les opérations nécessaires pour que le nœud capteur collabore avec d'autres nœuds dans l'exécution des tâches de détection assignées. Il effectue des tâches telles que le traitement des données, la prise de décision et la coordination au sein du réseau.

L'unité d'émission-réception facilite la communication entre le nœud de capteur et le réseau. Il permet la transmission et la réception de données vers et depuis d'autres nœuds ou une station de base centrale.

L'unité de puissance est un composant vital d'un nœud de capteur, fournissant l'énergie nécessaire pour soutenir ses opérations. Les unités d'alimentation peuvent inclure des batteries ou peuvent être complétées par des unités de récupération d'énergie telles que des cellules solaires, qui convertissent l'énergie solaire en énergie électrique.

De plus, il peut y avoir d'autres sous-unités dépendantes de l'application incorporées dans un nœud de capteur, en fonction d'exigences spécifiques. Ces sous-unités peuvent varier et peuvent inclure des composants tels que des capteurs ou des actionneurs spécialisés adaptés à un domaine d'application particulier.

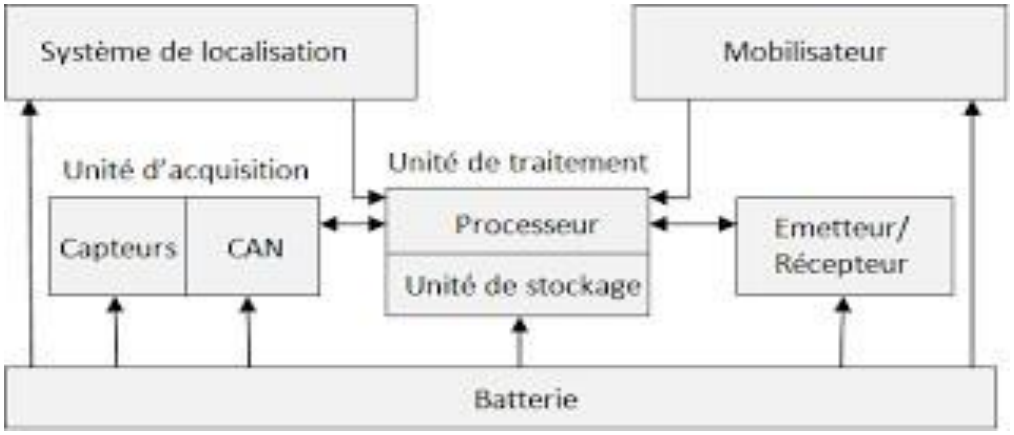


**Figure I.3 Composants d'un nœud capteur [1]**

## I.6 Problèmes de RCSF

- **Mémoire et espace de stockage limités**

Le capteur est un composant miniature qui présente des contraintes en termes d'espace mémoire, de stockage et de vitesse de calcul. Lorsqu'il s'agit de capteurs, il est important de prendre en compte leurs limitations en matière d'espace mémoire et de stockage [4]. En raison de leur petite taille, ces capteurs disposent souvent d'une quantité limitée de mémoire pour stocker les données qu'ils collectent. Cela signifie que les capteurs doivent être efficaces dans l'utilisation de l'espace mémoire disponible afin de stocker les informations essentielles.

- **Limitation en énergie**

La limitation en énergie est l'une des contraintes les plus importantes lors du déploiement de capteurs [3], en particulier dans des endroits inaccessibles ou difficiles d'accès. Dans de telles situations, il n'est pas possible de changer les batteries ou de les recharger facilement, ce qui rend leur utilisation coûteuse pour les capteurs. Par conséquent, il est crucial de préserver les ressources énergétiques embarquées

avec les capteurs afin de prolonger leur durée de vie et, par extension, celle de l'ensemble du réseau.

- **Risques inattendus**

L'application du réseau de capteurs peut varier entre une surveillance constante et une surveillance après une longue période. Les capteurs sont considérés sans surveillance lorsqu'ils sont déployés dans des zones telles que derrière les lignes ennemies. Cependant, cela présente plusieurs mises en garde.

Tout d'abord, les capteurs sans surveillance sont exposés à des attaques physiques [4]. Étant déployés dans un environnement ouvert aux ennemis, ils peuvent faire face à des conditions climatiques difficiles. Cela signifie qu'ils doivent être résistants aux agressions physiques et capables de fonctionner correctement même dans des situations hostiles.

Deuxièmement, la gestion à distance des capteurs sans surveillance est un défi. Étant donné que ces capteurs sont situés dans des zones inaccessibles ou dangereuses, la détection d'une attaque physique ou la maintenance des capteurs, telle que le remplacement de batteries, devient impossible. Il est donc essentiel de concevoir des capteurs autonomes et durables qui nécessitent peu ou pas de maintenance.

Il convient de noter qu'il existe deux types d'attaques, Attaque passive et l'attaque active. Telles que la première attaque consiste à écouter ou copier des informations de manière illicite (suivi de l'emplacement d'un capteur). Le second attaque (attaque active) consiste à altérer (modifier) des informations ou à altérer le bon fonctionnement d'un capteur.

L'attaque passive est divisée en deux parties principales :

Adversaire local/global : Un adversaire local peut surveiller seulement une petite partie du réseau, généralement l'équivalent de la portée de transmission d'un nœud de capteur ordinaire. Un adversaire global est capable de surveiller tout le trafic généré et transmis dans le réseau.

## I.7 Sécurité dans RCSF

Un réseau de capteurs sans fil (RCSF) est un type spécifique de réseau qui présente des similitudes avecles réseaux informatiques traditionnels tout en ayant ses propres caractéristiques uniques. Pour assurer la sécurité d'un RCSF, un protocole de sécurité doit répondre à plusieurs conditions [4], notamment la confidentialité des données, l'intégrité des données, la fraîcheur des données, l'auto-organisation, la localisation et l'authentification.

- **Confidentialité des données**

Est l'assurance que les données collectées, transmises ou stockées par les capteurs ne sont accessibles que par des entités autorisées. Cela implique que les données ne peuvent pas être lues ou interceptées par des acteurs malveillants ou non autorisés, même s'ils sont en mesure de capturer ou d'accéder au trafic du réseau.

- **Intégrité des données**

Pour empêcher la modification malveillante des données en transit, l'intégrité des données garantit

qu'aucune altération n'a eu lieu pendant leur transmission. Même en l'absence de nœuds malveillants, des altérations accidentelles peuvent survenir.

- **Fraîcheur des données**

En plus de la confidentialité et de l'intégrité, la fraîcheur des données est essentielle pour éviterles attaques de rejoue, où d'anciens messages sont renvoyés. Cela est particulièrement crucial lorsque des clés partagées sont utilisées, nécessitant leur renouvellement régulier.

- **Auto-Organisation**

Les réseaux de capteurs sans fil sont nécessitent une auto-organisation. L'absence d'infrastructure fixe pour la gestion du réseau pose des défis pour la sécurité, car chaque capteur doit être flexible et autonome.

- **Localisation**

La capacité à localiser automatiquement chaque capteur est essentielle, notamment pour détecter des anomalies. Un réseau de capteurs doit fournir des informations précises sur l'emplacement des défauts.

- **Authentification**

En plus de modifier les données, un adversaire peut injecter des paquets additionnels. L'authentification garantit que les données proviennent de la source prétendue. Elle est également nécessaire pour les tâches administratives. L'authentification peut être réalisée à l'aide de clés partagées pour calculer des codes d'authentification de message.

## I.8 Systèmes d'exploitation pour les RCSF

- **Contiki**

Contiki [3] est un système d'exploitation open source et portable spécialement conçu pour lesréseaux de capteurs. Il a été développé par l'équipe des systèmes embarqués de l'Institut des sciences informatiques suédoises et offre une compatibilité avec de nombreuses plateformes. Une caractéristique notable de Contiki est son environnement de simulation Netsim.

Ce système d'exploitation prend en charge le multitâche et implémente la pile protocolaire TCP/IP. Il est remarquablement peu exigeant en termes de mémoire, ne nécessitant que quelques kilooctets de code et quelques centaines d'octets de RAM. Contrairement à TinyOS, qui est basé sur le modèle d'événements, Contiki repose sur le multitâche et l'édition statique des liens.

- **TinyOS**

TinyOS [3] est un système d'exploitation open source conçu pour les RCSF. Il est basé sur une architecture orientée composants qui permet une implémentation rapide et favorise l'innovation. Le noyaugénéré par TinyOS est de petite taille, ne faisant que quelques kilo-octets, ce qui répond aux

contraintes de mémoire imposées par les réseaux de capteurs.

Les principales caractéristiques de TinyOS incluent sa faible consommation de ressources, sa modularité, sa prise en charge des communications sans fil et sa flexibilité en termes de programmation. TinyOS est capable de gérer les réseaux de capteurs de manière efficace et de traiter les données générées par ces capteurs de manière efficace. Il permet également la mise en œuvre de protocoles de communication avancés pour permettre une communication fiable entre les nœuds du réseau.

## I.9 Conclusion

Dans ce chapitre, on a découvert les réseaux de capteurs sans fil, et leurs applications et architecture. Nous avons également mentionné certaines mesures de sécurité dans RCSF. Dans le chapitre suivant, on étudiera les différents protocoles de préservation de la confidentialité d'emplacement d'une source et station de base dans les RCSF.

# II Chapitre 2

## État de l’art sur la confidentialité d’emplacement dans les RCSF

# II.1 Introduction

Un adversaire peut utiliser essentiellement deux manières pour repérer des cibles, à savoir les identités des nœuds et le modèle de trafic. Les paquets transmets dans le réseau contiennent à la fois les charges utiles et les entêtes. Les entêtes sont utilisés à chaque saut à des fins de routage et contiennent les identités de l'expéditeur et le destinataire du paquet. En supposant que la charge utile du paquet est protégée par chiffrement, l'attaquant peut toujours récupérer des informations sensibles à partir des en-têtes et les utiliser pour déterminer l'emplacement de ces nœuds. Par conséquent, la première étape pour assurer la confidentialité de l'emplacement est de cacher ces identifiants. Même si c'est informations sont bien protégées, un adversaire peut toujours trouver les informations d'emplacement en analysant le trafic généré par le réseau.

Dans ce qui suit, nous allons examiner les plus pertinentes stratégies de protection de la confidentialité d'emplacement dans les RCSF.

# II.2 Technique de Préservation la confidentialité d'emplacement d'un nœud source

- **Introduction**

L'objectif principal des mécanismes de confidentialité de l'emplacement de la source est d'empêcher un attaquant capable d'effectuer des attaques d'analyse de trafic de déterminer l'emplacement d'un nœud signalant la présence d'un événement dans son voisinage. En effet, l'intérêt de l'attaquant n'est pasle nœud lui-même mais l'emplacement de l'événement. Ce problème a été décrit pour la première fois dans ce qui bien connu sous le nom de « Panda Hunter Game : jeu du Panda et Chasseur » qui se réfère à un modèle formel d'applications de surveillance des biens qui peuvent bénéficier de la protection de laconfidentialité de l'emplacement source.

Afin de faciliter l'analyse et la discussion de la confidentialité de l'emplacement de la source/base station dans les réseaux de capteurs, nous utilisons ce modèle pour capturer la plupart des caractéristiques pertinentes des réseaux de capteurs et des adversaires potentiels. Dans ce chapitre, nous commençons par introduire le jeu du chasseur et panda, ensuite nous examinons plusieurs techniques qui fournissent la confidentialité d'emplacement de la source
/station de base existante.

- **Le modèle de Chasseur et Panda**

Avant d'examiner les techniques existantes pour protéger la confidentialité d'emplacement de la source de données, nous examinons brièvement en premier le « Panda Hunter Game », un problème classique, sur la base duquel la confidentialité d'emplacement de la source dans WSN a été largement étudiée dans la littérature.

Dans ce model [5], un large éventail de nœuds capteurs a été déployé par l'organisation Save-The-Pandapour surveiller le mouvement des pandas. Lorsqu'un panda se déplace sur le terrain, il sera détecté par un capteur à proximité, qui enverra un message à la station de base via des techniques de routage multi-sauts. Si le panda reste à proximité, le même capteur continuera à renvoyer des messages à la station de base. Si le panda se déplace, tous les capteurs qui sont à portée de son nouvel emplacement enverront des messages à la station de base. Le modèle Panda- Chasseur suppose également qu'il y a un chasseur dans le rôle de l'adversairequi peut écouter les communications entre les capteurs, qui sont cryptées, et tente de capturer le panda en analysant et traçant en arrière le chemin de routage des messages jusqu'à ce qu'il atteigne la source. Par conséquent, une technique de routage qui respecte la confidentialité devrait empêcher le chasseur de localiserla source, tout en livrant les données à la station de base. Dans le modèle Chasseur-Panda, il est supposé qu'il n'y a qu'un seul panda, donc une seule source, et cette source peut être fixe ou mobile. Pendant toute la durée de vie du réseau, les nœuds capteurs enverront continuellement des données, et le chasseur peut les utiliser à son avantage pour suivre et chasser le panda. Il est supposé que la source inclut son *ID* dans les messages chiffrés, mais seul la station de base peut déterminer l'emplacement d'un nœud à partir de son *ID*. Par conséquent, même si le chasseur est capable de casser le cryptage dans un délai raisonnablement court, il ne peut pas indiquer l'emplacement de la source.

- **Cas d'un adversaire local**

Les auteurs dans [5] ont examinés deux grandes classes de protocoles de routage : le routage par inondation et le routage impliquant seulement un chemin de la source vers la station de base. L'étude des performances de ces protocoles en termes de confidentialité, en considérant le compromis entre la confidentialité et la consommation d'énergie, montre que ces protocoles ne peuvent pas assurer la confidentialité de l'emplacement de la source. Afin de fournir des communications efficaces et privées de l'emplacement de la source, les auteurs ont proposé une nouvelle technique qu'ils ont appelé le routage fantôme ; qui est une combinaison d'un chemin unique variable et une inondation.

Dans le routage fantôme, la livraison de chaque message passe par deux étapes : (1) étape de marche aléatoire, qui peut être une pure marche aléatoire ou une marche dirigée, destinée à diriger le message vers une source fantôme, et (2) une étape ultérieure d'inondation/routage à chemin unique destinée à délivrer le message à la station de base. Lorsque la source transmet un message, le message est unicast de manière aléatoire pour un total de *h* sauts. Après les *h* sauts, dans l'inondation fantôme, le message est inondé à l'aide de l'inondation basique (ou probabiliste). Dans le routage fantôme à chemin unique, après les *h* sauts, la transmission du message basculer vers le routage à chemin unique.

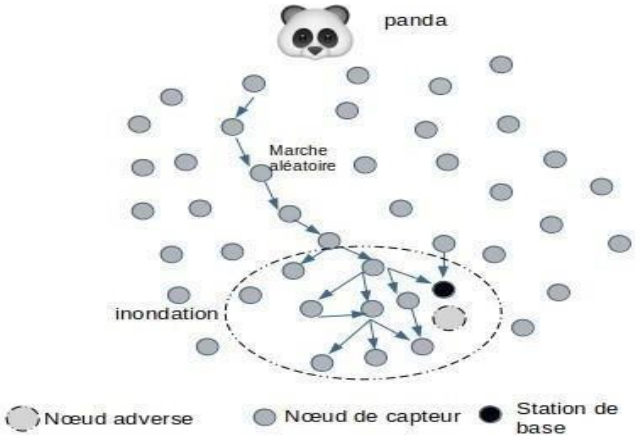


**Figure II.1 Routage fantôme[5]**

L'inondation (resp. Chemin unique) fantôme peut améliorer considérablement la période de sûreté, car chaque message peut emprunter un chemin différent (le plus court) pour atteindre n'importe quel nœud du réseau. Par conséquent, une fois que l'adversaire a entendu le message ***i***, il peut s'écouler beaucoup de temps avant qu'il ne reçoive (i +1). Lorsqu'il reçoit enfin le message (i+1), l'expéditeur immédiat de ce message peut éloigner l'adversaire de la source. Cependant, le problème de cette approche est la latence des messages et la consommation d'énergie qui deviennent élevées.

La méthode de piégeage cyclique (CEM : Cyclic Entrapement Method) [6] tente d'empêcher un adversaire d'atteindre la source en retardant son avancement sur le chemin de routage vers la source en créantdes boucles pour le piéger. Après le déploiement du réseau de capteurs et avant la transmission des données de la source vers la station de base, plusieurs boucles sont générées. Chaque boucle est constituée de plusieurs nœuds capteurs. Lorsqu'un message est transmis d'une source à la station de base, quand il arrive sur une des boucles préconfigurées, elle devient active et commencera à émettre de faux messages autour d'elle. Le faux trafic généré par les boucles peut coexister avec les vrais messages transmets par la source.

Un adversaire qui utilise l'analyse de trafic pour suivre la trace des messages vers la source arrive à un moment donné sur un nœud où le chemin réel se croise avec une boucle. A ce point, l'adversaire ne pourrapas distinguer le vrai message entrant transmet par le nœud source, qu'il cherche à suivre, des messages généréspar la boucle. Ainsi, il doit décider au hasard de la prochaine direction à choisir. En cas d'un mauvais choix, il sera entraîné dans la boucle. En s'assurant que le chemin réel d'un message est susceptible de traverser plusieurs boucles, cela peut augmenter le temps nécessaire à un adversaire pour localiser un nœud source.

Dans [7], les auteurs ont proposé une technique appelée GROW qui utilise la marche aléatoire de la source et de la SB. La SB initie en premier une marche aléatoire qui sert comme un chemin récepteur. La source transmet des paquets en utilisant GROW (greedy random walk) qui finira par se croiser avec

le chemin récepteur statique provenant de la station de base. Une fois que le message atteint le récepteur, il estexpédié vers la SB à travers le chemin préétabli.

L'algorithme GROW tente d'étendre la marche aléatoire autant que possible en évitant les nœuds visités. Pour cela, un nœud capte, à chaque instant, un de ces voisins qui n'a pas participé dans la marche aléatoire. Pour éviter à la marche aléatoire de rester autour de la source et de créer des chemins aléatoires sans nœuds commun, le protocole utilise un filtre qui stocke tous les voisins actuels dans le paquet transféré. Ainsi, quand un nœud capte au hasard l'un de ces voisins au prochain saut, il vérifie si ce dernier est déjà visité. Dans le cas où la source et la SB sont très proche l'une de l'autre, les chemins aléatoires créent de la source et de la SB ont une grande chance de se croiser à un point qui serait proche de la source et de la SB ; ce qui permet à un adversaire de tracer le chemin. Pour éviter cela de se produire, une longueur minimale pour le chemin de marche aléatoire est exigée.

PRLA [8] introduit l'angle d'inclinaison à la marche aléatoire, car dans plusieurs situations, l'augmentation de la longueur du chemin de routage n'augmente pas le niveau de protection, puisque la source fantôme n'est pas à un bon emplacement. Si le plus court chemin entre la source fantôme et la station de base traverse la zone de couverture du nœud source, alors la phase de marche aléatoire du chemin de routage fantôme ne fera aucune contribution dans le niveau de protection et la période de sécurité sera plus courte que la longueur du chemin de transmission. Un tel chemin de transmission introduit un gaspillage d'énergie et une latence sans améliorer la période de sécurité (voir la figure II.2). Pour résoudre ce problème, PRLA est proposée pour orienter la marche aléatoire afin de diminuer la probabilité de choisir un chemin de gaspillage. L'angle d'inclinaison d'un nœud est l'angle formé par la droite reliant ce nœud et la station de base et la droite reliant la source et la station de base.

L'idée de PRLA consiste en trois étapes suivantes :

1 La SB inonde une requête dans le réseau pour que chaque nœud puisse configurer le chemin le plus courtvers SB et diviser ses voisins en deux ensembles de directions selon leurs distances au nœud SB.

2 Le nœud source initie une inondation limitée dans la zone de couverture de la marche aléatoire. L'inondation limitée de la source permet à chaque nœud d'obtenir les angles d'inclinaison de ses voisins etde calculer la probabilité de transmission de chaque voisin.

3 La source envoie des paquets de données au nœud SB.

Selon l'angle d'inclinaison, chaque paquet de données sera d'abord transmis en utilisant une marche aléatoire avec *Hw* sauts. Ensuite, il sera transmis le long du plus court chemin de la source fantôme au nœud SB.

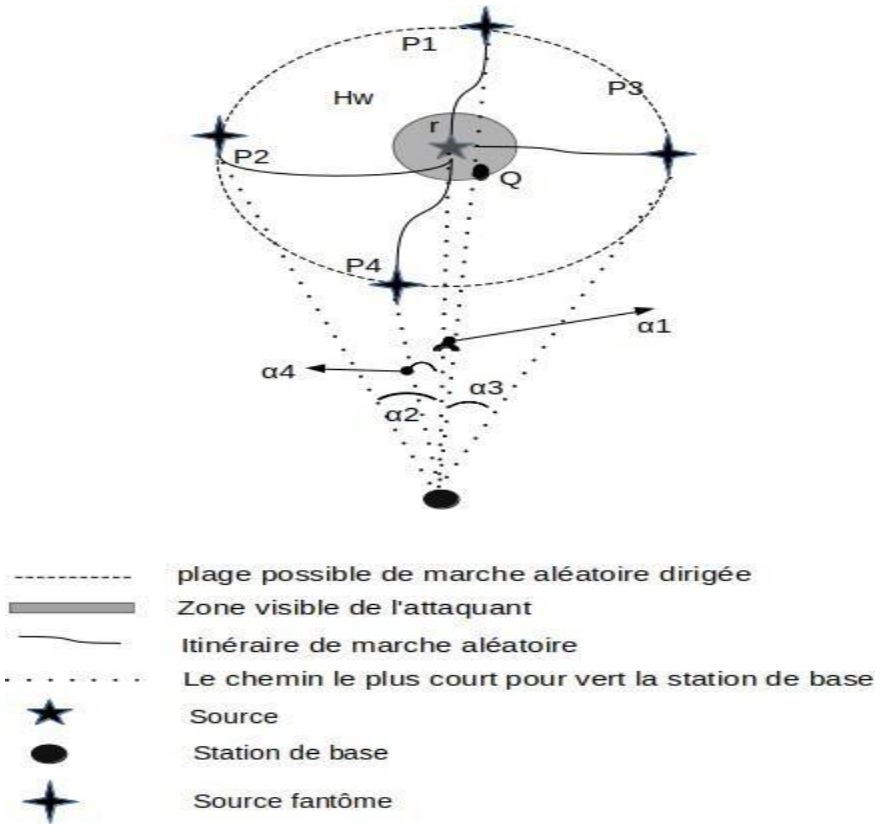


**Figure II.2 Routage de diffèrent messages [8]**

- ## Cas d'un adversaire global

Dans [9] sont proposés quatre algorithmes pour préserver la confidentialité d'emplacement d'une source contre un adversaire global, qui sont nommés : algorithme naïf, algorithme global optimal, algorithmeheuristique et algorithme probabiliste.

### 1. Algorithme Naïf

Cette technique consiste à utiliser des messages factices pour masquer les messages d'événement réels. Chaque nœud capteur diffuse un message factice à ses voisins à la fin d'une période de temps fixe, appelée période de maintenance. La période de maintenance est suffisamment longue pour que la durée de vie des capteurs soit grande.

La transmission d'un message réel est retardée et remplace un message factice. Ainsi, un adversaire ne peut pas distinguer le message réel, car il apparaît comme c'est un message de maintenance qui est transmet. Un nœud recevant le message réel doit attendre la fin de la période de maintenance en cours pour transmettre le message au nœud suivant le long du chemin de routage vers la SB. Cette solution assure un niveau élevé de confidentialité, car pour un adversaire, il n'existe pas de différence entre avant et après la transmission d'un événement. Cependant, la latence est élevée à cause d'attente en chaque période de maintenance.

## 2. Algorithme global

Dans cette approche, la durée des périodes de maintenance ne sera plus fixe, mais elle est déterminée par un générateur de nombres pseudo-aléatoires (PRNG). En utilisant un PRNG, il est possible pour un nœudsource de prédire les nombres pseudo-aléatoires à venir pour lui-même et aussi pour tous les nœuds du réseau.Ainsi, lorsque la topologie globale du réseau est disponible et tous les nœuds capteurs sont bien synchronisés dans le temps ; un nœud peut calculer le chemin de routage le plus rapide qui conduit à un délai de livraisonle plus court pour un message d'événement. Cette approche peut optimiser le délai de livraison en ajustant dynamiquement les périodes de maintenance en fonction des conditions du réseau.

## 3. Algorithme heuristique

L'algorithme global est optimal, mais il n'est pas pratique pour chaque nœud de stocker toute la topologie du réseau et calculer le plus rapide. Dans cette approche, chaque nœud sélectionne le nœud suivant vers la SB en se basant seulement sur les PRNG de ses voisins et de leur distance à la SB. De cette façon, chaque nœud n'a pas besoin de connaître la topologie globale et de stocker tous les PRNG pour tous les nœuds ; il luisuffit de stocker les PRNG de tous ses voisins. Un nœud peut sélectionner parmi tous ces voisins celui ayant le temps d'attente minimum comme nœud suivant dans le chemin de routage. Cependant, ce n'est pas toujoursla meilleure option, car il est possible que celui choisie soit plus éloignée de la station de base, ce qui augmentera le délai de livraison puisque le message passera par plus de nœuds intermédiaires.

## 4. Algorithme probabiliste

L'algorithme probabiliste vise à masquer les chemins de livraison et les sources des messages dans un réseau de capteurs tout en réduisant la surcharge de communication. L'algorithme suppose qu'un attaquant ne peut pas déterminer l'emplacement exact de l'expéditeur d'un message en écoutant la communication. Au lieude cela, l'attaquant doit surveiller différentes zones du réseau pour déterminer l'emplacement de l'expéditeur. Pour réduire la surcharge de communication, un nœud de capteur peut utiliser les messages de maintenance envoyés par ses voisins proches pour masquer ses messages d'événement réels. Cela signifie que seul un petitnombre de nœuds doivent envoyer des messages de maintenance après des périodes aléatoires, et leurs portéesradios combinés peuvent couvrir l'ensemble du réseau. Si l'attaquant entend toujours au moins un message à n'importe quel endroit et à n'importe quelle période de temps, il sera difficile pour eux d'identifier le chemin de livraison de tout message d'événement envoyé sur le réseau. En effet, il y aura de nombreux choix à chaquepoint du chemin puisque le message observé à un nœud de capteur donné peut provenir de n'importe lequel deses voisins.

Le schéma proposé dans [10] consiste en trois phases de routage : routage vers un nœud intermédiairechoisi aléatoirement (RRIN : *Routing to the Randomly Intemediate Node*), routage dans un

anneau de mixage réseau (NMR : *Network Mixing Ring*) et transmission des messages à la SB. (Voir la figure II.3)

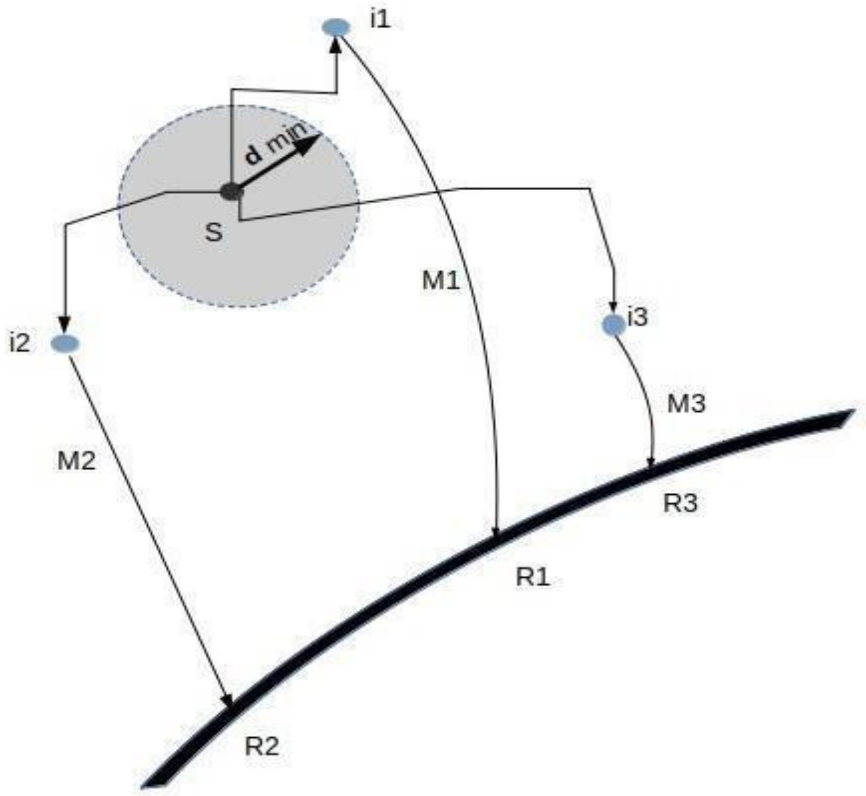


**Figure II.3 Illustration des deux premières phases de routage[10]**

La première phase fournit la confidentialité locale d'emplacement de la source. Le nœud intermédiaire est censé être éloigné du nœud source réel de sorte qu'il est difficile pour les adversaires d'obtenir les informations de la source réelle à partir du nœud intermédiaire sélectionné. Quand le nœud intermédiaire reçoitun message de données, il le transmet au nœud de l'anneau le plus proche.

Dans la deuxième phase, le paquet de données est transmet saut par saut et sera mélangé avec d'autres paquets via un anneau de mélange de réseau. Le message peut passer un nombre aléatoire de fois avant d'êtretransmet à la station de base. Tant qu'il est impossible pour un adversaire de distinguer l'initiateur du message du transitaire de message dans l'anneau, il serait alors impossible pour les adversaires d'identifier l'emplacement réel de source du message. Cette phase fourni une confidentialité de l'emplacement de la sourceau niveau du réseau (global). Enfin, le paquet de données sera transmis au nœud SINK à partir de certains nœuds spécifiques de l'anneau de mélange avec une certaine probabilité. Cette probabilité est un paramètre lié au nombre de nœuds de l'anneau mélangeur.

Dans [11] les auteurs proposent d'utiliser le trafic factice bien choisi pour dissimuler la source d'événement qui est combiné avec un mécanisme de suppression de paquets factice pour éviter la surcharge du trafic du réseau. Le mécanisme consiste sélectionner quelques nœuds capteurs comme des praxies chargésde filtrer les paquets factices sur leur chemin vers la station de base. Étant donné que le

placement optimal des mandataires est un problème complexe, des heuristiques de recherche locale sont utilisées. Deux schémassont proposés : le schéma de filtrage basé sur les proxys (PFS) et le schéma de filtrage basé sur les arbres (TFS)pour localiser précisément les mandataires.

## 1. Schéma de filtre basé sur proxy (PFS)

Après le déploiement du réseau, chaque proxy diffuse un message « hello » avec un TTL (time to live) qui est assez grand pour atteindre tout nœud dans le réseau. Chaque nœud recevant le message « hello » enregistre le proxy qui lui est le plus proche comme proxy par défaut. Chaque nœud envoie également une repose à son proxy afin qu'il soit informé des nœuds qu'il sert. Lorsqu'un nœud détecte un événement, il reporte la transmission du message d'événement chiffré au prochain intervalle probabiliste, afin qu'il ne soit pas différencié du trafic factice par l'analyse de trafic temporelle.

Lorsqu'un proxy reçoit un message, s'il s'agit un message factice, il est rejeté sinon, le proxy le déchiffreen utilisant la clé partagée avec BS, le met en mémoire tampon appropriée puis le retransmet vers la SB. Dans le cas où un message réel n'est pas disponible, le proxy envoie un message factice chiffré à sa place. A noter qu'un proxy peut distinguer un message réel d'un message factice, car un message réel peut le déchiffrer correctement à l'aide de la paire de clé correspondante. Si un proxy reçoit un message d'un autre proxy, il le transmet simplement au saut suivant. Pour optimiser le trafic réseau, le critère considéré dans le placement d'un proxy est la minimisation du trafic agrégé. Cependant, trouver une solution optimale est complexe. Ainsi, une heuristique basée sur la recherche locale est proposée.

## 2. Schéma de filtrage basé sur un arbre (TFS)

Dans PFS, même si un message peut traverser plusieurs proxys, il est filtré uniquement par le proxy par défaut du nœud qui est l'origine du message. Si le nombre de proxys est assez élevé, il est possible de réduireencore le trafic factice, en le filtrant au niveau de plusieurs proxys le long du chemin de la source vers la station de base. En se basant sur cette idée, les proxys sont organisés sous forme d'un arbre dont la racine est la station de base. Ainsi, les proxys, dans TFS, forment une hiérarchie où chaque proxy a un nœud parent et peut avoir plusieurs nœuds fils. Un filtrage à plusieurs niveaux peut diminuer le trafic réseau en éliminant les messages inutiles. Cependant, il augmente la latence, car un message doit passer par plusieurs proxys et peut subir des retards induits par la mise en mémoire tampon au niveau des proxys le long du chemin vers la SB.

L'idée de base de l'approche proposée dans [12] est d'exploiter les balises de la couche Mac, qui sonttransmises régulièrement pour transférer les messages des événements réels vers la station de base, sans ajouter de trafic factice. Deux versions de la solution ont été proposées appelées respectivement Cross-layer et doubleCross- layer. Une solution naïve (voir la solution 1 dans la figure II.4) consiste à diffuser un message en utilisant uniquement la couche Mac. La confidentialité obtenue

atteint niveau parfait, puisque toutes les balisesmodifiées fonctionnent exactement de la même manière que les balises régulières. Cependant, la latence peut être trop élevée, car elle est décidée par l'intervalle des balises et la distance entre la source et la SB.

**La solution Cross-layer** (voir la solution 2 dans la figure II.4) a deux étapes : étape de la couche Mac et étape de routage. Dans la première étape, les nœuds fonctionnent de la même manière que la solution naïve. Quand un nœud capteur détecte un événement, il diffuse le message d'événement dans les balises de la couche MAC pendant h sauts (hast un paramètre système) vers un nœud appelé pivot. Ensuite, il bascule vers l'étape de routage et message est routé à SB. Dans cette solution, la latence est déterminée par l'étape 1. Donc,pour avoir une faible latence, le pivot doit être très proche de la source.

**La solution double Cross-layer** (voir la solution 3 dans la figure II.4) permet de contrôler la latence et améliorer la confidentialité. Dans cette solution, l'étape de diffusion sur la couche Mac est divisée en deux parties. De même que la méthode cross-layer, après la première diffusion par la couche Mac, un nœud *pivot* est choisi. Le pivot transmet l'événement vers un nœud aléatoire choisi du réseau au lieu de SB, en utilisant le routage. A partir de ce nœud, l'événement entame la seconde étape de diffusion par la couche Mac vers un deuxième nœud *pivot* choisi dans le réseau qui route l'événement vers la SB. Cette solution permet de fournir un niveau de sécurité plus élevé. La latence peut être similaire que cross-layer si la distance h est choisie avecsoin.

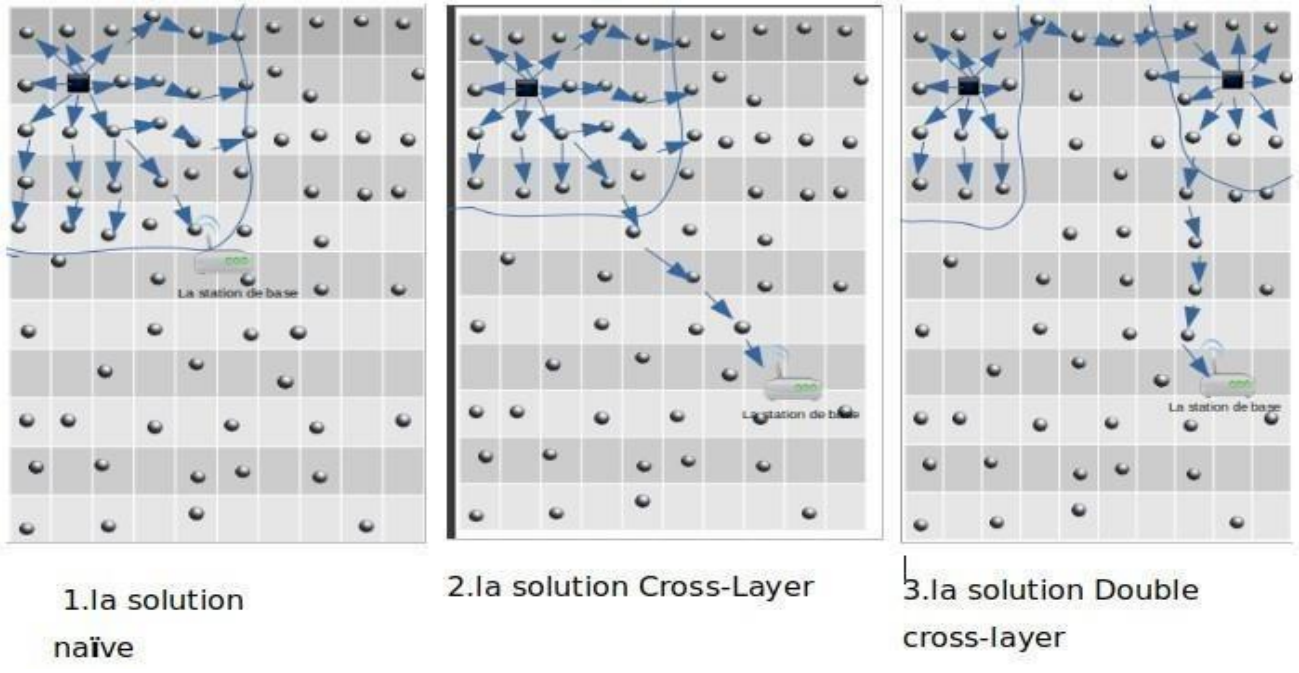


**Figure II.4 1) la solution naïve 2) la solution cross-layer 3) la solution double cross-layer [12]**

- ## Comparaison

Le tableau 2.1 illustre la comparaison des principales techniques de protection de la confidentialité d'emplacement d'un nœud source dans les RCSF, sur les quatre critères de performance suivants : période de sécurité, consommation d'énergie, latence et le type d'adversaire.

**Tableau 2 Comparaison des techniques de protection de la confidentialité d'emplacement d'un nœud source dansles RCSF.**

| Schéma | Période de sécurité | Énergie | Latence | Type d'adversaire |
|---|---|---|---|---|
| Routage Fantôme [5] | Forte | Élevée (M.A : un h élevé augmente la consommation d'énergie sans augmenter la période de sécurité) | Élevée (M.A+ Routage) | Locale |
| CEM [6] | Selon la compétence d'un adversaire | Faible (les boucles sont activées seulementpendant la communication) | Faible (si le plus court chemin est utilisé) | Locale |
| GROW [7] | Forte | Moyenne (M.A d'un seul coté) | Élevée (M.A) | Local |
| PRLA [8] | Similaire au routage fantôme | Inférieur au « routage fantôme » | Similaire au routage fantôme | Local |
| NMR[10] | Forte | Les nœuds en anneau Risquent d'épuiser leurs batteries rapidement | Élevée (M.A) | Globale |
| PFS /TFS [11] | Forte | Élevée (utilise des messages factice) | Élevée (un message est mis en mémoire tampon au niveau de plusieurs proxys) | Globale |
| Cross-layer [12] | Plus la zone de balisage est grande, meilleure est la protection | Faible | Moins la zone de balisage est petite meilleure est la latence | Globale |

## II.3 Conclusion

Dans ce chapitre, on a étudié les différents protocoles de préservation de la confidentialité d'emplacement d'une source dans les RCSF, C'est contre les types d'attaque locale et globale, Où chaque attaque a ses propres protocoles de sécurité. Aussi, on a comparé ces protocoles sur quatre termes importants (période de sécurité, consommation d'énergie, latence et le type d'adversaire). Dans le chapitre suivant, on étudiera les différents protocoles de préservation de la confidentialité d'emplacement d'une station de base et l'identité des nœuds dans les RCSF.

# III Chapitre 3

## Etat de l’art sur la confidentialité d’emplacement d’une station de base et la confidentialité d’identité d’un nœud dans RCSF

# III.1 Confidentialité d'emplacement de la station de base

## • Introduction

La station de base dans les RCSF est un dispositif qui joue un rôle essentiel dans la gestion et la coordination des capteurs déployés dans le réseau. Elle est non seulement chargée de collecter et d'analyser les données, mais également utilisée comme passerelle reliant le RCSF au réseau extérieur sans fil ou filaire. Par conséquent, si un adversaire parvient à l'atteindre, il peut prendre le contrôle du réseau ou même le rendre complètement inutile en le détruisant, ce qui peut entrainer le dysfonctionnement de l'ensemble du réseau. Donc, l'emplacement de la stationde base est indispensable à protéger. Pour cela, nous présentons quelques pertinents protocoles de protection de l'emplacement de la SB parmi ceux proposés dans la littérature.

## • Techniques de préservation de la confidentialité d'emplacement de la station de base

Dans [13] les auteurs ont étudié deux types d'attaques qui peuvent conduire à isoler ou échouer de la station de base. Les premiers types d'attaques pour isoler la SB consiste à bloquer la communication entreles nœuds capteurs et la SB, en utilisant par exemple l'attaque DOS.
Le second type d'attaques pour échouer la SB consiste à utiliser l'analyse de trafic pour découvrir l'emplacement de SB puis la détruire.

Pour contrer ces attaques, deux techniques de sécurité ont été proposées. En premier lieu, utiliser un routage multi-chemins sécurisé vers plusieurs destinations de SB pour fournir la tolérance aux intrusions. En second lieu, plusieurs stratégies pour contrer l'analyse de trafic ont été proposées qui aident à déguiser l'emplacement de SB des écoutes clandestines.

Les auteurs ont introduit une technique pour protéger l'identité et l'emplacement de la SB d'être facilement découvert. Par exemple, si un attaquant est capable d'espionner le trafic de paquets et sait que tous les paquets sont acheminés vers la SB, l'attaquant pourrait suivre les paquets et tracer progressivement le chemin jusqu'à la SB et découvrir ainsi le voisinage de la station de base.

Il existe plusieurs manières pour tracer l'emplacement de la station de base :

- Si un adversaire peut découvrir le contenu d'un paquet en cours de transmission, il pourra corréler ceux qui sont transmis vers la station de base. Cela permet à l'adversaire de suivre la direction de ces paquetsvers le voisinage de la SB, ce qui conduit à la découverte et à la destruction de la SB.
- Si une corrélation temporelle existe entre l'instant de réception et l'instant d'émission d'un paquet par unnœud, un adversaire pourra utiliser cette corrélation temporelle pour trouver la direction vers la SB.
- Si le trafic réseau n'est pas contrôlé, un nœud proche de la SB enverra, en général, des données plus fréquemment qu'un nœud plus éloigné de la SB, car les données s'accumulent au fur et à mesure qu'elles

sont acheminées vers la SB. En surveillant le débit de transmission des données, un adversaire peut suivre la trace des paquets vers l'emplacement de la SB

L'ensemble des contre-mesures de base qui sont proposés pour empêcher un adversaire d'utiliser les techniques d'analyse de trafic citées ci-dessus, pour découvrir l'emplacement de la station de base sous certains communs schémas de transmission de données sont :

✓ ***Cacher l'adresse de destination d'un paquet*** :

Chaque nœud chiffre l'adresse de destination, le type du paquet et le contenu du paquet avecsa clé de son cluster (le réseau est clustérisé). L'identifiant de la source reste en clair afin que le récepteur puisse choisir la bonne clé pour déchiffrer le paquet. Le format d'un paquet est :

$$ID_{src}||E_{KC_{SrC}}(type||ID_{dst}||data)$$

Quand un nœud reçoit un paquet, il vérifie l'$ID_{src}$ pour déterminer la clé du cluster à utiliser pour déchiffrer le paquet. Après avoir déchiffré le paquet, le nœud vérifie s'il est la destination du paquet. De cette manière, l'apparence du paquet est modifiée en chaque saut le long du chemin, ce qui éliminela divulgation de l'emplacement de la station de base.

✓ ***Décorrélation du temps d'envoi d'un paquet***

Le chiffrement d'un paquet peut cacher sa destination, mais ne peut pas cacher son émetteur. En surveillant attentivement le temps d'envoi des paquets de chaque nœud, un adversaire peut obtenir des informations sur les flux de trafic de données. Par exemple, si un nœud parent *s* reçoit un paquet de son nœud enfant (c) et transmet ce paquet immédiatement, un adversaire peut observer le court intervalle de temps entre (s) et (c) et éventuellement déduire la hiérarchie parent-enfant après suffisamment d'observation. Afin de dé-corréler cette relation spécifique, la période de temps *T* est divisée en *m* tranches s'il existe (m-1) nœuds enfants et un nœud parent. Chaque nœud se voit attribuer une tranche et choisit aléatoirement un instant dans sa tranche de temps pour envoyer son paquet.

✓ ***Uniformisation du taux d'envoi de paquets :***

Dans certains cas, les nœuds peuvent avoir des débits différents. Par exemple, si la SB a besoin d'un rapport de topologie, chaque nœud lui transmet des informations de voisinage. Si chaque nœud envoi les paquets avec le même débit alors les nœuds qui sont proche de la station de base doivent non seulement envoyer leur propre donnée, mais également relayer les données de capteurs plus éloignés de la station de base, et présente donc un taux de transmission élevé. En surveillant le débit de transmission des paquets, un adversaire peut facilement trouver la SB. Une technique préservant la confidentialité a été proposée dans [13] qui définit un contrôle d'envoi de paquets entre un nœud parent et ses nœuds-enfants, afin de maintenir le même taux d'envoi sur l'ensemble du réseau de capteurs en contrôlant le retard des données réelles.

Dans [14] les auteurs ont proposé un ensemble de contre-mesures plus avancées pour contrer les attaques d'analyse de trafic qui cherchent l'emplacement d'une station de base, telles que l'introduction de l'aléatoire dans le chemin qu'emprunte un paquet et création de plusieurs zones aléatoires d'activités de communication appelées « hot spots » pour tromper un adversaire de l'emplacement réel station de base.

- **Routage multi-parents (MPR: Multi-Parent Routing**)

Pour réduire la rigidité des chemins prononcés causés par le routage du plus court chemin, chaque nœud qui désire transmettre un paquet, sélectionne au hasard l'un de ses nœuds parents pour router les données vers la station de base. Deux méthodes ont été proposées pour configurer plusieurs parents pour chaque nœud. Dans la première méthode, la station de base met en place une structure de routage en diffusant un message « balise » qui contient un champ de niveau initialisé à zéro. Lorsqu'un nœud transmet un messagebalise, il l'incrémente de 1. Ainsi, la valeur de niveau représente le nombre de sauts qu'un nœud effectue depuis la station de base le long d'un chemin particulier. Un nœud capteur S sélectionne tous les nœuds voisins ayants la valeur de niveau inférieure à cette de S comme ses nœuds parents. Dans la deuxième méthode, un nœud surveille tous les messages balises qu'il reçoit avant de transmettre le premier message balise. Puisqu'un nœud S doit attendre un certain temps avant de transmettre un message balise (attente dansla couche MAC), il sélectionne tous les nœuds dont il reçoit un message balise en attendant de transmettrele premier message balise reçu comme ses nœuds parents (voir la figure III.1.a)

- **Marche aléatoire (**RW: Random Walk**)**

Pour diversifier davantage les chemins de routage et réduire les attaques de surveillance du débit, le routage par marche aléatoire (*RW*) est proposé. Dans *RW*, lorsqu'un nœud reçoit un paquet, il transmet le paquet à l'un de ses nœuds parents avec une probabilité (pr). Cependant, il utilise un algorithme de transfertaléatoire avec probabilité (*1- pr*). Dans l'algorithme de transfert aléatoire, le nœud transmet le paquet à l'unde ses nœuds voisins avec une probabilité égale. (Voir la figure III.1. b). Dans cette méthode, la consommation d'énergie et la latence sont élevées puis certains paquets traversent des chemins longs pourattendre la station de base.

- **Propagation fractale (**FP : fractal propagation**)**

MPR et RW sont toujours vulnérable à l'attaque de corrélation temporelle. Généralement, le nombrede parent est inférieur de moitié aux nombres de voisins, et pour des considérations d'énergie et d'efficacité, $pr > 0{,}5$. Par conséquent, la possibilité qu'un nœud transmet un paquet à son nœud parent est plusélevée qu'il transmet à l'un de ses autres voisins. Un adversaire peut exploiter cette faille pour lancer une attaque de corrélation temporelle, soit en injectant des données de rapport anormales, soit en surveillant sur une longue période.

Pour combler ces défauts, la technique nommée propagation fractale est proposée. Dans cette

technique, plusieurs paquets factices sont créés et propagés dans le réseau pour introduire plus d'aléatoire dans le modèle de communication. Lorsqu'un nœud entend que son nœud voisin transmet un paquet à la station de base, il génère un paquet factice avec probabilité *pc*, et le transmet à l'un de ses nœuds voisins. Pour contrôler la plage de propagation, le paquet factice contient un paramètre initialisé à une constante *k* qui est connue de tous les nœuds. Lorsqu'un nœud reçoit un paquet factice, il décrémente K de 1. Si K supérieur à zéro, le nœud transmet le faux paquet à l'un de ses nœuds voisins, pas nécessairement en direction de la station de base ; sinon le nœud arrête de transmettre le paquet factice. De plus, un nœud quientend que son voisin transmet un faux paquet à un autre nœud ayant un niveau inférieur à K, il génère et transmet un autre paquet factice avec une probabilité **pc** et un niveau (K – 1). Ces faux paquets sont propagésdans le réseau et leurs chemins de transmission forment un arbre (voir figure III.1.c).

• **Propagation fractale différentielle enfoncée** (DEFP : Differential Enfonced Fractal Propagation)

Le problème de la propagation fractale simple est la génération d'un trafic élevé à proximité de la SB. Cela augmente le taux de collision et la perte des paquets. Pour contourner ce problème, un nœud utilise différentes probabilités pour générer les faux paquets. Quand un nœud transmet des paquets plus fréquemment, il utilise une faible probabilité pour créer de nouveaux faux paquets ; et quand le taux de transmission d'un nœud est plus élevé, le nœud génère des faux paquets avec une probabilité élevée.Cette technique est appelée propagation fractale différentielle (DFP). Pour compliquer encore la tâche d'un adversaire, des zones locales de haut débit sont créés dans le réseau qui sont appelées « hot spot ». Un adversaire peut être piégé dans ces zones et ne pourra pas déterminer le bon chemin vers la station de base. Il est facile de détruire un *hot spot* et d'en construire un autre à un endroit différent quand les nœuds reçoivent un message de diffusion de la station de base. Un adversaire peut rester en attente au niveau d'un hot spot jusqu'à ce que le modèle de communication change pour se rendre compte qu'il estd'un point chaud. Cette longue attente permet d'augmenter le délai pour trouver l'emplacement de la SB

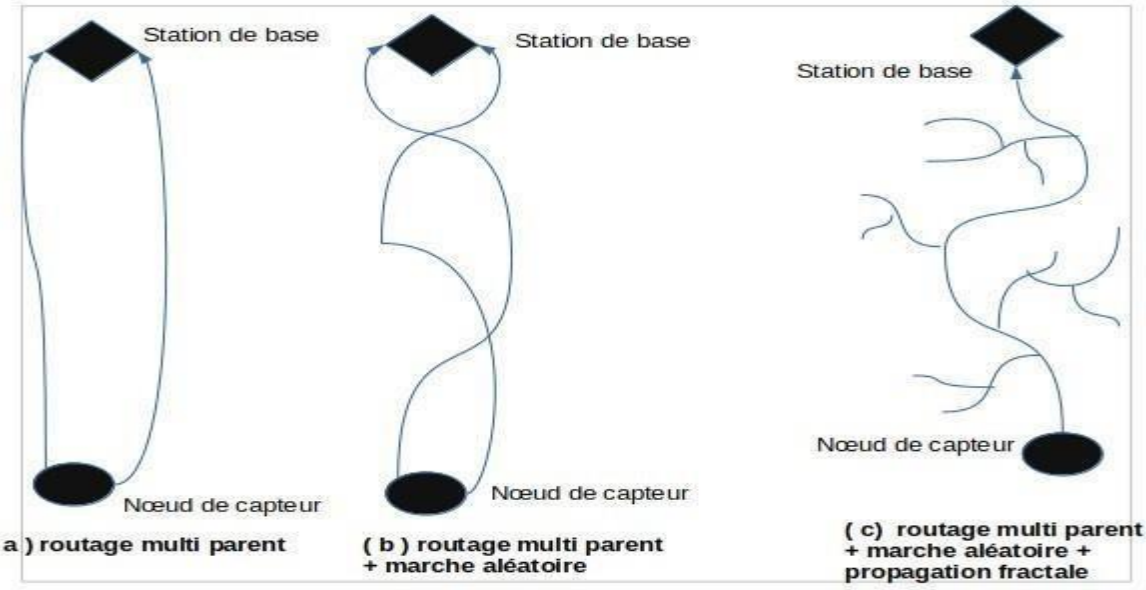


**Figure III.1 Techniques pour contrer l'analyse du trafic [14]**

Les auteurs ont proposé dans [15] une solution pour assurer la confidentialité d'emplacement d'unnœud récepteur SB contre l'attaque de traçage de paquets. La solution consiste en deux étapes : d'abord, Ils ont conçu un nouveau protocole de routage nommé LPR [15] pour fournir la diversité de chemin, puis ceprotocole de routage est combiné avec l'injection de paquets factice pour minimiser les informations qu'unadversaire peut déduire des paquets entendus en direction vers la station de base.

LPR utilise le routage aléatoire afin que la direction de transfert des paquets ne soit pas toujours versla SB. Ainsi, un adversaire est obligé d'effectuer plus de sauts avant d'atteindre la SB, car il est souvent conduit vers de mauvaises directions. De plus, des faux paquets sont ajoutés pour LPR de sorte que la probabilité de transmettre un paquet pour n'importe quel voisin soit égale, ce qui rend inutile d'entendre lespaquets pour un adversaire. Les détaille du protocole LPR sont :

Chaque nœud capteur divise ses nœuds voisins en deux listes : la *liste-proche* qui consiste en nœuds qui sont poche du récepteur, et la *liste-loin* qui consiste en voisins qui sont loin (ou à une distance égale aurécepteur). Une fois que les deux listes sont construites, LPR fonctionne comme suit :

Quand un nœud transmet des paquets, si le saut suivant est choisi aléatoire alors la longueur du chemindes paquets d'un même nœud n'est pas fixe. Ainsi, si les paquets sont routés par des nœuds choisi principalement de la liste-proche (resp. Liste-loin) alors la consommation en énergie sera faible (resp. élevée) ; mais la confidentialité de l'emplacement du récepteur sera faible (resp. forte). Dans LPR, chaquefois qu'un capteur transmet un paquet, il sélectionne le prochain saut depuis la *liste-loin* avec une probabilité *pf*, et depuis la liste-proche avec une probabilité $1 - pf$, où *pf* est un paramètre système. En ajustant la valeur de pf, on peut trouver un compromis entre la confidentialité de l'emplacement et l'efficacité énergétique.

Si LPR est applique seul, la confidentialité d'emplacement ne sera pas assez forte, car la tendance globale du trafic dans le réseau pointe toujours vers le récepteur. Ce problème peut être minimisé en définissant une valeur plus élevée pour *pf*, mais cela conduit à un long délai de livraison des paquets et un coût d'énergie élevé. Pour remédier à cette faiblesse, un mécanisme supplémentaire est introduit pour éliminer la tendance du trafic, en injectant un faux trafic dans la direction opposée du récepteur. Cela consiste à transmettre un faux paquet à un nœud voisin qui est choisi au hasard de la liste loin, chaque foisque le nœud transmet un vrai paquet au saut suivant. Un adversaire peut être attiré par ce faux paquet et tracer dans la mauvaise direction au lieu du vrai saut suivant. Chaque paquet factice a un paramètre $TTL_{fake}$ spécifiant le nombre maximum de sauts qu'il sera transmis loin du récepteur. Il est à souligner que $TTL_{fake}$ doit être initialisé au moins à 2 sauts pour que le nœud du prochain saut transmette un faux paquetpour que cela ne soit pas détecté par un adversaire.

Quand un nœud reçoit un faux paquet il effectue ce qui suit :

1 Le nœud décrémente de 1 le champ TTL qui est initialisé à $TTL_{fake}$.

2 Si le champ TTL est positif, le nœud choisit aléatoirement un voisin depuis la liste-loin et lui

transmet le faux paquet.

3 Si le champ TTL est zéro, le nœud écarte le faux paquet.

L'injection d'un faux trafic peut réellement améliorer la confidentialité de l'emplacement du récepteur. Néanmoins, son coût est également élevé. Afin de contrôler le compromis entre la consommationd'énergie et la force de protection, un autre paramètre système $P_{fake}$ est utilisé pour spécifier la probabilitéavec laquelle un nœud génère un paquet factice quand il transmet un vrai paquet. Plus la valeur de $P_{fake}$ estélevée, plus le nombre de faux paquets générés est élevé, et plus l'énergie consommée est élevée.

Lorsque la LPR est combinée avec l'injection de faux paquets, si les paramètres système ($pf, TTL_{fake}$ et $P_{fake}$) sont correctement définis, il est alors très difficile pour un adversaire d'effectuer l'analyse de traficbasée sur des informations collectées localement pour déduire la direction vers le récepteur.

Les auteurs ont proposé dans [16] un schéma de collecte de données aléatoire pour préserver la confidentialité d'emplacement de la station de base, qui consiste en deux phases :

- **Phase de transfert et stockage de données aléatoires :** lorsqu'un nœud capteur rapporte un message à la SB, il Le chiffre le message par sa clé symétrique Ki et le transmet en utilisant un chemin aléatoire. Contrairement à d'autres algorithmes de routage, le paquet n'inclut pas l'emplacement ou l'identifiant de la SB lors de la transmission des données. Cette approche permet d'empêcher les attaquants de découvrir la destination du paquet même s'ils entendent par hasard des messages sur des nœuds intermédiaires.
- **Phase de mouvement aléatoire des SB pour la collecte de données :** la SB mobile parcourt le réseau Pour Collecter les données des capteurs. Pour éviter d'être suivie et attaquée, elle change de direction au hasard et demande occasionnellement des données à ses voisins locaux. A chaque diffusion, la SB collecte toutes les données depuis du tampon de chacun de ses nœuds voisins, puis filtre les données qui ont été déjà reçues. Seules les données reçues pour la première fois seront enregistréeset communiquées aux utilisateurs. Les nœuds voisins libéreront leur tampon après avoir reporté toutes leurs données à la SB.

Le tableau 3 ci-dessous résume la comparaison des méthodes de protection de la confidentialité de l'emplacement de la station de base, en termes de période de sécurité, énergie et latence.

**Tableau 3 Comparaison des techniques de protection de la confidentialité d'emplacement d'une station de basedans les RCSF**

| Schéma | Période de sécurité | Energie | Latence |
|---|---|---|---|
| MPR [14] | Faible | Faible | Faible |
| Marche aléatoire [14] | Faible | Elevée (marche aléatoire) | Elevée (marche aléatoire) |
| Propagation fractale (PF) [14] | Moyenne | Moyenne (dû au faux trafic) | Elevée (marche aléatoire) |
| DEFP [14] | Forte | Élevée (dû au faux trafic +zone chaude) | Élevée (marche aléatoire) |
| LPR [15] | Forte | Moyenne (dû au faux trafic) | Faible |
| Schéma de collecte de donné aléatoire [16] | Forte | Élevée | Dépend de la distance si la distance est grande donc latence sera élevée |

## III.2 Confidentialité de l'identité des nœuds

- **Introduction**

Dans une communication, les identifiants d'une source et d'une destination sont transmet en claire pour permettre aux nœuds intermédiaires d'effectuer le routage. Un adversaire peut élaborer une correspondance entre les nœuds du réseau et leur emplacement dans le champ après un nombre d'observations. Pour protégerl'identifiant réel de chaque capteur, des pseudonymes peuvent être utilisés pour les nœuds de capteurs au lieudes identifiants réels. Cependant, l'utilisation de pseudonymes fixes ne peut pas empêcher la fuite d'informations d'identité des nœuds de capteurs, car une écoute passive à long terme peut déduire la topologiedu réseau par l'analyse du trafic. Un pseudonyme est un nom ou un identifiant qui peut être utilisé à la place d'un vrai nom.

- **Protocoles pour protéger l'identité d'un nœud capteur**

Le protocole SAS (Simple Anonymity Scheme) est le premier schéma fourni pour protéger l'identité d'un nœud [17]. Il consiste en un espace de pseudonymes (pool) à l'échelle du réseau qui utilise k bit pour tous les nœuds. Par conséquent, l'espace total de pseudonymes de $2^k$. La station de base divise l'espacedes pseudonymes uniformément en sous-ensembles de taille $2^m$ et attribue pour chaque nœud N sous- ensemble choisies au hasard de l'espace des pseudonymes pour communiquer avec ses voisins. La valeur de m est choisie de manière à ce que l'espace des pseudonymes puisse être divisé au moins en $N^2$ sous- ensembles. Ce sous-ensemble de pseudonymes pour chaque voisin est contigu. La SB crée une table pour stocker les plages de pseudonymes de chaque nœud. Cela assure à la SB quand elle reçoit un message d'un nœud, elle est capable de déterminer la bonne clé pour déchiffrer et authentifier un message. Pour identifier émetteur, chaque nœud construit une table de pseudonymes dans

laquelle il stocke les plages de pseudonymes pour communiquer avec chaque nœud dans son voisinage. La table lie les pseudonymesdes messages entrants et sortants pour chaque voisin et leurs clés secrètes correspondantes partagées entre eux.

Lorsqu'un nœud veut envoyer un message à un voisin spécifique, il choisit au hasard un pseudonymedepuis la plage de pseudonymes qu'il partage avec ce voisin et le concatène avec l'index de la ligne à partirde laquelle il a choisi le pseudonyme. Quand le nœud destinataire reçoit le message, il vérifie si le pseudonyme reçu appartient à la plage de pseudonymes entrant correspondant à l'index donné et, si tel est le cas, il utilise la clé secrète partagée pour déchiffrer le message. Le principal inconvénient de cette approche est la quantité de mémoire nécessaire pour stocker l'espace complet des pseudonymes, qui doit être suffisamment long pour éviter les répétitions.

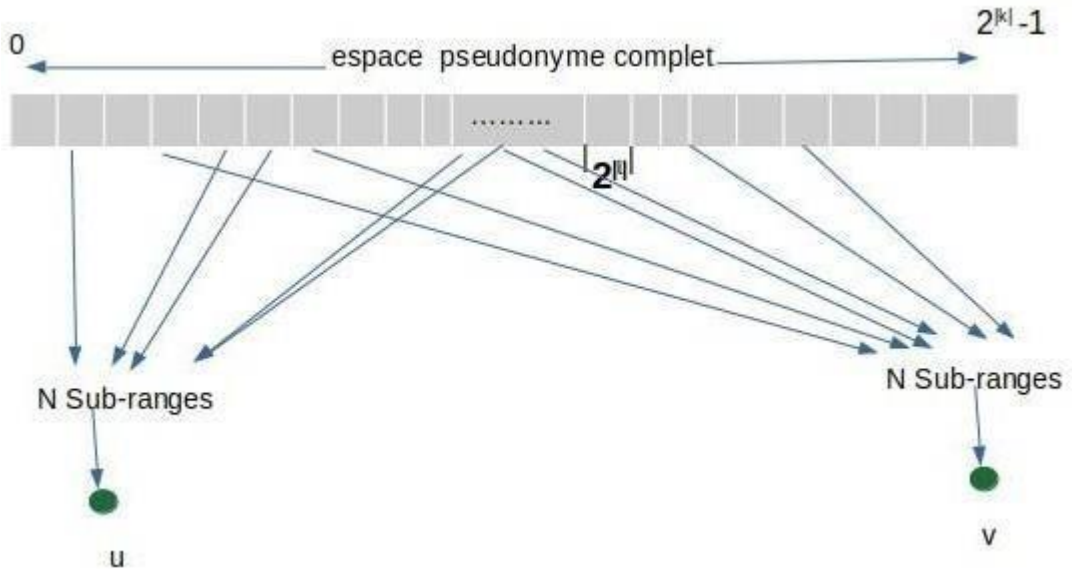


**Figure III.2 Attribution d'espace d'identification de pseudonymes[17]**

Afin de réduire la quantité importante de mémoire nécessaire dans SAS, le schéma CAS (Cryptographic Anonymity Scheme) est proposé [17]. Ce schéma utilise une fonction de hachage à clé pour générer les pseudonymes. Avant le déploiement du réseau, chaque nœud est lui attribué les paramètres nécessaires pour communiquer anonymement avec la station de base. Ces paramètres sont : une fonction pseudo-aléatoire, une clé secrète et un nonce aléatoire partagé avec la station de base. Dans la phase de déploiement, pour qu'un nœud communique anonymement avec son voisin, la paire de nœuds nécessite departager les trois paramètres suivants : une clé de hachage, un nonce aléatoire, un numéro de séquence qui est initialisé à 1. Chaque nœud partage également quatre paramètres avec tous ses voisins, pour une communication anonyme dans le cluster lorsqu'il agit comme un cluster-Head. Ces paramètres sont : clé dehachage, deux nonces et un numéro de séquence.

Pour chaque nœud v dans son voisinage qui a un identifiant inférieur à lui-même, le nœud u génère les informations nécessaires à la communication anonyme et les stocke dans une table de pseudonymes. De plus, u communique en toute sécurité ces informations pour une communication

anonyme mutuelle à chaque voisin v, ainsi que les informations pour v pour déchiffrer la communication du cluster lorsque u est le cluster-Head. Dans le même message, u envoie également l'index dans la table des pseudonymes où il stocke ces informations. Le nœud capteur v répond en envoyant un message à u contenant les informations nécessaires à u pour déchiffrer les messages de cluster anonymes envoyés par v en tant que cluster-Head, ainsi que l'index dans la table des pseudonymes où il stocke toutes les informations correspondant à u. La figure III.3 illustre les messages communiqués entre u et v.

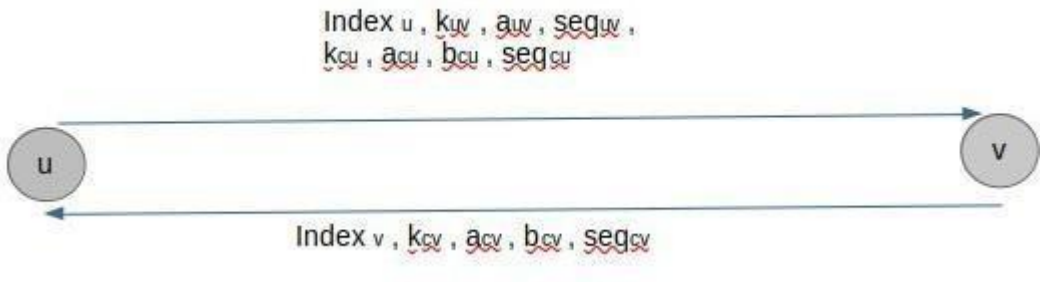


**Figure III.3 Échanges de messages de phase de configuration entre u et v[17]**

Après l'échange mutuel sécurisé des informations nécessaires à la configuration, les entrées de la table de pseudonymes de chaque nœud u stockent les informations nécessaires à la communication mutuelle et à la communication intra-cluster, avec chacun de ses voisins. u stocke dans la table des pseudonymes également les index de ses voisins où sont stockées ses informations. De plus, u supprime le vrai identifiant ID des voisins ainsi que la fonction pseudo-aléatoire qu'il a utilisée pour générer les clés duhachage.

Chaque fois qu'un nœud désire envoyer des données à la station de base, en utilisant un voisin comme intermédiaire, il crée un message M qui est composé de : $sID \,||\, rID||$Charge utile chiffrée||seq, où sID et rID sont les pseudonymes générés après avoir appliqué les fonctions de hachage à clé à la nonce aléatoire et au numéro de séquence partagé avec la station de base et le nœud l'intermédiaire, respectivement.

Lorsque v reçoit le message de u, il utilise l'Index dans le message pour indexer sa table de pseudonymes et obtenir les valeurs de la clé secrète et le nonce. En utilisant les valeurs obtenues et le numéro de séquence, il construit $rID'$. Si $rID' = rID$, alors v a vérifié l'expéditeur et peut utiliser la clé secrète correspondante pour déchiffrer la charge utile, sinon il détruit le message. A la fin de cette procédure, le nœud v incrémente le numéro de séquence de 1 si le paquet reçu est vérifié. L'inconvénient dece schéma est la surcharge de calcul au niveau de tout voisin recevant le paquet qui doit calculer une valeurhachage de clé avant de découvrir que le paquet n'est pas lui adressé.

Afin de réduire le risque d'attaques de compromission de nœuds existant dans le schéma CAS, deux méthodes basées sur des chaînes de hachage à clé ont été proposées dans [18], pour produire une séquence de valeurs de hachage comme identifiants pour un nœud. Dans le schéma HIR (Hashing-based

*ID* Randomisation), chaque nœud partage avec ses voisins une clé secrète qui est utilisé pour générer un nouveau pseudonyme pour chaque message en hachant le pseudonyme résultant de l'application de la fonction de hachage à clé au vrai identifiant du nœud. Cela rend difficile pour un adversaire d'obtenir les anciens pseudonymes. Le protocole en détaille est comme suit :

Dans la phase de déploiement, un nœud capteur se localise et signale son emplacement à la station de base en envoyant un message contenant son identifiant et ses coordonnées. La station de base ajoute ces informations dans une table qui fait la correspondance entre les identifiants et les emplacements réels correspondants. Chaque nœud détermine aussi les nœuds voisins ayants les liaisons sortantes et entrantes. Par nœud de liaison sortante « B » du nœud « A » on entend que B est sélectionné de manière qu'il soit plus proche de la station de base que A. Inversement, Le nœud A est le nœud de liaison entrante du nœud B.

Initialement, un nœud $S_i$ diffuse un message à ces voisins avec son identifiant $ID_i$ et le nœud $S_j$ renvoie un message ACK avec son identifiant $ID_j$. Les nœuds *Si* et *Sj* calculent leur clé secrète et le nœud Sidécide si *Sj* est un nœud de liaison sortante ou entrante, et crée une table de routage $R_i$ qui comprend les valeurs de hachage des clés des identifiants des nœuds voisins. Un exemple de table de routage R est présenté dans la table 5 pour le nœud A de la figure III.4.

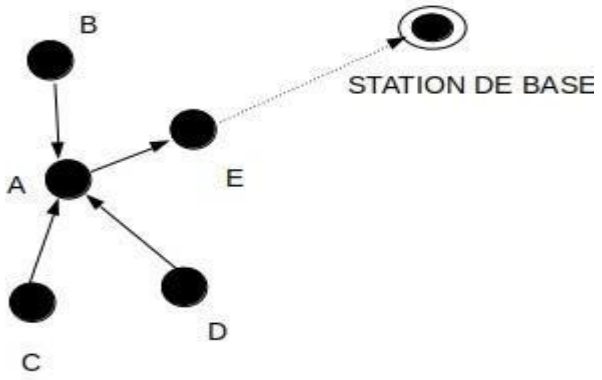


Figure III.4 **Exemple de nœud A créant la table R [18]**

**Tableau 4 Un exemple de Tableau R**

| Temps de hachage (HT) | Valeurs de hachage (HV) | Lien |
|---|---|---|
| 1 | $HK\ AB\ (ID\ A)$ | down |
| 2 | $H^2\ (ID_{KAC}\ A)$ | down |
| 4 | $H^4\ (ID_{KAD}\ A)$ | down |
| 2 | $H^2\ (ID_{KAE}\ E)$ | up |

Après la phase de déploiement, les messages envoyés par un nœud sont de la forme : $M = H1||H2||J||D$, où « || » indique la concaténation, $H1 = (H^{t}{}_{Kij}(IDi)$ est une valeur de hachage qui identifie le destinataire du message, $H2 = (H^{t}\ (IDi)$ est une valeur de hachage qui identifie l'expéditeur du message d'origine, J est un index qui indique quelle valeur de hachage de H2 est utilisée, et D est un bloc de données collecté par l'expéditeur. Un nœud possède un compteur t pour compter le nombre de messages qu'il a envoyés à la station de base ; c'est également le nombre de fois où le nœud a haché son *ID* d'origine.

Pour protéger l'identifiant du récepteur, le champ valeur de hachage *HV* est utilisé pour notifier le récepteur réel. Si le nœud récepteur $S_j$ trouve une correspondance dans la table de routage et que le messageprovient d'un nœud de liaison entrante, le nœud $S_j$ sait que ce message est lui destiné et doit être transmis à la station de base ; sinon, il supprime le message. Pour maintenir sa table de routage, chaque nœud mettra àjour ses entrées après chaque utilisation.

Quand la station de base reçoit un message, elle peut facilement l'identifier l'émetteur en appliquant *t* fois le hachage à clé aux identifiants de tous les nœuds quelle possède pour interpréter correctement le champ *H2* (hachage à clé appliqué t fois au nœud i).

Le schéma RHIR (Reverse Hashing ID Randomisation) utilise les mêmes opérations que le schémaHIR. Dans cette technique, un nœud utilise cette chaîne de hachage dans l'ordre inverse. Ainsi, un nœudest lui attribué un en arrière, depuis la fin de la chaîne de hachage jusqu'au début.

Ce changement améliore la sécurité de la méthode, mais consomme beaucoup de mémoire.

## III.3 Conclusion

Dans ce chapitre, on a analysé divers protocoles pour protéger l'emplacement de la station de base et la confidentialité des nœuds dans RCSF. Aussi, avec cette explication, On a pu identifier les avantages et les inconvénients de chaque protocole, et ceci grâce à la comparaison qui on a faite entre chaque protocole en termes de période de sécurité, la consommation d'énergie et latence. Dans le chapitre suivant, on proposera une solution pour protéger la station de base dans RCSF.

# IV Chapitre 4

## Proposition d’une solution pour protéger l’emplacement d’une station de base dans les RCSF

# IV.1 Introduction

Dans le chapitre président divers protocole de protection la confidentialité d'emplacement des nœuds source et la station de base dans RCSF ont été expliqués. Dans ce chapitre, une proposition développée sera présentée pour protéger la confidentialité de la station de base, c'estce qu'on appelle mobilité des nœuds.

Afin de protéger l'emplacement de la station de base, notre idée consiste à générer des messages factices pour cacher le vrai message. Notre solution suppose un réseau de capteurs mobiles.

Les nœuds mobiles dans les réseaux de capteurs sans fil sont des entités qui peuvent se déplacer à l'intérieur du réseau de capteurs. Contrairement aux nœuds statiques, qui sont généralement immobiles, les nœuds mobiles peuvent changer de position, ce qui peut avoir un impact significatif sur le fonctionnement et les performances du réseau. Les nœuds mobiles peuvent être utilisés dans différentes applications des réseauxde capteurs sans fil, notamment la collecte de données, la surveillance de l'environnement et le routage adaptatif.

# IV.2 Fonctionnement de l'algorithme

Quand un nœud source désire communiquer des données à une station de base, le protocole agit comme suit : Initialement, chaque nœud divise ses voisins en deux listes : la liste_proche qui contient les nœuds voisins ayant la distance, en termes de sauts, à la station de base inférieur ou égale à sa distance) et la liste_loin qui contient les autres nœuds.

* Lorsqu'un nœud source (initial) à un paquet à transmettre ou un nœud intermédiaire reçoit un paquet, d'abord, il déplace directement à un de ces voisins choisis aléatoirement parmi la liste_proche.
* À ce stade, le nœud source et le nœud mobile se trouvent à proximité les uns des autres. Ces deux nœuds se synchronisent pour transmettre simultanément deux paquets (vrais et faux paquets) vers son voisin. Le nœud ayant le vrai paquet le transmet à un de ces voisins qui est choisi de la liste_proche (le plus court chemin), puisque le vrai paquet contient la vraie destination qui est la station de base. Le nœud mobile génère un paquet factice avec une probabilité *P* et le transmet à un de ces voisins choisit de la liste_loin,
* Pour Contrôler la plage de propagation, chaque nouveau paquet factice généré contient un paramètre « *L* » fixé à une constante *K* connue de tous les nœuds. Quand un nœud reçoit un faux paquet, il décrémente *K* de 1. Si « *K* » est supérieur à zéro, le nœud retransmet le paquet en suivant les étapes 1) et 2), sinon si «*K* » est égale zéro, le nœud arrête de transmettre un faux paquet.
* Le champ de capteurs est constitué de faux paquets qui se dirigent dans la direction qui les éloignentde la station de base et le vrai paquet qui se dirige dans la direction vers la station de base.
* Un nœud mobile intermédiaire recevant un paquet (vrai ou factice) se comporte comme une source. Il déplace vers un nœud voisin et transmet le paquet vers un voisin choisit la liste_proche.

***** Les opérations se poursuivent en répétant les étapes 1), 2) et 3) jusqu'à ce que le vrai paquet arrive à la station de base, tandis que la transmission d'un paquet factice s'arrête quand *K* atteint 0.

En suivant ce processus, les paquets sont transmis de manière efficace dans le système, en utilisant à la fois des signaux pour guider les nœuds mobiles et des protocoles de routage le plus court chemin pour minimiser la latence. La figure IV.1 ci-dessous montre le fonctionnement de notre algorithme.

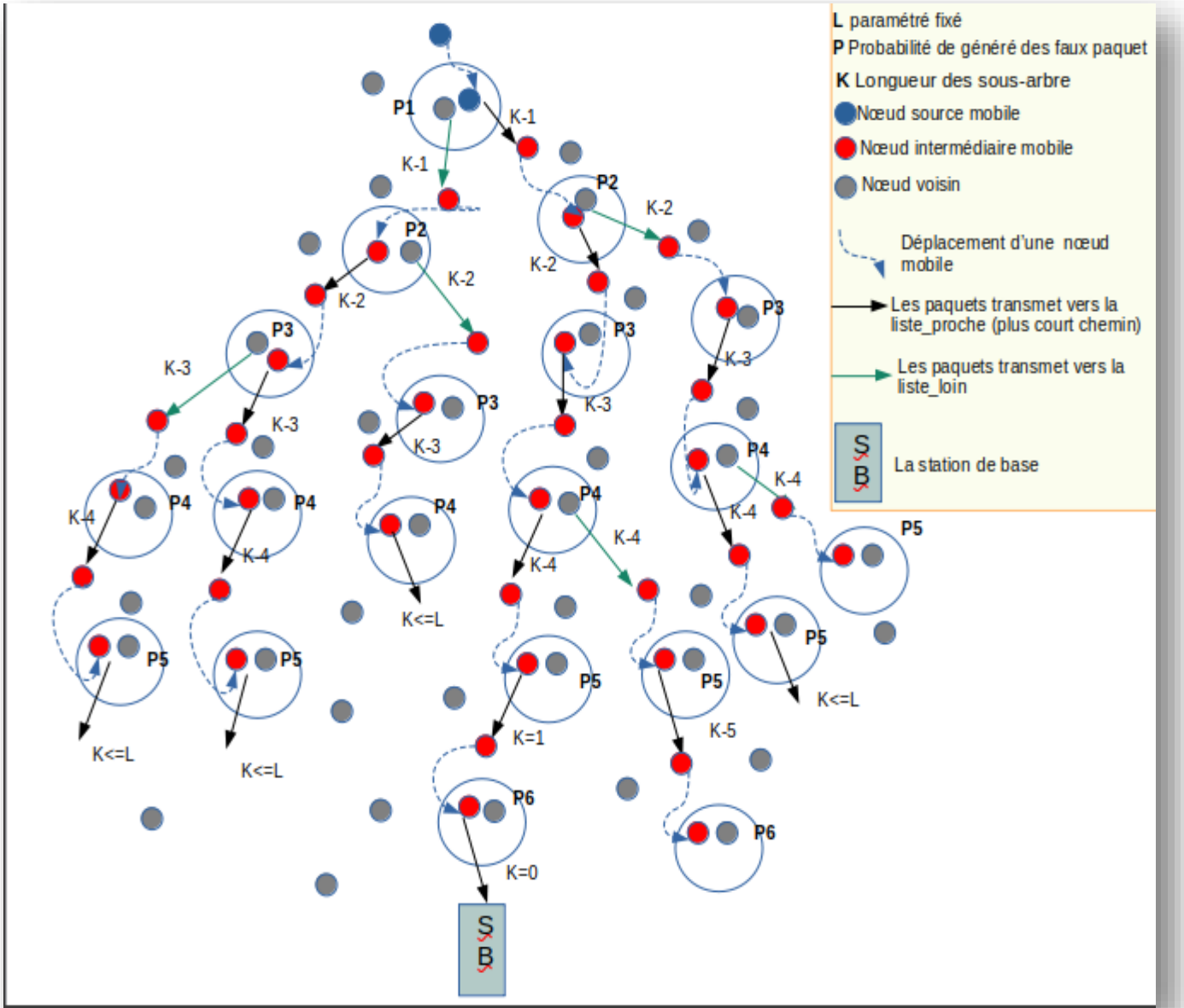


**Figure IV.1 Schéma explique le protocole de nœud mobiles collecte des faux paquets.**

## IV.3 La formule d'évaluation période de sécurité

Un adversaire qui désire atteindre l'emplacement de la station de base, tente de tracer (suivre) les paquets transmis depuis le nœud source. Les paquets factices propagés dans le réseau permettent d'éloigner l'adversaire de la station de base. Leur transmission forme des sous-arbres de paquets factices.

Soit f(*k*) la taille du sous-arbre généré à un nœud quelconque sur le chemin de routage des données. Sila probabilité *P* de générer un paquet factice est nulle, c'est-à-dire, alors les transitions forment un sous- arbre dégénéré de taille *K* sauts. Si la probabilité *P* de générer un paquet factice est égale à 1, c'est-à-dire, chaque nœud d'un sous arbre transmet le paquet reçu et le nœud mobile qui est à sa proximité génère et transmet un paquet factice ; et les transmissions forment un sous arbre complet et sa taille est ($2^{k+1}$-1). Si la probabilité de générer un paquet factice est entre 0 <*P* < 1 alors les transmissions forment un sous-arbre et sa taille est donné par l'équation récursive suivante [14] :

$$(k) = p * (k-1) + (k-1) + 1 \qquad (1)$$

Où 1 compte la transmission en cours, *f* (*k-1*) le sous-arbre du sous-arbre en cours à générer si (k > 0) et *P* f* (*k-1*) le sous-arbre du sous-arbre en cours à générer si (P > 0) et (k > 0).

La résolution de cette équation, donne [14] :

$$f(k) = \sum_{i=0}^{i=k-1} (p+1)^i \qquad (2)$$

$$f(K) = \begin{cases} [(P+1)^K - 1]/P & si\ P > 0 \\ K & sinon \end{cases} \qquad (3)$$

On sait que la distance entre un nœud source et la station de base est égale ***n*** et chaque nœud du chemin de routage des données génère un paquet factice avec une probabilité *P*. Ainsi, la taille totale T des sous- arbres générés par tous les nœuds sur le chemin de routage depuis le nœud source vers la station de baseest égale à la somme des tailles de tous les sous-arbres générés en chaque nœud par la probabilité *P* que le nœud génère un sous arbre. Si la distance entre un nœud source et la station de base est n alors on obtient :

$$T = \sum_{J=1}^{j=n-1} P * (k) \qquad (4)$$

$$T = \begin{cases} \sum_{j=1}^{j=n-1}((p+1)^k - 1) & si\ p > 0 \\ n & sinon \end{cases} \quad (5)$$

La période de sécurité ρ est mesurée comme étant le nombre de saut nécessaires pour atteindre la station de base depuis la source. Ainsi, le nombre de saut entre la source et la station de base est égal à la somme de tous les sauts générés par paquets factices, donnés par la formule mathématique (3) et les paquets de données qui est égale à ***n***. Donc, on obtient ρ comme suit :

$$\rho = \begin{cases} n + \sum_{j=1}^{j=n-1}((p+1)^k - 1) & si\ p > 0 \\ n & sinon \end{cases} \quad (6)$$

## IV.4 Algorithme pour la proposition

**Début**

Lire(L); /* paramètre fixé */

Lire(K); /**constante Connue par tous les nœuds* */

**Si** (K> 0) alors /* le paquet n'a pas encore atteint la station de base*/

K := K – 1 ;

-le nœud Source déplace vers le nœud voisin

**Fonction** Nœud voisin Envoyé Paquet Avec Probabilité ()

P:Random ; /* *Générer un nombre aléatoire entre 0 et 1 pour la probabilité de transmission d'un faux paquet**/

si (p >= Q) **Alors** /* *Q est un paramètre qui mesure le degré de génération de faux paquets désiré par l'utilisateur* */

-le nœud source envoyé un vrai paquet

-le nœud voisin envoyé le faux paquet

**Fonction** Envoyer paquet vers nœud voisin aléatoire ():

Nœud Destinataire: Sélectionner Nœud Voisin Aléatoire ()

Envoyer Paquet (Nœud Destinataire)

**Fonction** Attente Traitement Nœud ():

**Si** (K<=L) **Alors:**

-Terminer le traitement d'un paquet () :

**Sinon:**

P:Random ()

**Si** (P<= Probabilité Transmission) **Alors:**

Envoyer un paquet vers un nœud voisin aléatoire.

**Fin Si**

**Fonction** Terminer Traitement Paquet ():

Envoyer Paquet Vers Station de base() ;

## IV.5 Conclusion

Dans ce chapitre on a expliqué le protocole de nœud mobile en ce qui concerne sa fonctionnalité. Ona déduit une formule sur la façon de déplacement des nœuds mobile et comment on transmet des paquets factices dans le champ de capteurs entre les nœuds voisins, et la façon d'envoyer le vrai paquet vers la station de base. Dans le chapitre suivant, on passe à la simulation de notre proposition.

# V Chapitre 5
# Analyse des performances

# V.1 Introduction

Après avoir mis en œuvre notre méthode de nœud mobile, on a passé à la simulation de notre proposition afin d'évaluer ces performances en termes de période de sécurité ρ de la station de base.

On vise par la simulation à extraire et analyser les différents résultats qu'on peut obtenir à l'aide de l'équation estimant la période de sécurité, déduite de notre proposition, qui consiste à générer un faux trafic quand une source transmet des données à la station de base. On a calculé la période de sécurité ρ en fonction de la profondeur *K* des sous-arbres générés par les nœuds recevant un vrai paquet, de la probabilité que ce nœud génère un paquet factice *P* et de la distance ***n*** entre la source et la station de base.

# V.2 Environnement de simulation

- **Simulateur MATLAB**

Dans cette section, on a décrit l'environnement de simulation et les configurations du protocole utilisé pour générer les résultats. On a utilisé un environnement de simulation MATLAB (version 9.14.0.2206163 (R2023a)). MATLAB est un langage de programmation largement utilisé par des millions d'ingénieurs et de scientifiques du monde entier. C'est un outil essentiel pour les professionnels qui souhaitent analyser et concevoir des systèmes.

Le langage MATLAB se base sur des matrices, ce qui offre une méthode naturelle pour exprimer des complexes mathématiques de calcul. Il fournit également des graphiques intégrés pour faciliter la visualisation et l'interprétation des données. Dans notre simulation, nous avons utilisé MATLAB pour évaluer les performances de notre solution.

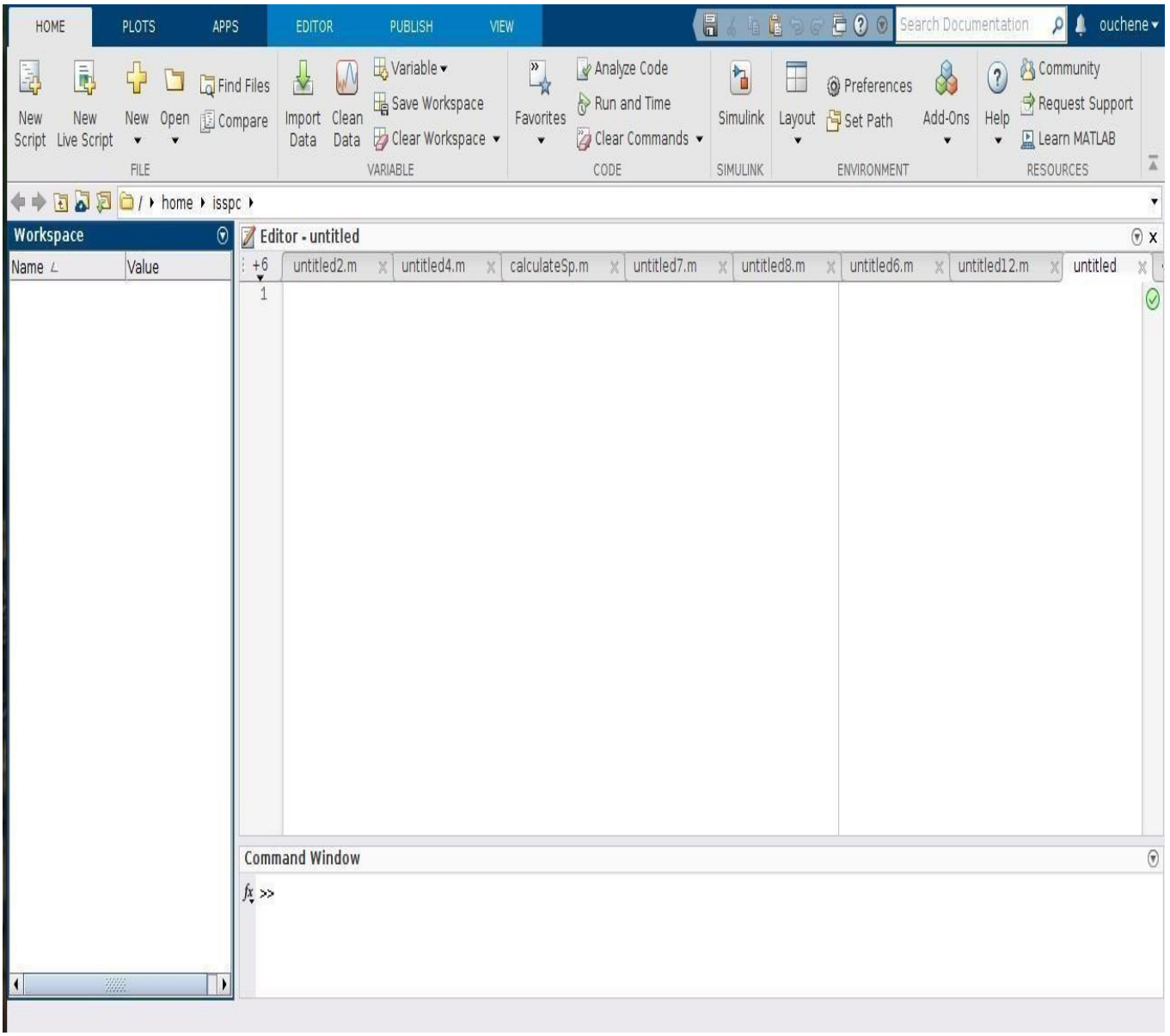


**Figure V.1 Une interface de MATLAB**

## V.3 Validation de notre proposition par le simulateur MATLAB

À ce stade, On a parlé sur les résultats de simulation et cela pour notre programme (la sécurité avec les nœuds mobile). On a utilisé logiciel MATLAB pour calculer la période de sécurité après avoir transmet et généré des paquets factices dans le champ des capteurs. Ainsi, pour tracer un graphe de la période de sécurité en fonction de la probabilité de création du paquet factice *P*, la profondeur *K* des sous-arbres générés par le nœud source et de la distance ***n*** entre la source est la station de base ; on a utilisé la formule suivante :

$$\rho = \begin{cases} n + \sum_{j=1}^{j=n-1} ((p+1)^k - 1) & si\ p > 0 \\ n & sinon \end{cases} \qquad (6)$$

## V.4 Évaluation et analyse des performances

L'évaluation de notre proposition «la sécurité par la mobilité des nœuds » sous différents paramètres est comme suit :

- **Période de sécurité ρ en fonction de la profondeur *k***

On fixe la probabilité de génération de faux paquets ***p*** à [0.1, 0.5, 0.9] et la distance ***n*** à100 et on varie ***k***, on obtient la figure V.2 ci-dessous :

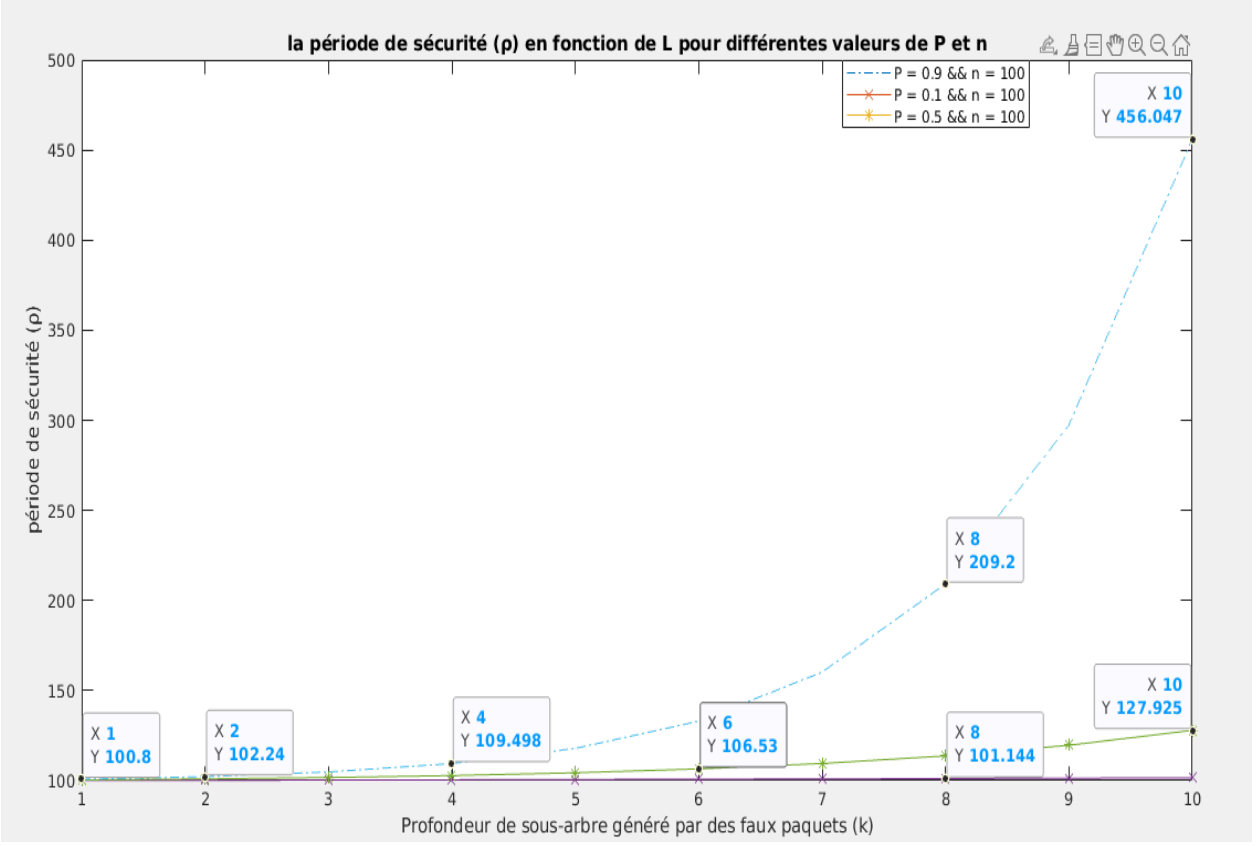


**Figure V.2 Période de sécurité ρ en fonction de la profondeur *k***

La figure V.2 montre que, plus la profondeur *k* est grande plus la période de sécurité ρ augmente (on a mesuré la période de sécurité ρ par les nombre des sauts). On constate que l'augmentation n'est pas linéaire ; cela signifie que certains sous arbres ne sont pas dégénérés. Par exemple, sur la courbe correspondante à la probabilité $P = 0.9$; quand on fixe $k = 4$, la période de sécurité ρ = 109.498, et quand on fixe $k = 10$ (donc k = L, telles que L'est un paramètre fixé), la période de sécurité ρ =456.047. On constate aussi que pour des valeurs de *k* très petit, la période de sécurité est très faible. Exemple, pour k ϵ [0..5], ρ s'approche de la distance *n* qui est la valeur minimale.

- **Période de sécurité ρ en fonction de la probabilité *P* de la génération des paquets factices**

On fixe la profondeur *K* à [1, 5, 10] et la distance ***n*** à 100 et on varie *P*, on obtient la figure V.3 ci-dessous :

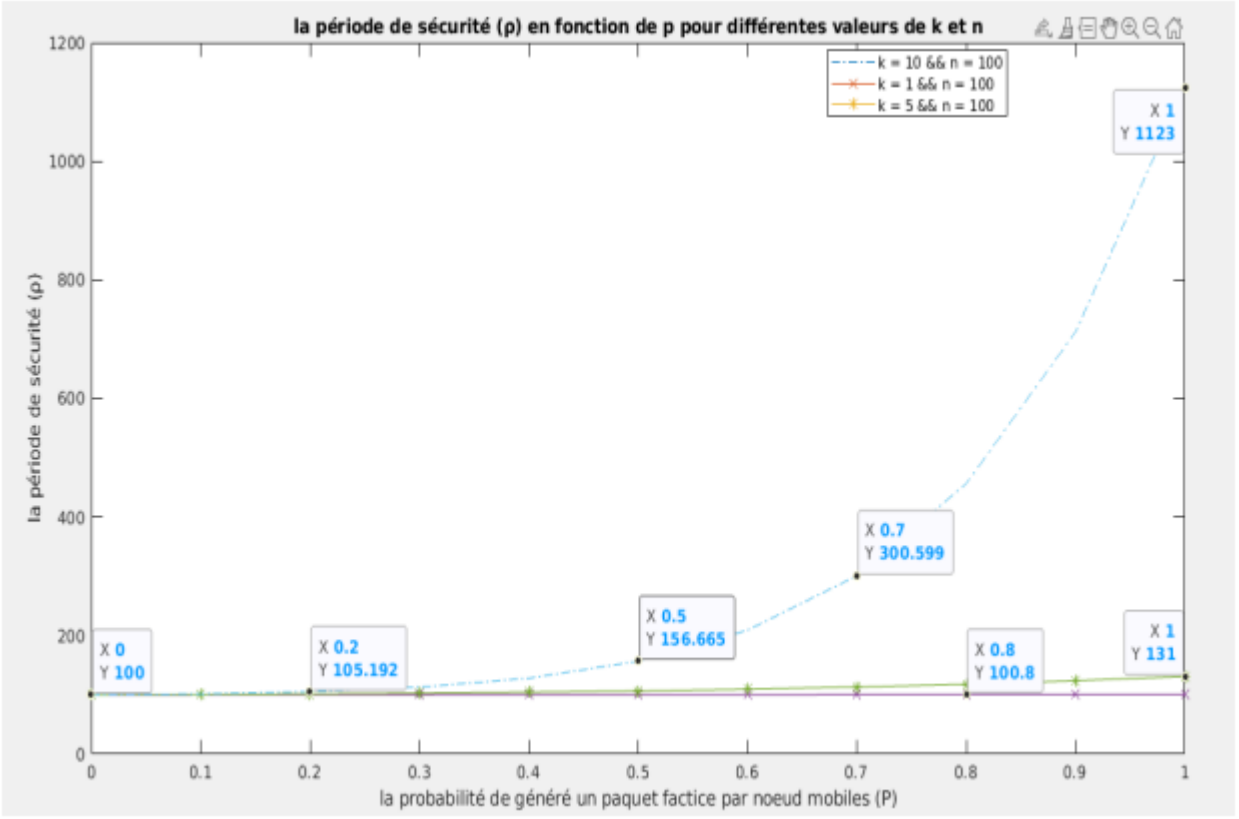


**Figure V.3 Période de sécurité (ρ) en fonction de la probabilité (P) de création des paquets factices.**

L'analyse des courbes graphiques de la figures V.3 montre que plus *P* augmente, plus la période de sécurité est grande. Par exemple, sur la courbe correspondante à $k = 10$ ; quand la probabilité est fixée à une valeur maximale $P = 1$, la période de sécurité atteint le maximum **ρ =** 1123 et quand la probabilité de génération d'un sous-arbre est très faible p ϵ [0..0,2] la période de sécurité devient très faible et s'approche de la valeur minimale ***n,*** ρ ϵ [100..105.2].

Lorsque $k = 0$ (les sous arbres de profondeur 0) ou $P = 0$ (aucun sous arbre n'est généré), on constate que la période de sécurité ρ égale à *n* qui est la distance en sauts entre le nœud source et la station de base.

- **Période de sécurité ρ en fonction de la distance n entre la source et la station de base**

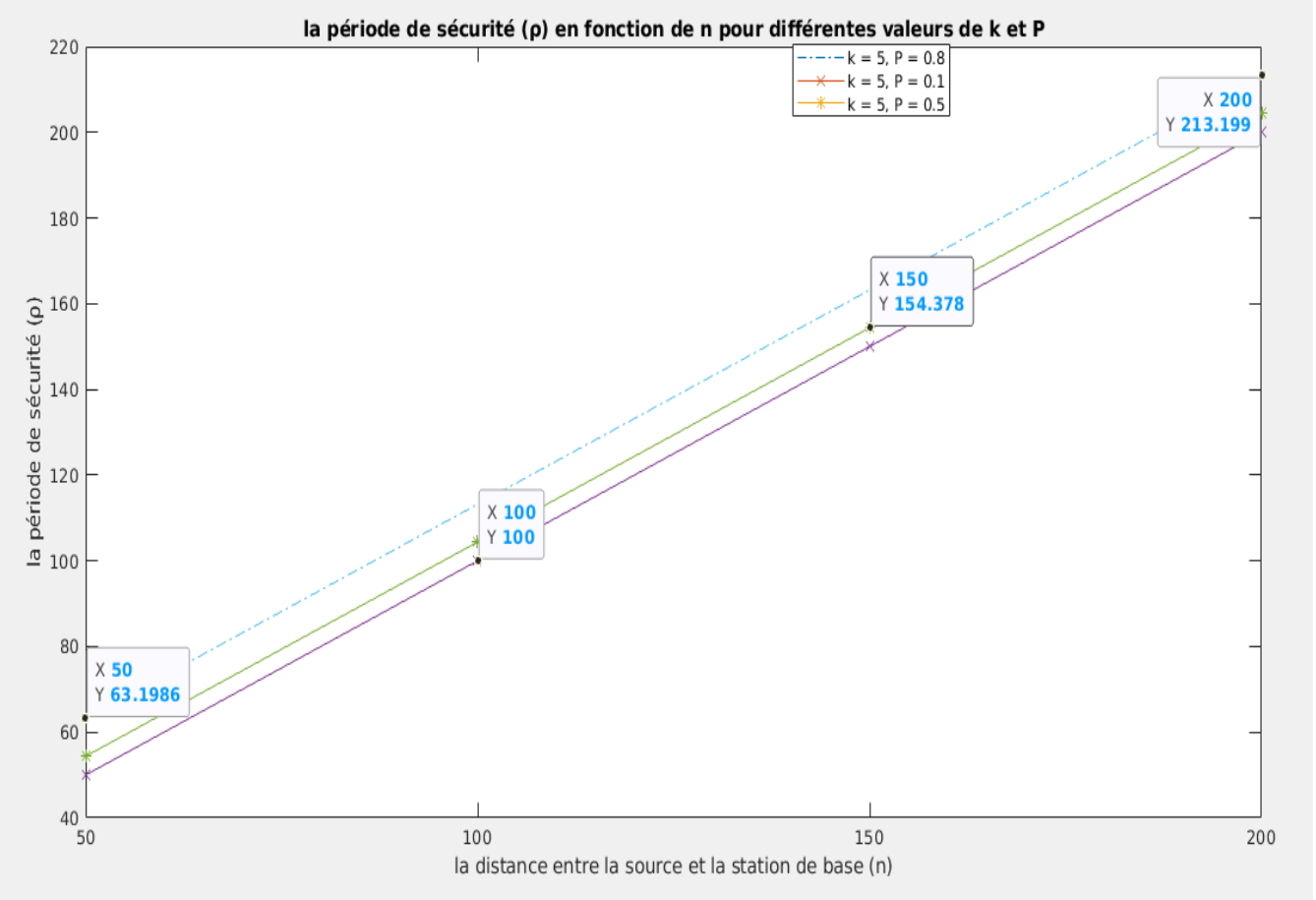


**Figure V.4 Période de sécurité en fonction de la distance entre le nœud source et la station de base n en fixant *k* et *P*.**

D'après les résultats obtenus, la période de sécurité augmente linéairement. Cette faible augmentation peut s'expliquer comme suit : quand ***n*** augmente de ***x*** sauts, la période de sécurité ρ augmente aussi de ***x*** sauts, car c'est linéaire ; contrairement à l'augmentation de *k* qui consiste à augmenter plusieurs branches du sous arbre de ***x*** sauts. De même pour le paramètre *P* qui consiste à générer plus de sous arbres quand p augmente.

Dans la figure V.4, quand on a fixé la profondeur d'un sous arbre K à 5 et la probabilité p =0.8 et on varie ***n***, le graphe obtenu est linéaire. De même, pour *k* = 5 et *P* = 0.5 puis *P*= 0.1, les graphes obtenus sont toujours linéaires. Cependant, les trois graphes sont différents à cause de P qui n'est pas le même.

Dans l'expérience représentée dans la figure V.5, on a refait la même expérience que précédemment en variant ***n***, mais on fixe *P* et prend différentes valeurs de *k*. On fixe la probabilité de création des paquets factices *P* à 0,5 et k = 1, 5 et 10.

En examinant la relation entre la distance ***n*** et la période de sécurité, nous constatons que la période de sécurité augmente toujours linéairement. Cela s'explique comme précédent. D'après les figures V.4 et V.5, on constate que l'augmentation de la période de sécurité est insignifiante quand la distance entre la source et la station de base augmente.

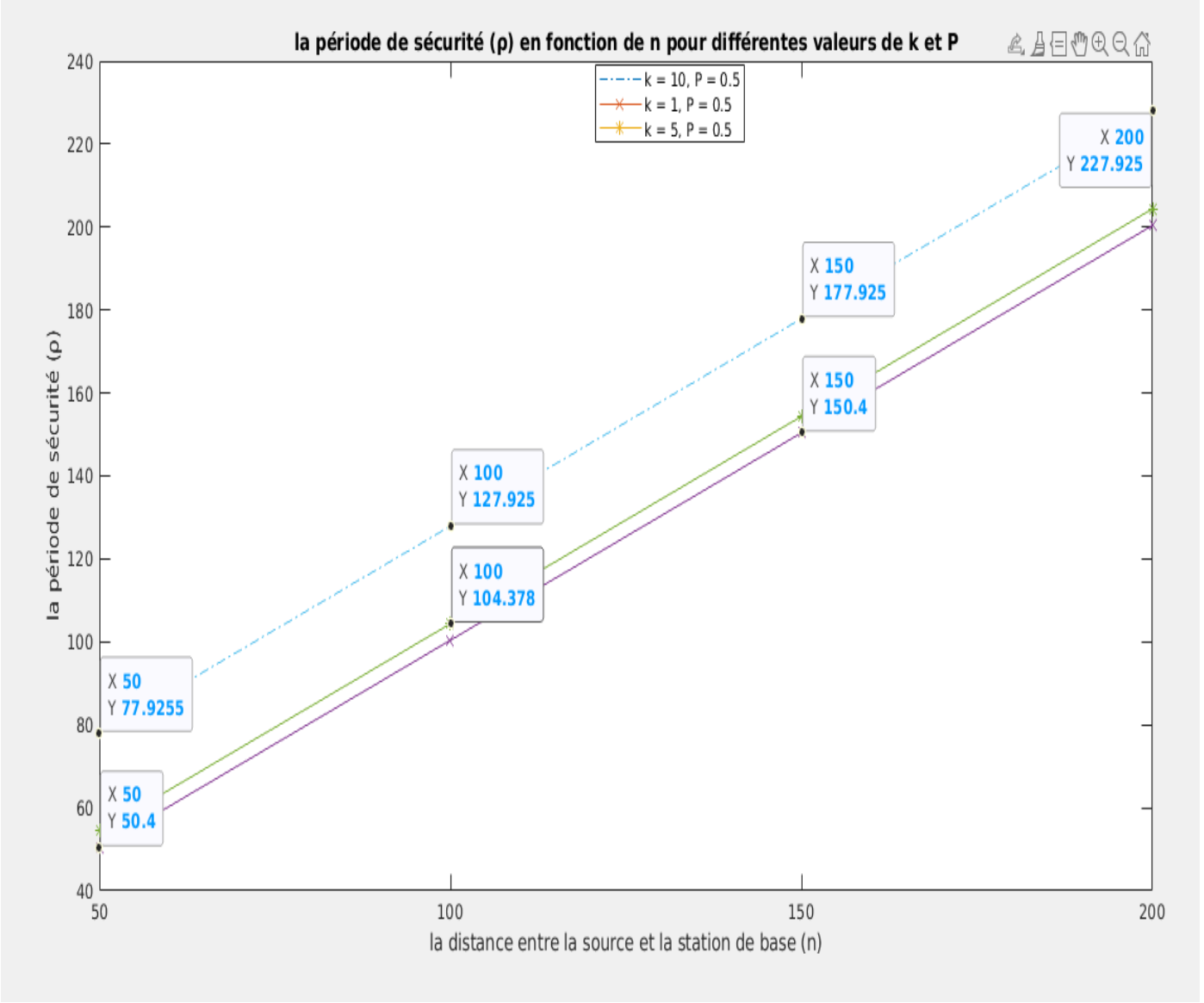


**Figure V.5 Période de sécurité en fonction de la distance entre le nœud source et la station de base n en fixant *k* et *P*.**

## V.6 Conclusion :

Dans ce chapitre, on a utilisé MATLAB pour évaluer la période de sécurité fournit par notre solution pour protéger la confidentialité de la station de base dans les RCSF, en se basant sur différents paramètres tels que la probabilité de génération d'un faux trafic au niveau de chaque nœud le long du chemin entre la source et la station de base et la profondeur *k* du faux trafic généré sous forme de sous- arbres.

En utilisant MATLAB, on a développé une fonction qui prend en compte les valeurs de *k*, *P* et la distance *n* pour déduire les différentes périodes de sécurité. On a ensuite tracé des graphiques à partir de ces résultats pour visualiser les variations des périodes de sécurité en fonction des paramètres.

L'objectif de cette analyse était de comprendre comment les différentes valeurs de *k*, *P* et n influent sur les périodes de sécurité dans le système RCSF. En utilisant MATLAB, on a pu obtenir des résultats précis et visualiser ces résultats sous forme de graphiques, ce qui facilite la compréhension des relations entre la profondeur de génération des sous-arbres par des nœuds, la probabilité de généré des paquets factices et les périodes de sécurité.

# Conclusion général

Cette recherche a exploré un parcours détaillé à travers les complexités des réseaux de capteurs sans fil, mettant en lumière des approches innovantes pour renforcer la sécurité et protéger la confidentialité des données sensibles, en particulier les emplacements des sources et des stations de base.

Notre exploration a débuté avec une plongée dans les profondeurs des réseaux de capteurs sansfil, révélant leurs multiples applications et leur rôle crucial dans la collecte et le transfert de données dans des environnements variés. Cette première étape a intégré un solide fondement pour les développements ultérieurs axés sur la sécurité.

La suite de notre exploration a relevé le voile sur une gamme de protocoles de sécurité, chacun étant conçu pour préserver la confidentialité des emplacements des sources et des stations de base, en plus d'assurer l'authenticité de l'identité de la source. Cette étape a souligné de manière éloquente l'importance cruciale de sécuriser les informations sensibles, dans un monde où la connectivité peut également introduire des vulnérabilités.

Le point culminant de cette expédition intellectuelle a résidé dans le troisième chapitre, où nous avons élaboré un protocole innovant. Spécifiquement conçu pour préserver la confidentialité des emplacements des stations de base, ce protocole a été forgé à travers une réflexion approfondie et une conception soigneuse de mécanismes de sécurité avancés. Son mais ultime : renforcé la résilience potentielle du système face aux menaces et garantir la confidentialité des données sensibles.

Enfin, nous avons mis à l'épreuve notre protocole via des simulations avec MATLAB, en fonction de la période de sécurité. Ces résultats concrets ont ajouté une dimension pratique à notre travail, fournissant des preuves tangibles de l'efficacité et de la pertinence du protocole en des situations variées.

En somme, notre exploration a tracé un parcours de la création des réseaux de capteurs sans fil à la conception d'un protocole de confidentialité innovant, en passant par l'exploration approfondie des protocoles de sécurité existants et la prise en compte des subtilités préoccupations relatives aux emplacements. Les résultats dissimulations ont enrichi notre travail en fournissant des éléments concrets pour une utilisation plus sécurisée des données dans un monde de plus en plus connecté. Ce projet apporte une contribution précieuse au domaine en constante évolution de la sécurité des réseaux de capteurs sans fil, ouvrant la voie à des solutions plus fiables et confidentielles pour l'avenir.

# Bibliographie

**[1]** I.F. Akyildiz, W. Su *, Y. Sankarasubramaniam, E. Cayirci. “Wireless sensor networks: a survey”, Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology,Atlanta, GA 30332, USA .

**[2]** Athmani.S [2010]. ”Protocole de sécurité pour les réseaux de capteur sans fil”. Doctoral dissertion, université Batna 2

**[3]** Bouallegue, M. (2016). “*Protocoles de communication et optimisation de l'énergie dans les réseaux de capteurs sans fil ”*.(Doctoral dissertation, Université du Maine).

**[4]** Drira, W., Bekara, C., & Laurent, M. (2008).“*Sécurité dans les réseaux de capteurs sans fil: conception et implémentation*”.(Doctoral dissertation, Dépt. Logiciels-Réseaux (Institut Mines- Télécom-Télécom SudParis); Services répartis, Architectures, MOdélisation, Validation, Administration des Réseaux (Institut Mines-Télécom-Télécom SudParis-CNRS)).

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

**[6]** Ouyang, Y., Le, X., Chen, G., Ford, J., & Makedon, F. (2006, June). “Entrapping adversaries for source protection in sensor networks”. In *2006 International symposium on a world of wireless, mobile and multimedia networks (WoWMoM'06)* (pp. 10-pp). IEEE.

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

**[8]** Wang, W. P., Chen, L., & Wang, J. X. (2008, May). “A source-location privacy protocol in WSN based on locational angle”. In *2008 IEEE International Conference on Communications* (pp. 1630-1634). IEEE.

**[9]** Ouyang, Y., Le, Z., Liu, D., Ford, J., & Makedon, F. (2008, September). “Source location privacy against laptop-class attacks in sensor networks”. In *Proceedings of the 4th international conference on Security and privacy in communication netowrks* (pp. 1-10).

**[10]** Yun li and Jian ren, “Mixig Ring-Based Source-Location Privacy in Wireless sensor network”. Department of electrical and computer Engineering Michigan State University East Lansing, MI 48824.

**[11]** Yang, Y., Shao, M., Zhu, S., Urgaonkar, B., & Cao, G. (2008, March). Towards event source unobservability with minimum network traffic in sensor networks. In Proceedings of the first ACM conference on Wireless network security (pp. 77-88).

**[12]** Shao, M., Hu, W., Zhu, S., Cao, G., Krishnamurth, S., & La Porta, T. (2009, June). Cross-layer enhanced source location privacy in sensor networks. In 2009 6th Annual IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks (pp. 1-9). IEEE.

**[13]** Deng, J., Han, R., & Mishra, S. (2004, June). "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks". In *International Conference on Dependable Systems and Networks, 2004*(pp. 637- 646). IEEE.

**[14]** Deng, J., Han, R., & Mishra, S. (2006). "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks". *Pervasive and Mobile Computing*, *2*(2), 159-186.

**[15]** Jian, Y., Chen, S., Zhang, Z. et Zhang, L. (2007, mai). "Protéger la confidentialité de l'emplacementdu récepteur dans les réseaux de capteurs sans fil". Dans *IEEE INFOCOM 2007-26th IEEE InternationalConference on Computer Communications* (pp. 1955-1963).IEEE.

**[16]** Ngai, E. C. H., & Rodhe, I. (2009, October). "On providing location privacy for mobile sinks in wireless sensor networks". In *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems* (pp. 116-123).

**[17]** J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor NetworkSecurity: A Survey",Department of Computer Science Wayne State University.

**[18]** Ouyang, Y., Le, Z., Xu, Y., Triandopoulos, N., Zhang, S., Ford, J., & Makedon, F. (2007, July). Providing anonymity in wireless sensor networks. In *IEEE international conference on pervasive services* (pp. 145-148). IEEE.

# Résumé

Notre projet se penche sur la préservation de la confidentialité d'emplacement dans les réseaux de capteurs sans fil. Il consiste à fournir la confidentialité d'emplacement de la source d'un événement ainsi que sadestination. La première mesure de protection est de cacher l'identité de l'émetteur et du recepteur.la deuxième mesure de sécurité est de cacher le modèle de trafic. Des méthodes ont été explorées qui tentent augmentateur l'incertitude des modèles de trafic pour contre carrer les attaques d'analyse de trafic. Pour ce faire, on a examiné plusieurs protocoles de sécurité et évaluez leur avantage et leurs inconvénients. De plus, on a proposé une approche novatrice axée sur la confidentialité de la station de base. Cette proposition vise à renforcer la protection de l'emplacement de en la rendant moins vulnérable aux attaques d'analyse de trafic.


**Mots clés** : RCSF, confidentialité d'emplacement, attaques d'analyse de trafic. Matlab, identité d'un noeud.



# Abstract

Our project focuses on preserving location privacy in wireless sensor networks. It consists of providing location confidentiality of the event source as well as its destination. The first protection measureis to hide the sender and receiver identity. The second security measure is to hide the traffic pattern. Methods have been explored that attempt to increase the uncertainty of traffic patterns to thwart traffic analysis attacks. To do this, we examined several security protocols and evaluate their advantages and their disadvantages. Additionally, an innovative approach focused on base station privacy was proposed. This proposal aims to strengthen the location privacy protection by making it less vulnerable to traffic analysis attacks.



**Keywords**: WSN, location privacy, traffic analysis attaks, Matlab, node identity.