REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE ET DE l'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DES SCIENCES APPLIQUEES ET DE TECHNOLOGIE

DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études pour l'obtention du :

Master en Réseaux, Sécurité et Systèmes Distribués (R2SD)

Authentification Mutuelle dans les Réseaux de Capteurs Sans Fil (RCSF)

Présenté par :

Melle Mame Diarra B. NIANG

Sous la direction de :

Pr. Chérif DIALLO

Jury :

Président :	M.
Examinateur :	M.
Examinateur :	M.
Examinateur :	M.
Encadrant :	M. Chérif DIALLO

Année Académique 2021/2022

Dédicace

Je dédie ce mémoire à ma grand-mère qui est partie trop tôt...

A ma mère

A mon père

Ames frères et sœurs

Et A toute ma famille, amis et proches

...

Remerciements

Tout d'abord, on rend grâce à Dieu, Le Tout Puissant…

Mes remerciements s'adressent :

A mes chers parents Adja Ndèye Samb DIOUF et Bassirou NIANG qui m'ont toujours soutenu pendant toutes mes années d'étude et qui ont fait de moi la personne que je suis aujourd'hui ;

A mon oncle paternel Abibou NIANG qui m'a toujours accompagné et encouragé tout le long de mon cursus ;

A ma cousine et sœur Henriette DIOP (« ance ») qui a été la première à m'intégrer au sein de l'université Gaston Berger ; à mes petites sœurs du campus Marie Louise Diouf et Seynabou Sangaré ;

A toute ma famille qui a été avec moi dans les bons comme dans les mauvais moments et qui m'a toujours supporté moralement ;

A tous mes camarades de promotion et à tous nos professeurs qui nous ont accompagné durant ce cycle universitaire ;

Et enfin, je ne saurais terminer sans remercier particulièrement mon Encadrant et Professeur Monsieur Chérif Diallo pour ses précieux conseils, sa patience et sa disponibilité ;

Tout le mérite vous revient…

RESUME

“L’homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. ” Albert Einstein

Un RCSF est composé d'un ensemble de nœuds capteurs capables de recueillir et de transmettre des données d’une manière autonome. Ces réseaux doivent être surveillées à temps réel surtout dans certains domaines d’applications critiques. Les solutions de sécurité utilisées dans les réseaux traditionnels ne sont pas directement applicables dans les RCSF, car développer des primitives de sécurité en utilisant de faibles ressources devient un véritable défi. C’est dans cette perspective que nous avons eu l’idée d’orienter notre recherche sur l’authentification mutuelle dans les RCSF afin d’apporter notre contribution. Le travail principal dans ce mémoire a consisté à proposer une amélioration du protocole de Vaidya et al au niveau de la topologie du réseau mais aussi de l’implémentation de l’algorithme afin de le rendre plus efficace et efficient en termes de sécurité et de consommation énergétique.

Mots Clés : RCSF, sécurité, authentification mutuelle, Vaidya et al, algorithme

ABSTRACT

"Man and his safety must be the first concern of any technological adventure" Albert Einstein

A WSN (Wireless Sensor Networks) is made up of a set of sensor nodes able of collecting and transmitting data autonomously. These networks need to be monitored in real time, especially in certain critical applications. The security solutions used in traditional networks are not directly applicable in WSN, as developing security primitives using limited resources becomes a real challenge. It is in this perspective that we decide to focus our research on mutual authentication in WSN to make our contribution. The main work in this master's thesis consisted in proposing an improvement to the Vaidya et al' s protocol in terms of network topology but also the implementation of the algorithm to make it more effective and efficient in terms of security and energy consumption.

Keywords : WSN, security, mutual authentication, Vaidya et al, algorithm

Liste des Illustrations

Figure 1 : Architecture de base d'un capteur [B] 11
Figure 2 : Architecture d'un RCSF [A] 12
Figure 3 : Topologie plate d'un RCSF [8] 13
Figure 4 : Topologie hiérarchique d'un RCSF [8] 14
Figure 5 : Domaines d'application des RCSF [C] 15
Figure 6 : L'attaque par Jamming [9] 20
Figure 7 : Attaque par Expédition Sélective [3] 21
Figure 8 : L'attaque Sinkhole [3] 22
Figure 9 : L'attaque Sybil [3] 23
Figure 10 : L'attaque Wormhole [3] 24
Figure 11 : Contraintes et défis de sécurité des RCSF 26
Figure 12 : Chiffrement symétrique [D] 27
Figure 13 : Chiffrement asymétrique [D] 28
Figure 14 : Chiffrement hybride [E] 29
Figure 15 : Authentification par mot de passe [F] 31
Figure 16 : Critères d'évaluation des protocoles d'authentification 32
Figure 17 : : Fonction de hachage 35
Figure 18 : Phase d'enregistrement 42
Figure 19 : Phase de Login-Authentification 43

Liste des Tableaux

Tableau 1 : Comparaison de quelques protocoles d'authentification 34
Tableau 2 : Notations 37
Tableau 3 : Comparaison protocoles d'authentification et solution proposée 46

Sigles et Abréviations

RCSF	Réseaux de Capteurs Sans Fil
DoS	Déni de Service
IEEE	Institute of Electrical and Electronics Engineers
WSN	Wireless Sensor Network
CRC	Contrôle de Redondance Cyclique
ACK	Acknowledgement (Accusé de Réception)

Table des matières

REPUBLIQUE DU SENEGAL 1
INTRODUCTION GENERALE 9
1 10
ETAT DE L'ART SUR LES RESEAUX DE CAPTEURS SANS FIL 10
I.1 Définitions 10
I.2 Architecture de base d'un capteur 10
I.3 Architecture de base d'un RCSF 12
I.4 Type d'architecture des RCSF 12
I.5 Domaines d'application des RCSF 15
I.6 Facteurs principaux de conception 16
2 18
PROBLEMATIQUE DE LA SECURITE DANS LES RESEAUX DE CAPTEURS SANS FIL 18
II.1 Les objectifs de sécurité des RCSF 18
II.2 Les attaques connues dans les RCSF 19
II.3 Les contraintes influençant la sécurité d'un RCSF 25
II.4 Analyse de la sécurité et solutions envisageables 25
3 31
ETUDE COMPARATIVE DE QUELQUES TRAVAUX ET ANALYSE DE PERFORMANCE 31
III.1 Protocoles d'authentification des utilisateurs 31
III.2 Critères d'évaluation 32
III.3 Comparaison de quelques protocoles 33
4 35
CONTRIBUTION : AMELIORATION D'UN PROTOCOLE D'AUTHENTIFICATION DES RCSF 35
IV.1 L'authentification par hachage pour sécuriser les RCSF 35
IV.2 Description du protocole de Vaidya et Al 36
IV.3 Vulnérabilités du protocole d'authentification 40
IV.4 Solution proposée 41
CONCLUSION GENERALE 47
BIBLIOGRAPHIE 48
WEBOGRAPHIE 50

INTRODUCTION GENERALE

La convergence de la micro-électronique et des technologies de communication sans-fil a permis la création d'une combinaison entre les systèmes embarqués et les systèmes distribués ayant engendré les Réseaux de Capteurs Sans-Fil ou RCSF (Wireless Sensor Networks). Depuis les dernières décennies, les réseaux de capteurs sans fil (RCSF) ont émergé comme une technologie clé dans de nombreux domaines, tels que la surveillance environnementale, l'agriculture intelligente, les villes intelligentes et les systèmes de santé. Les RCSF permettent de collecter des données provenant de capteurs répartis dans un environnement physique et de les transmettre sans fil vers une station de base pour analyse et traitement ultérieur.

Cependant, l'essor des RCSF soulève également des préoccupations majeures en matière de sécurité. Ces nœuds capteurs qui opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie, peuvent être soumis à des actions perturbatrices et malveillantes susceptibles de compromettre l'essence même d'un RCSF. L'objectif de la sécurité a toujours été globalement le même, à savoir assurer les services de sécurité de base tels que l'authentification, le contrôle d'accès, la confidentialité, l'intégrité, la disponibilité etc...

Dans ce mémoire, nous allons nous intéresser particulièrement à la problématique de l'authentification mutuelle dans les réseaux de capteurs sans fil. Il comporte quatre parties.

Dans un premier temps, nous allons faire l'état de l'art des réseaux de capteurs sans fil, plus précisément l'architecture, les domaines d'application, les facteurs de conception des RCSF.

Nous aborderons la problématique de la sécurité dans les réseaux de capteurs dans le deuxième chapitre : les objectifs de sécurité, les attaques connues dans les RCSF, les contraintes à la sécurité, les solutions envisageables.

Dans le chapitre 3, nous effectuerons une comparaison de quelques protocoles de sécurité après avoir présenté les critères d'évaluation des protocoles d'authentification des utilisateurs.

Enfin, dans le chapitre 4, nous nous consacrerons à l'authentification mutuelle par hachage et ferons une description du protocole de Vaidya et al. Par la suite, nous proposerons notre solution qui consiste en l'amélioration du protocole d'authentification de Vaidya et al et l'évaluerons par rapport aux autres protocoles déjà examinés au chapitre précédent.

1

ETAT DE L'ART SUR LES RESEAUX DE CAPTEURS SANS FIL

I.1 Définitions

Un **capteur** est un dispositif électronique qui mesure une grandeur physique ou chimique et la convertit en un signal exploitable par un système électronique ou informatique. Les capteurs lient le monde physique avec le monde digital en capturant et en relevant les phénomènes réels sous une forme qui permet de les traiter, de les stocker et d'interagir.

Les capteurs sont utilisés dans de nombreux domaines, tels que l'industrie, l'automobile, l'aéronautique, la médecine, l'environnement, la sécurité, les télécommunications, l'informatique, etc. Ils sont souvent intégrés à des systèmes de contrôle et d'acquisition de données pour surveiller et contrôler les processus en temps réel, détecter des anomalies ou des pannes, ou encore collecter des données pour des analyses ultérieures.

Un **Réseau de Capteurs Sans Fil (WSN en anglais)** est un réseau ad hoc d'un grand nombre de nœuds, qui sont des micro-capteurs capables de recueillir et de transmettre des données d'une manière autonome. Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Les nœuds capteurs sont des capteurs intelligents "smart sensors", capables d'accomplir trois tâches complémentaires : le relevé d'une grandeur physique, le traitement éventuel de cette information et la communication avec d'autres capteurs.

I.2 Architecture de base d'un capteur

Un capteur est composé de quatre (04) unités principales :

- L'unité de **Capture**

L'unité de capture ou sonde est un dispositif permettant de transformer l'état d'une grandeur physique observée en une grandeur utilisable notamment une tension électrique, une température ou une intensité lumineuse. Elle est composée de deux sous-éléments à savoir :

- Le capteur recevant des données analogiques ;
- Le convertisseur faisant passer les données analogiques du capteur à des données numériques envoyées à une unité de calcul.

- L'unité de **Traitement**

L'unité de traitement est généralement composée d'un processeur et d'une unité de stockage. Elle fonctionne à l'aide d'un système d'exploitation et permet de stocker les données, d'exécuter les tâches de perception qui lui sont assignées.

- L'unité de **Transmission** (Communication)

L'unité de transmission permet la communication entre les nœuds de réseaux de capteurs sans fil via des liaisons radio. Elle est composée d'un émetteur et d'un récepteur. Ces liaisons radio peuvent être de type optique ou radio fréquence.

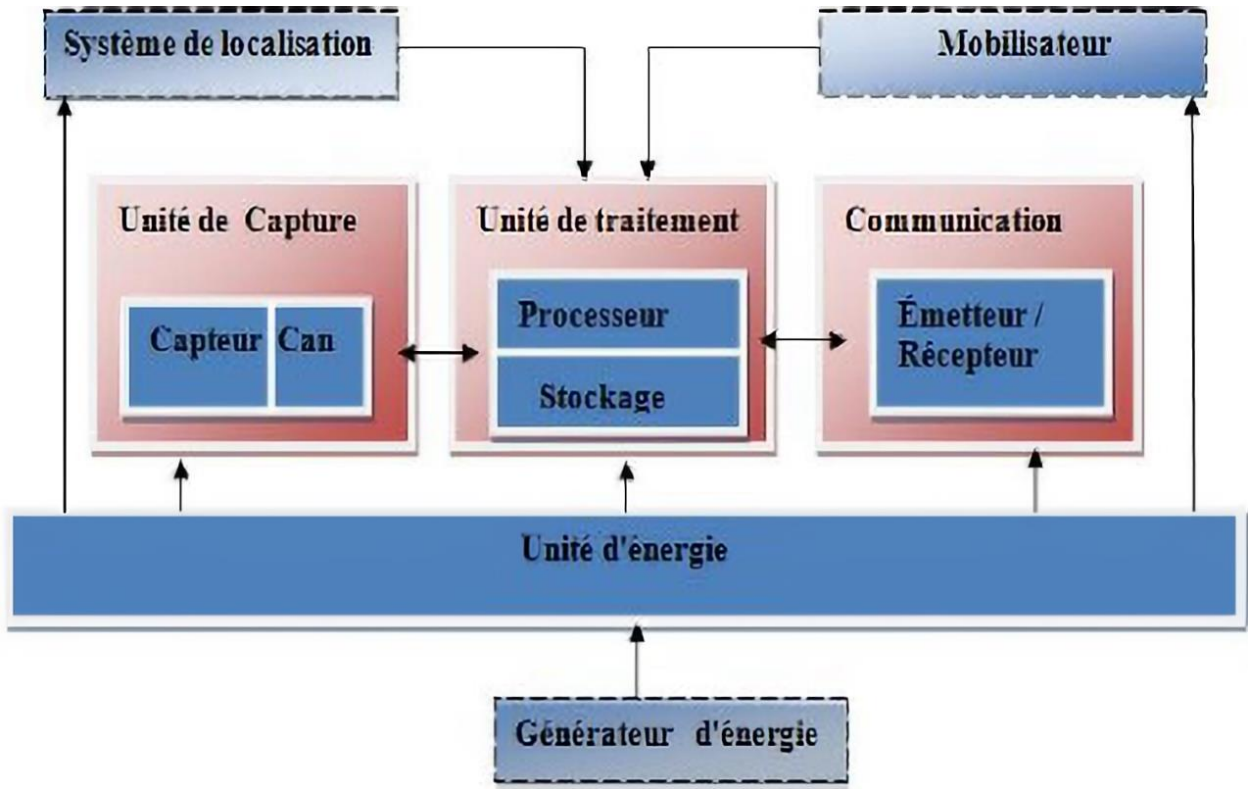


Figure 1 : Architecture de base d'un capteur [B]

I.3 Architecture de base d'un RCSF

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

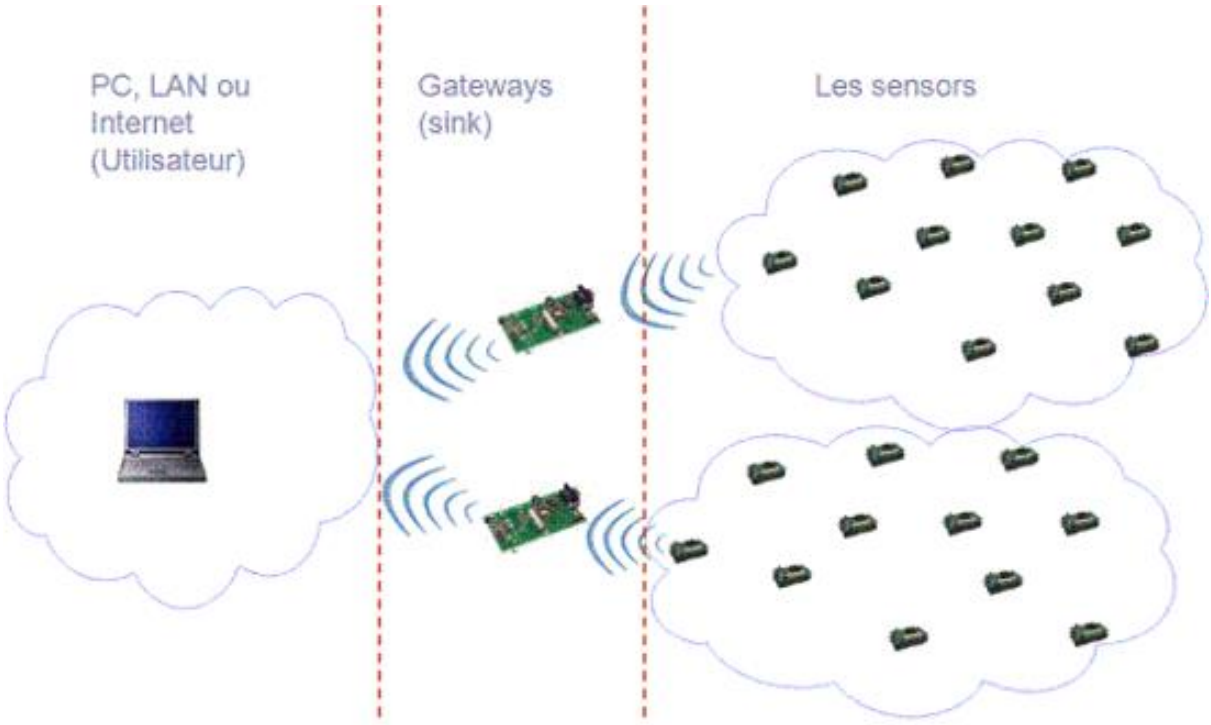


Figure 2 : Architecture d'un RCSF [A]

I.4 Type d'architecture des RCSF

Les réseaux de capteurs sans fil peuvent être organisés en deux types d'architecture : plate ou hiérarchique.

I.4.1 Topologie plate

Dans le contexte des RCSF (Réseaux de Capteurs Sans Fil), l'architecture plate est une structure de réseau où tous les nœuds du réseau sont considérés comme égaux en termes de rôle et de responsabilités. On peut distinguer deux manières de communication dans une telle architecture.

On peut distinguer deux manières de communication dans une telle architecture. La première consiste à transmettre les données directement au puits. C'est-à-dire, chaque nœud peut directement faire passer ses informations traitées à la station de base avec une puissance élevée d'émission. La deuxième manière de communication permet d'utiliser le mécanisme des intermédiaires appelé mode multi-saut. Pour que ces informations atteignent leur destination, elles passent d'un nœud à l'autre jusqu'à atteindre leur destination. Ce mode est le plus implémenté. Car, sa consommation énergétique est faible au niveau des nœuds ainsi sa gestion des redondances et sa tolérance aux pannes sont bonnes.

L'architecture plate est souvent utilisée dans les réseaux de capteurs sans fil pour les applications telles que la surveillance de l'environnement, la surveillance de la santé et la surveillance de la sécurité. Cependant, pour les applications plus complexes, une architecture plus hiérarchique peut être nécessaire pour gérer la charge de trafic et assurer une communication efficace entre les nœuds.

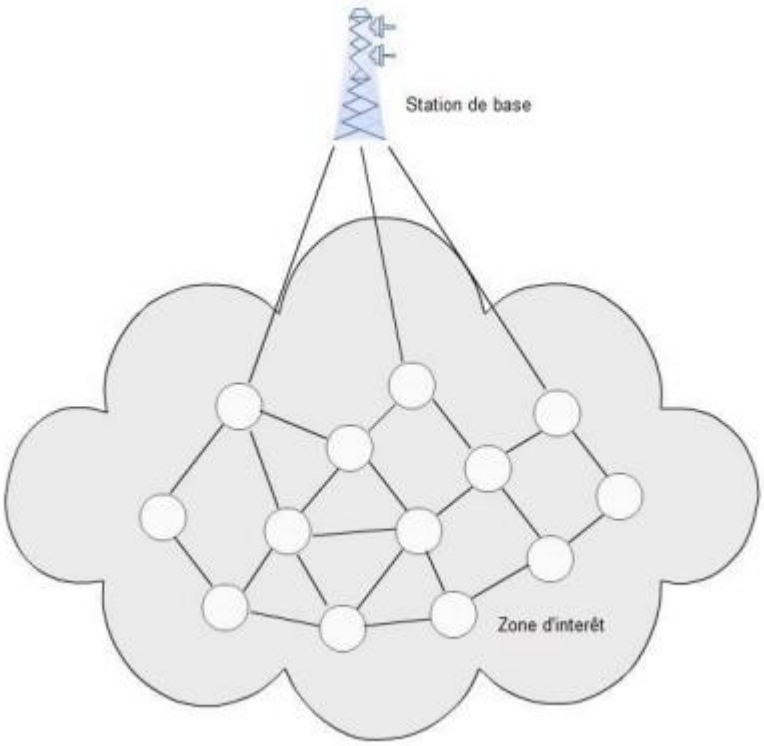


Figure 3 : Topologie plate d'un RCSF [8]

I.4.2 Topologie hiérarchique

Dans une architecture hiérarchique, les nœuds du réseau sont organisés en plusieurs niveaux, chacun jouant un rôle spécifique.

Le niveau supérieur est généralement composé de nœuds plus puissants, appelés "nœuds relais" qui sont des chefs de groupe. Ces nœuds ont pour fonction de gérer le trafic de données entre les différents nœuds du niveau inférieur et d'agréger les données collectées par ces derniers.

Le niveau inférieur est constitué des nœuds de capteurs, qui sont responsables de la collecte de données sur l'environnement surveillé et de leur transmission aux nœuds relais. Ces nœuds sont généralement moins puissants et ont des capacités de traitement et de stockage plus limitées que les nœuds relais.

L'architecture hiérarchique dans les RCSF permet d'optimiser la consommation d'énergie et d'augmenter la durée de vie du réseau en réduisant le nombre de transmissions de données entre les nœuds. De plus, elle permet d'améliorer la fiabilité et la robustesse du réseau en permettant la récupération des données à partir de plusieurs nœuds en cas de défaillance d'un nœud.

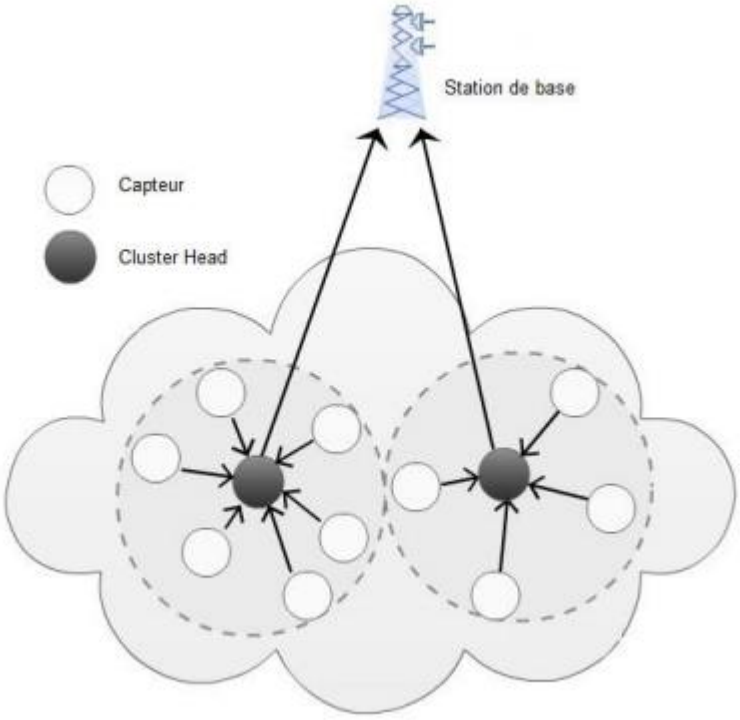


Figure 4 : Topologie hiérarchique d'un RCSF [8]

I.5 Domaines d'application des RCSF

Grace aux évolutions de la technologie touchant les domaines : électronique, informatique industrielle, instrumentation, réseaux et télécommunication, le champ d'application des réseaux de capteurs sans fils est de plus en plus en élargissement. Les RCSF peuvent être utilisés dans une grande variété de domaines d'application.



Figure 5 : Domaines d'application des RCSF [C]

I.5.1 Applications militaires

Les applications militaires sont très étroitement liées au concept des réseaux de capteurs sans fil. Comme la plupart des technologies, les applications militaires étaient les premières à intégrer les RCSF. Un réseau de capteurs est déployé sur un secteur stratégique pour détecter les mouvements ennemis dans des zones sensibles, telles que les zones frontalières et les bases militaires, pour suivre les équipements militaires et les véhicules sur le terrain, détecter les substances chimiques dangereuses, telles que les gaz toxiques, qui peuvent être utilisées comme armes…

I.5.2 Applications médicales

En implantant sous la peau de mini capteurs vidéo, on peut recevoir des images en temps réel d'une partie du corps sans aucune chirurgie. Les RCSF peuvent être utilisés pour assurer une surveillance permanente des patients, mesurer des signes vitaux tels que la fréquence cardiaque, la tension artérielle, la température… Les données peuvent être utilisées pour identifier des

tendances et aider les professionnels de la santé à élaborer des plans de soins personnalisés pour chaque patient. Des réseaux de capteurs permettraient également une surveillance temps réel des maternités (détection de vol de bébés) ou des patients.

I.5.3 Applications environnementales

Ces types de RCSF peuvent servir à l'observation d'un site susceptible de subir les effets d'une pollution, ou bien d'éventuel incendie, inondation, volcan ou tsunami, à la capture des informations environnementales telles que la pression barométrique, la température ambiante, l'humidité atmosphérique, la direction et la vitesse du vent, le niveau de l'eau souterraine.

I.5.4 Applications commerciales

Dans le domaine de la grande distribution, les réseaux de capteurs pourraient améliorer le processus de stockage et de livraison. Le réseau ainsi formé pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison. Un client attendant un paquet peut alors avoir un avis de livraison en temps réel et connaître la position du paquet.

Grâce aux réseaux de capteurs, les entreprises pourraient offrir une meilleure qualité de service tout en réduisant leurs coûts.

I.5.5 Applications industrielles

En industrie, les réseaux de capteurs sans fil peuvent chacun garantir la communication entre les machines de production d'une manière permanente.

Parmi les applications des réseaux de capteurs sans fil dans le milieu industriel, nous citons la surveillance de l'état de santé d'un ouvrier ou du risque de le voir exposé à des conditions de travail dangereuses (exposition à la radioactivité), la gestion des stocks, contrôle des machines à distance…

I.6 Facteurs principaux de conception

- La tolérance aux pannes

La tolérance de fautes est la capacité de maintenir les fonctionnalités du réseau sans interruptions dues à une erreur intervenue sur un ou plusieurs capteurs. Cette défaillance peut être causée par une perte d'énergie, dommage physique ou interférence de l'environnement.

- La scalabilité

La notion de scalabilité est utilisée pour dire que l'architecture et les protocoles de communications du réseau doivent s'adapter et prendre en compte l'ajout ou la perte de nœuds dans le réseau. La scalabilité et l'adaptabilité sont des contraintes étroitement liées à la nature des applications de réseaux de capteurs.

- La topologie du réseau

Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie. Cette maintenance consiste en trois phases : Déploiement, Post-déploiement (les capteurs peuvent bouger, ne plus fonctionner), redéploiement de nœuds additionnels.

- Les contraintes matérielles

La principale contrainte matérielle est la taille du capteur. Les fonctionnalités mises en œuvre par la partie matérielle se doivent d'être aussi simples que possible, car l'augmentation de la complexité de cette dernière peut conduire à une augmentation de la consommation d'énergie.

- Les coûts de production

Souvent, les réseaux de capteurs sont composés d'un très grand nombre de nœuds. Afin de pouvoir justifier son intérêt, le coût global d'un réseau de capteurs sans fil doit être faible par rapport à celui d'un réseau classique et « raisonnable » par rapport aux objectifs de l'application. En effet, un RCSF doit être conçu afin que la maintenance et le support soient des plus aisés et de moindres coûts.

- L'auto-configuration

Un réseau de capteurs doit pouvoir configurer tous ses paramètres indépendamment de son environnement d'installation. Le réseau doit par exemple être capable d'identifier les positions des nœuds, ce qui lui permettra d'identifier et de tolérer d'éventuelles pannes (problème de batterie) ou bien encore d'intégrer de nouveaux nœuds.

- La consommation d'énergie

Les nœuds capteurs embarquent en général une quantité d'énergie très limitée. En effet, la difficulté de changement de batterie des capteurs rend la nécessité de trouver d'autres moyens de minimisation de la consommation d'énergie.

Par conséquent, pour atteindre cette autonomie, il est crucial de minimiser la consommation moyenne des capteurs. Une des alternatives explorées aujourd'hui par les chercheurs consiste à extraire l'énergie de l'environnement (énergie solaire, vibrations mécaniques, bruit acoustique…).

2

PROBLEMATIQUE DE LA SECURITE DANS LES RESEAUX DE CAPTEURS SANS FIL

II.1 Les objectifs de sécurité des RCSF

Les réseaux de capteurs sans fil sont souvent utilisés pour surveiller des environnements sensibles tels que les installations militaires, les centrales nucléaires, les infrastructures critiques ; donc la sécurité est une préoccupation majeure. Ils partagent certaines similitudes avec un système informatique classique en termes d'exigences en sécurité.

Les applications des RCSF n'ont pas les mêmes besoins en sécurité, mais en général, les objectifs primaires que l'on doit considérer en implémentant la sécurité dans les RCSF sont : la confidentialité, l'authentification, l'intégrité, la disponibilité, la non-répudiation, l'anonymat, la localisation.

II.1.1 La confidentialité

Elle consiste à s'assurer que personne ne pourra interférer dans la communication entre deux nœuds A et B afin de récupérer les données lors de leur transfert. De nos jours, les algorithmes cryptographiques peuvent assurer une confidentialité optimale mais sont lourds en termes de mémoire et de calcul. C'est pourquoi il est nécessaire de les adapter par rapport aux contraintes énergétiques des RCSF.

II.1.2 L'authentification

L'authentification est l'un des aspects les plus importants pour les systèmes de sécurité. L'authentification est le fait de pouvoir vérifier et connaître avec une grande certitude l'identité d'un nœud. L'authentification a lieu à plusieurs niveaux : au niveau des parties communicantes, au niveau des messages. Elle pourra être assurée implicitement dans un système à chiffrement symétrique, car dans un tel système, deux entités partagent d'une façon sûre une seule clé secrète. Dans les systèmes asymétriques, l'authentification pourra être assurée lors de l'utilisation d'un certificat d'identification. C'est une relation sûre entre la clé publique et l'identité de l'entité.

II.1.3 L'intégrité

L'intégrité vise à s'assurer que l'information qui transige entre les différents intervenants ne puisse être falsifiée d'aucune façon (ni modifiée, ni altérée, ni détruite). En fait, on veut éviter

qu'un intrus puisse modifier cette information pour en tirer certains avantages et aussi protéger cette dernière des modifications accidentelles.

II.1.4 La disponibilité

Ce service désigne la capacité du réseau à assurer ses services pour maintenir son bon fonctionnement en garantissant aux parties communicantes la présence et l'utilisation de l'information au moment souhaité.

II.1.5 La non-répudiation

C'est le fait qu'aucun nœud ne pourra nier le fait d'avoir participer à l'échange des informations. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

II.1.6 La localisation

L'utilité d'un réseau de capteurs dépend principalement de sa capacité à localiser automatiquement et avec précision chaque capteur dans le réseau. Le but de la localisation (traçabilité) est de garder privé l'emplacement physique des capteurs.

II.2 Les attaques connues dans les RCSF

Les différentes caractéristiques des réseaux de capteurs sans fil (énergie limitée, faible puissance de calcul, et l'utilisation des ondes radio) les exposent à de nombreuses menaces de sécurité. Les RCSF sont plus vulnérables aux attaques que les réseaux filaires puisqu'ils sont déployés dans des fréquences radio ouvertes.

Une classification des attaques consiste à distinguer les attaques passives des attaques actives. Dans les écoutes passives (indiscrètes), le but de l'attaquant est d'intercepter et d'analyser des données sur le réseau sans bousculer son fonctionnement en utilisant une antenne radio. Dans les attaques actives, l'attaquant essaie de modifier les données échangées sur le réseau. Il peut également ajouter son propre trafic et perturber le réseau en provoquant un déni de service.

Les attaques se font sur les différentes couches de communication à savoir : la couche physique, la couche liaison, la couche transport, la couche réseau (routage), la couche application.

II.2.1 La couche physique

- Le brouillage ou jamming

Une attaque bien connue sur la communication sans-fil, est celle qui consiste à perturber le canal radio en envoyant des informations inutiles sur la bande de fréquences utilisées. C'est une attaque de type Déni de Service (DoS) qui vise à perturber la communication. L'adversaire place son antenne proche des nœuds ciblés par l'attaque. La plupart des adversaires préfèrent attaquer

une station qui représente un point de passage obligatoire pour une grande partie du trafic comme un routeur ou une station de base.

Plusieurs techniques peuvent être utilisées pour faire le brouillage : soit en émettant un signal radio sans interruption, soit en émettant régulièrement à intervalle fixe ou de façon aléatoire sur le canal ou soit en émettant que si le signal est actif.

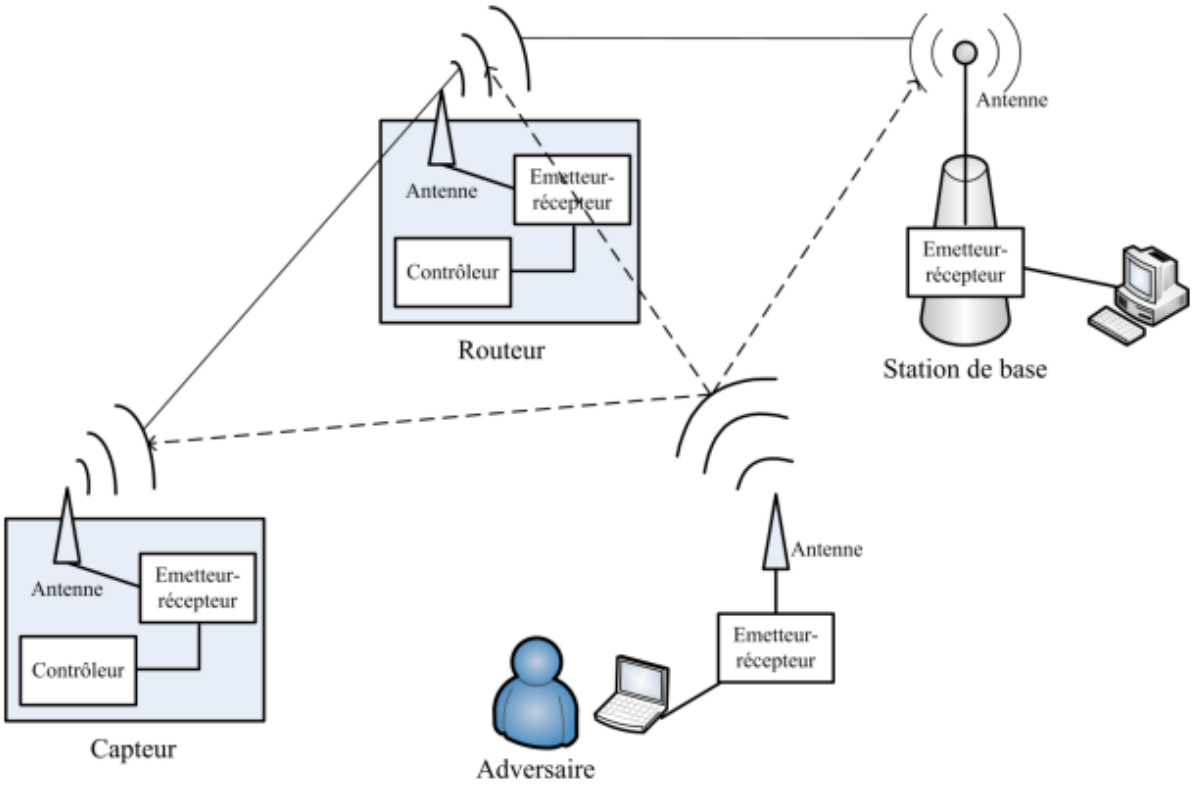


Figure 6 : L'attaque par Jamming [9]

- La falsification ou tampering

Elle consiste à la capture et à l'accès physique au nœud afin d'extraire toutes les informations présentes comme les clés de chiffrement qui peuvent être utilisées pour lancer d'autres attaques. Une telle attaque nécessite un protocole de gestion des clés pour protéger les nœuds.

II.2.2 La couche liaison de données

- La collision

Comparable au jamming, un nœud malveillant peut interférer dans une communication en transmettant un paquet « en sens inverse » pour causer une collision. La collision crée une erreur de contrôle CRC et le message est détruit et une demande de retransmission qui risque d'épuiser

la batterie. En effet, le nœud malveillant cible une trame d'accusé de réception (ACK) dans le but de bloquer ou retarder la communication. La détection d'une telle attaque est difficile car le temps d'attaque est court et les paquets envoyés par le nœud malveillant sont similaires à des paquets normaux.

II.2.3 La couche réseau

- Selective forwarding

Dans cette attaque, un nœud malveillant agira comme un nœud normal en transférant des messages mais va sélectivement jeter certains. Certains nœuds malveillants ou compromis sélectionnent sélectivement les données à transmettre et à ne pas transmettre. Cette attaque peut être très préjudiciable car elle peut empêcher la collecte complète des données et conduire à des résultats inexacts dans les applications de capteurs sans fil.

On peut utiliser un protocole de routage multi-chemins (prochain saut vers la destination aléatoire) pour diminuer la probabilité que le message passe par un nœud malveillant.

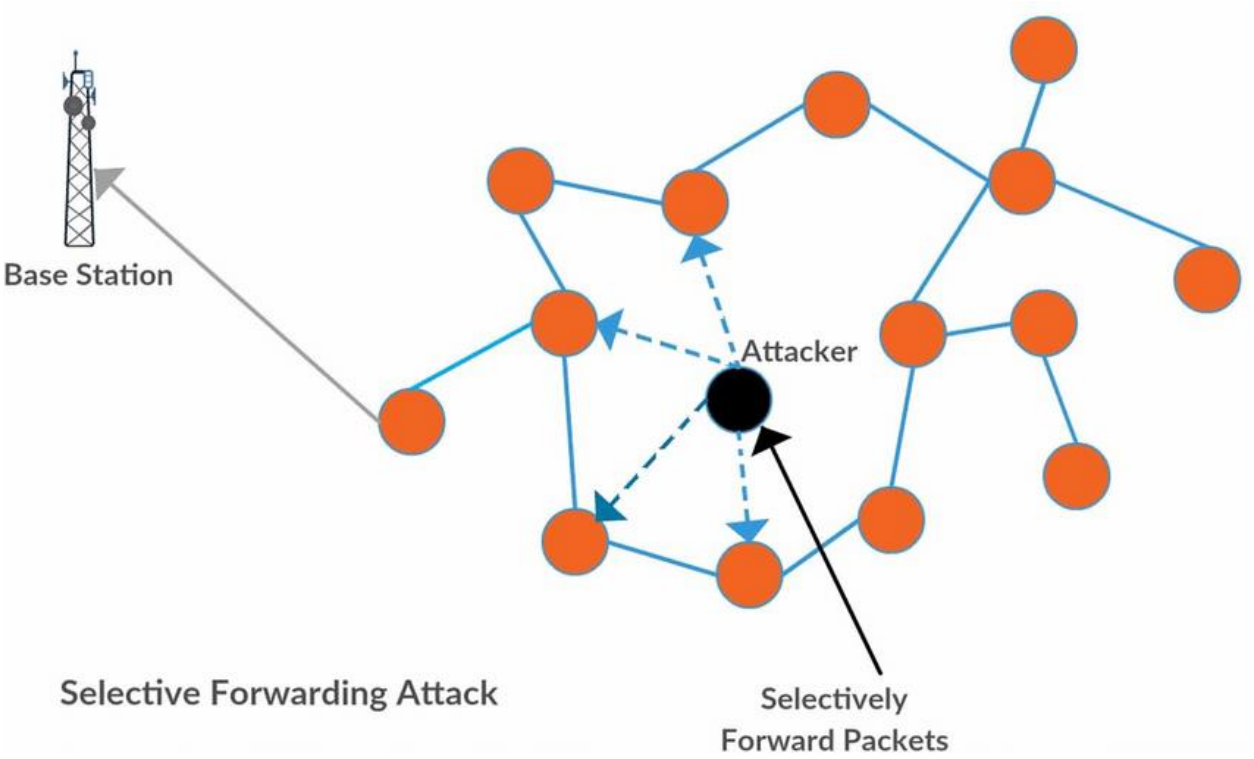


Figure 7 : Attaque par Expédition Sélective [3]

- Sinkhole

L'attaque Sinkhole fait partie de l'ensemble des attaques qui causent un déni-de-service du réseau. Dans cette attaque, le nœud malveillant agit comme une station de base en attirant les paquets vers lui et en les empêchant de continuer leur chemin. L'intention de cette attaque est de créer une fausse station de base et une fausse topologie. Elle exploite le fait que les identités et les liens entre les nœuds ne sont pas vérifiés.

Afin de préserver l'énergie des nœuds, les protocoles de routage dans les RCSF sont souvent basés sur des objectifs comme l'exploitation des chemins avec un minimum de sauts ou un minimum de délai sur les liaisons de bout-en-bout. Les attaques comme Sinkhole exploitent ces propriétés en proposant de faux chemins optimaux aux nœuds du réseau, c'est par ce fait qu'elles attirent les paquets vers un nœud qui va les absorber.

L'attaque par Sinkhole est parfois assimilée à une attaque de type Black Hole (le trou noir) où un nœud malveillant falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou trou noir dans le réseau. Les RCSF dotés d'une station de base sont plus vulnérables à ce type d'attaque.

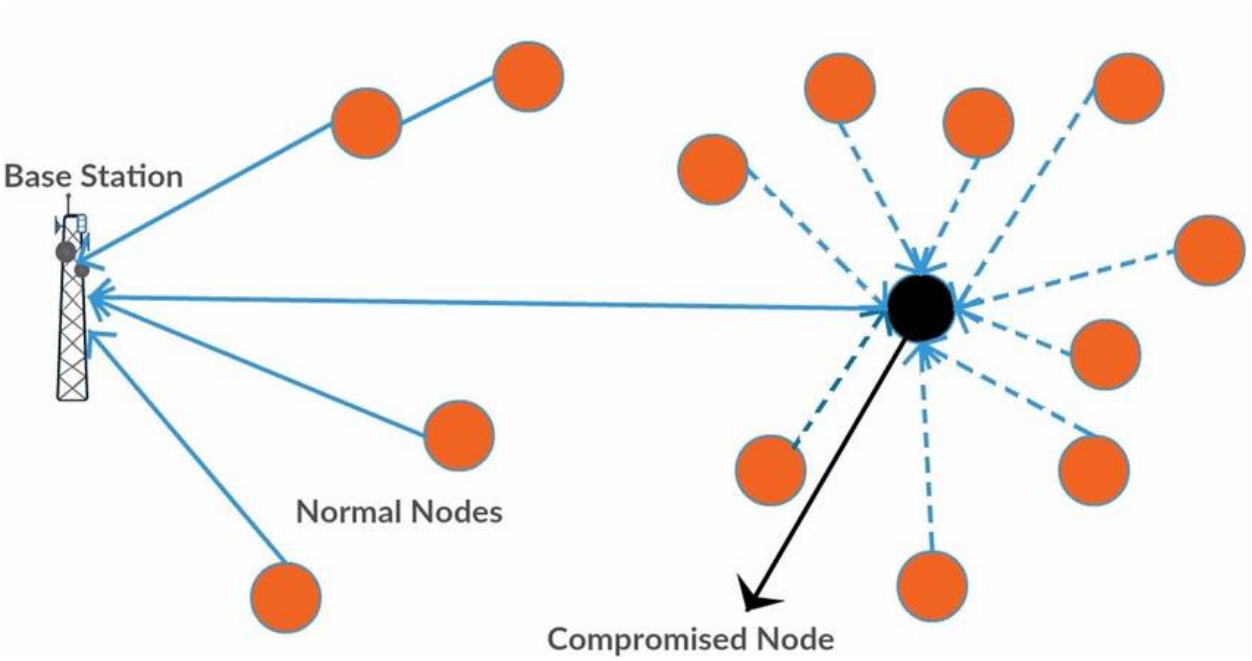


Figure 8 : L'attaque Sinkhole [3]

- Sybil

Un nœud malveillant peut prétendre avoir de multiples identités en utilisant les identités des nœuds ciblés par l'attaque. Cette attaque est localisée entre la couche liaison et la couche réseau. Elle vise à dégrader l'intégrité des données, le niveau de sécurité et l'utilisation des ressources.

Les techniques d'authentification et de chiffrement sont des solutions optimales pour contrer ce type d'attaque.

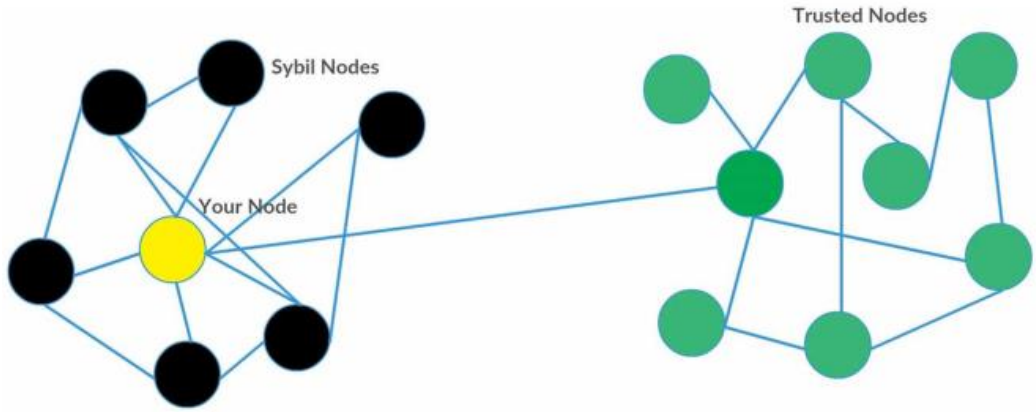


Figure 9 : L'attaque Sybil [3]

- Hello Flood

De nombreux protocoles de routage utilisent des paquets "HELLO" pour découvrir les nœuds voisins et ainsi établir une topologie du réseau. L'attaquant envoie un paquet de type Hello d'un nœud à un autre avec plus d'énergie. Cet attaquant utilise un signal radio à longue portée pour inonder une partie du réseau en provoquant de fausses listes de voisins. Les capteurs recevant ces paquets sont convaincus que l'adversaire est leur voisin, et en conséquence passent par l'attaquant pour envoyer leurs informations à la station de base.

- Wormhole

Dans l'attaque wormhole, appelé *tunneling* ou *trou de ver*, un nœud compromis enregistre les paquets et les envoie via un lien ou tunnel de faible latence vers un autre nœud malicieux dans le réseau.

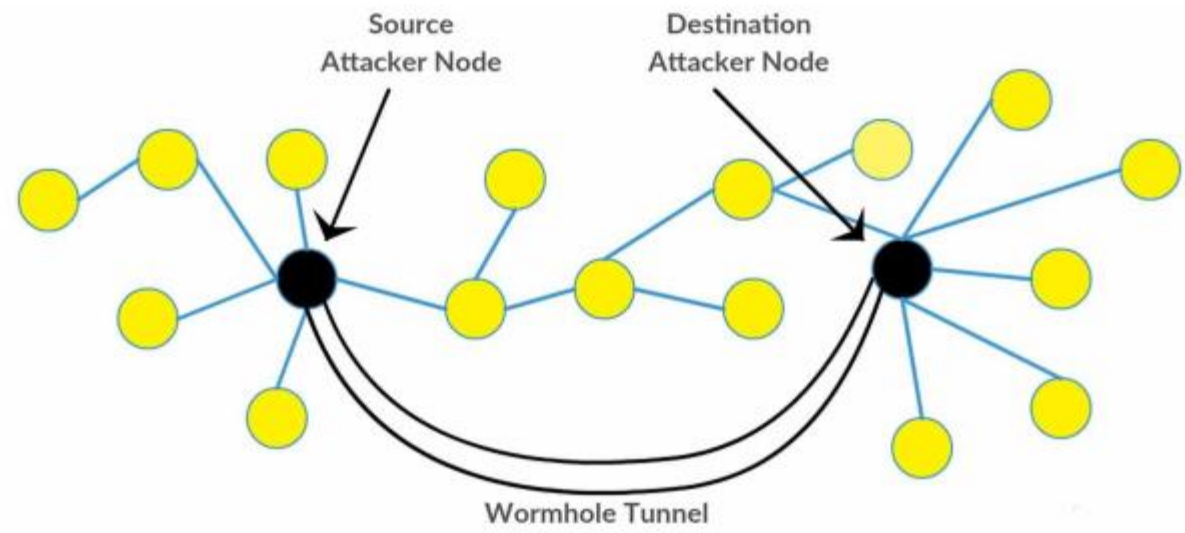


Figure 10 : L'attaque Wormhole [3]

II.2.4 La couche transport

- Désynchronisation

Cette attaque fait partie des attaques d'épuisement de ressources. L'adversaire fait croire à un nœud qu'il n'a pas reçu un certain nombre de paquets en faussant la séquence des paquets réellement échangés. Il suffit d'envoyer successivement aux deux nœuds des messages avec de faux numéros de séquence, ce qui les oblige à rompre leur synchronisation.

L'une des solutions contre cette attaque est d'utiliser un mécanisme d'identification afin de contrôler l'identité et l'intégrité des paquets.

II.2.5 La couche application

- Forced delay

Un nœud malveillant retarde délibérément les paquets à l'intérieur de son élément de transmission afin de retarder la transmission des événements importants. Cette attaque peut être efficacement utilisée pour dégrader la qualité de service des applications dans les systèmes temps réel.

- Submersion attack

Un attaquant peut tenter de submerger les nœuds du réseau avec stimuli de capteur, obligeant le réseau à transférer de gros volumes de trafic vers une station de base. Cette attaque consomme de la bande passante réseau et de l'énergie des nœuds.

II.3 Les contraintes influençant la sécurité d'un RCSF

En général, l'objectif des RCSF est de réunir des données de surveillance et d'agir dans l'environnement. Les nœuds capteurs opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie.

- Puissance d'énergie faible

L'énergie des nœuds de capteur est limitée, et généralement irremplaçable. Les capacités de transmission/réception du nœud capteur sont limitées pour des besoins de conservation d'énergie. La transmission est l'opération la plus couteuse dans les RCSF. La réserve d'énergie de chaque nœud doit être conservé pour prolonger sa durée de vie et ainsi que celle de l'ensemble du réseau.

- Espace mémoire et capacité de calcul limités

Le nœud capteur est doté d'un processeur d'une capacité de calcul très limitée d'où l'exécution impossible d'algorithmes cryptographiques complexes. Également, après le chargement du système d'exploitation, le nœud capteur ne dispose pas suffisamment d'espace mémoire pour le stockage de certaines clés et l'exécution de certains algorithmes.

- Communication sans fils multi-sauts

La communication multi-sauts est indispensable pour la diffusion des données dans un RCSF car la portée de la communication radio des nœuds est limitée en raison de considérations énergétiques. Cela introduit de nombreuses failles de sécurité à deux niveaux différents : attaque de la construction et maintenance des routes, et attaque des données utiles par injection, la modification ou la suppression de paquets. En effet, la communication sans fil introduit d'autres vulnérabilités à la couche liaison en ouvrant la porte à des attaques de brouillage et de type déni de service.

II.4 Analyse de la sécurité et solutions envisageables

II.4.1 Défis de sécurité

Les RCSF sont menacés facilement à cause de l'utilisation de l'air comme moyen de transmission et ont besoin d'être protégés par des méthodes adaptées à leurs applications. Les méthodes de protection comme les algorithmes de chiffrement intégrés dans les protocoles de sécurité sont suffisamment sécurisées pour être utilisés dans les RCSF mais l'effort d'adaptation représente un grand défi.

Basés sur l'analyse sur les buts de sécurité et des attaques dans les RCSF, nous récapitulons les conditions suivantes pour un bon mécanisme de sécurité dans les RCSF :

- Gestion des clés : confidentialité, intégrité, et authentification sont des services critiques permettant d'empêcher un adversaire de compromettre la sécurité d'un RCSF ; la gestion et l'établissement des clés est nécessaire pour assurer cette protection dans les RCSF. L'échange de clés et des informations qui concernent leur création doit être réalisé rapidement puisque les communications passent via les signaux radio et risquent d'être interceptées facilement ;

- Capture physique des nœuds : la nature du déploiement des RCSF pour certaines applications rend les nœuds vulnérables à une capture physique. Il faut faire en sorte qu'un utilisateur ou capteur non autorisé qu'on appellera adversaire ou attaquant, ne réussisse pas à intégrer ou à utiliser les services du réseau de capteurs.

- Ressources énergétiques et capacité de calcul : Le mécanisme doit également prendre en compte les exigences des capteurs en termes de capacité de stockage, de calcul et de transmission. Ainsi, le mécanisme de contrôle d'accès doit minimiser le stockage des clés, les transmissions et utiliser des algorithmes cryptographiques moins coûteux en calcul.

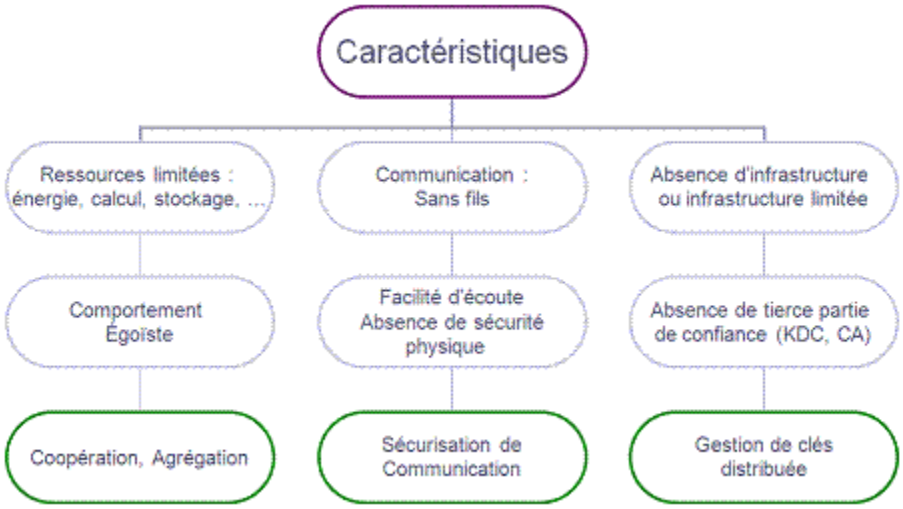


Figure 11 : Contraintes et défis de sécurité des RCSF

II.4.2 La cryptographie dans les RCSF

Dans la plupart des mécanismes de sécurisation actuelle, la cryptographie est certainement la technique la plus utilisée dans le cadre des réseaux filaires et des réseaux sans fil traditionnels disposant d'une capacité de calcul et de mémoire conséquente. Les solutions de cryptographie sont réputées comme des solutions sûres qui répondent à l'ensemble des problèmes liés à la sécurité des données.

La **cryptographie** est une discipline qui se concentre sur la sécurisation de l'information en la transformant de manière qu'elle ne puisse être comprise que par des personnes autorisées. Elle est souvent utilisée pour protéger les données confidentielles, telles que les transactions financières, les informations médicales, les communications militaires et les secrets d'entreprise. Elle implique l'utilisation de techniques mathématiques et informatiques pour coder et décoder l'information. La cryptographie peut être utilisée dans de nombreux contextes différents, y compris la communication sécurisée entre deux parties, le stockage sécurisé de données, l'authentification d'identité et la signature électronique de documents.

Les caractéristiques des réseaux de capteurs, à savoir une faible puissance de calcul et une mémoire limitée auxquelles se rajoute la problématique de conservation de l'énergie, sont des freins considérables à l'utilisation des systèmes cryptographiques courants. La solution consiste à trouver des algorithmes basés sur une cryptographie légère ; tout aussi efficaces en termes de sécurité, de temps d'exécution et de consommation énergétique.

La cryptographie est divisée en deux sous-groupes : la cryptographie symétrique dite à clé secrète et la cryptographie asymétrique ou à clé publique. Il y'a également l'existence du système hybride (qui utilise à la fois les deux types de cryptographie).

II.4.2.1 **Système symétrique**

La cryptographie symétrique dite à clé secrète, nécessite que les deux entités communicantes partagent une clé commune secrète connue seulement d'eux. En raison de sa facilité d'implémentation sur un matériel qui dispose de ressources (mémoire, calcul, énergie) limitées, La plupart des schémas de sécurités destinées aux RCSF utilisent uniquement la cryptographie à clé symétrique.

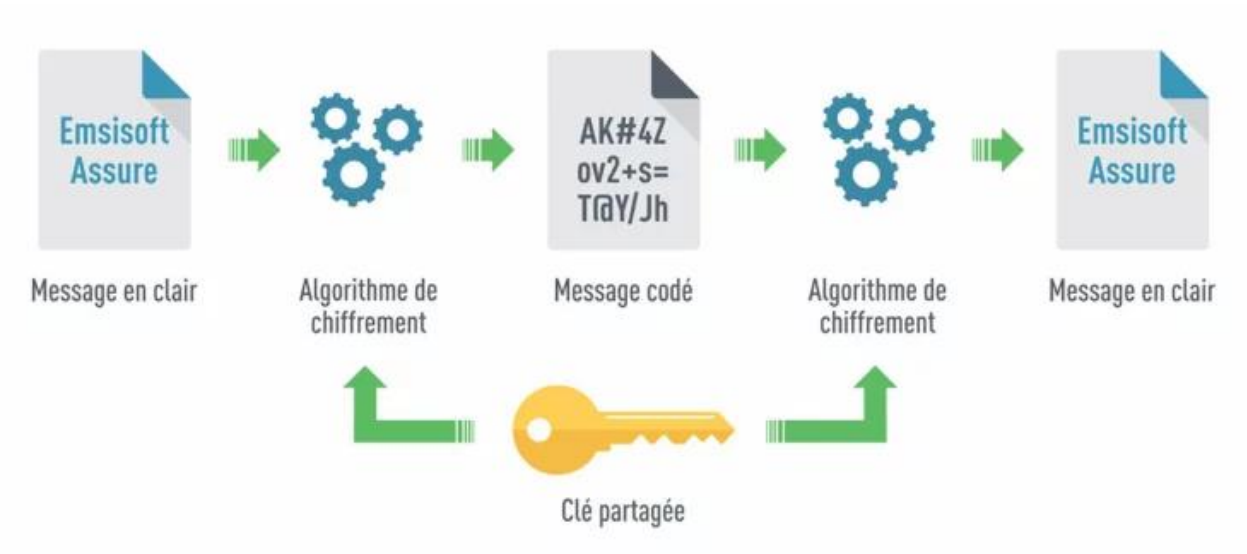


Figure 12 : Chiffrement symétrique [D]

Cependant, si le chiffrement à clé symétrique est possible au sein des réseaux de capteurs, la sécurité totale de ce type de solution reste à démontrer. D'une part parce que le chiffrement a clé symétrique ne garantit pas l'authentification des données comme peut le faire la signature numérique des chiffrements à clés publiques, et d'autre part parce que se pose le problème de la distribution des clés de chiffrement. Ainsi, si le protocole IEEE 802.15.4 spécifie la méthode de chiffrement à utiliser, à aucun moment elle ne spécifie comment doivent être gérées les clés et comment permettre l'authentification des données.

II.4.2.2 **Système asymétrique**

La cryptographie asymétrique, également connue sous le nom de cryptographie à clé publique, est une méthode de cryptage qui utilise deux clés différentes pour chiffrer et déchiffrer des données. Dans ce système, chaque utilisateur dispose d'une paire de clés : une clé publique et une clé privée. La clé publique est partagée avec d'autres utilisateurs pour permettre le chiffrement des données, tandis que la clé privée est gardée secrète par l'utilisateur pour permettre le déchiffrement.

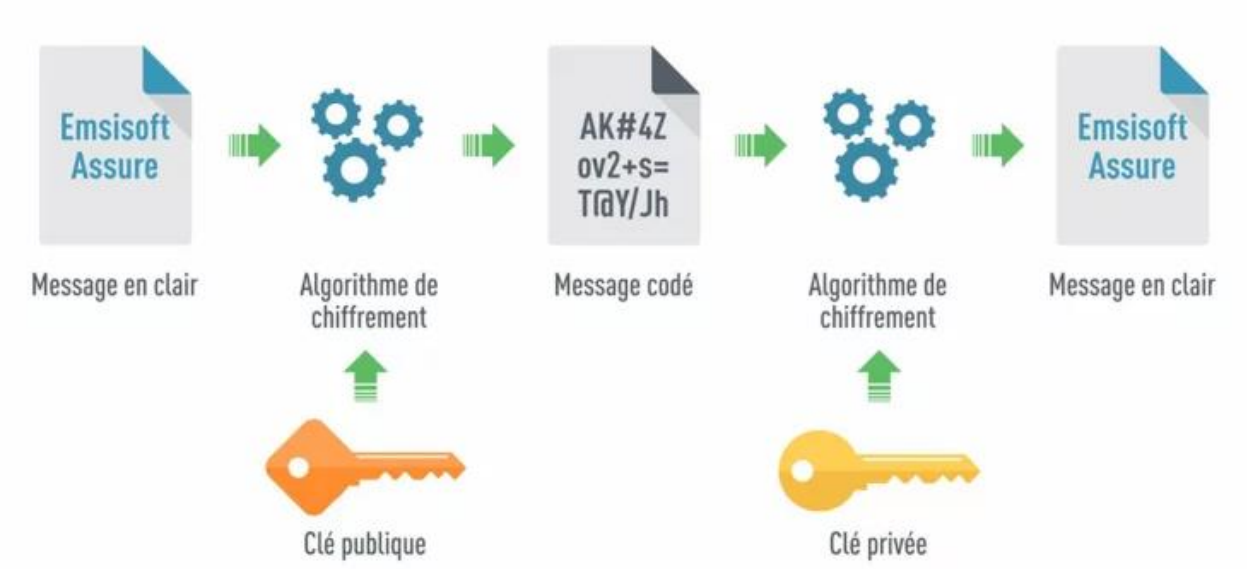


Figure 13 : Chiffrement asymétrique [D]

Elle permet non seulement le chiffrement d'informations mais aussi la garantie d'authentification des auteurs des messages en utilisant la signature numérique à l'aide d'un chiffrement par clé privée et l'utilisation des certificats numériques.

Les mécanismes de cryptographie asymétriques sont potentiellement de bonnes solutions de sécurité quand le nombre de nœuds est très élevé comme les réseaux de capteurs. Ils posent moins de problèmes pour la gestion des clés. Cependant, la cryptographie asymétrique utile à l'établissement de clés partagées entre nœuds n'est pas réaliste. Les demandes en temps de calcul et en mémoire sont si fortes dans ce cas en plus de la nécessité d'une infrastructure centralisée pour la gestion des clés.

II.4.2.3 **Système hybride**

Le chiffrement hybride est une technique de cryptographie qui combine les avantages de la cryptographie symétrique et de la cryptographie asymétrique.

Pour des applications où le besoin est d'échanger beaucoup de données, le chiffrement asymétrique est inutilisable en pratique, parce qu'il consomme beaucoup de temps et de ressources. De ce fait, ce dernier est utilisé seulement pour échanger une clé secrète afin d'utiliser un chiffrement symétrique à la suite.

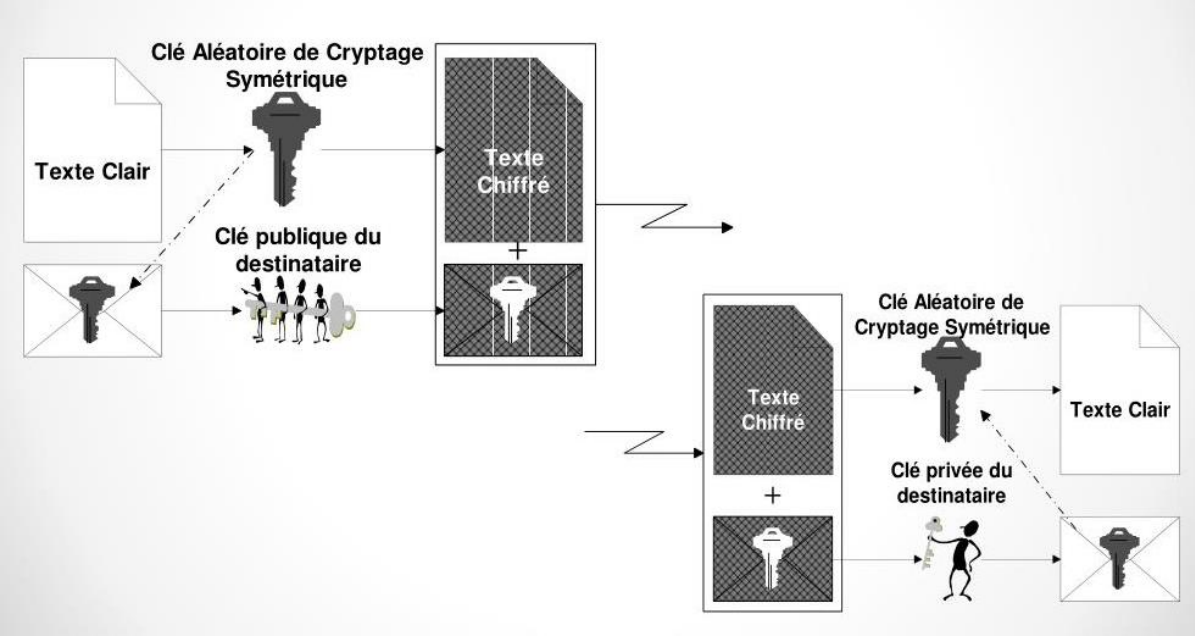


Figure 14 : Chiffrement hybride [E]

II.4.3 Gestion des clés dans les RCSF

L'établissement d'une clé secrète entre deux nœuds ou plusieurs est l'un des services de sécurité le plus important qui assure la confidentialité et l'intégrité des échanges dans un RCSF. Dans les réseaux traditionnels, les méthodes employées dans la gestion des clés sont complexes.

Cependant, fournir une gestion des clés sure dans des réseaux de capteurs est difficile dues à la topologie et aux limitations du réseau de capteurs sans fil et à la dynamique des ressources. Le problème principal est la distribution des clés secrètes entre les parties communicantes pour fournir des propriétés de sécurité telle que le secret et l'authentification.

Afin d'atteindre ce but d'une façon sécurisée, nous avons besoin d'un protocole de gestion de clés qui permet de gérer : (a) la pré-distribution de clés avant le déploiement, (b) l'établissement de clés d'une façon sécurisée après le déploiement, (c) la délivrance, (d) le renouvellement et la (e) révocation des clés pendant toute la durée de vie du réseau. Le protocole doit non seulement intégrer rapidement les nouveaux arrivés en leur délivrant des clés certifiées, mais aussi révoquer les clés des anciens nœuds menacés ou enlevés pour une maintenance.

Il existe dans la littérature des propositions basées sur le système de chiffrement symétrique, le système asymétrique et le système hybride (qui utilisent les deux autres à la fois).

3

ETUDE COMPARATIVE DE QUELQUES TRAVAUX ET ANALYSE DE PERFORMANCE

III.1 Protocoles d'authentification des utilisateurs

L'authentification des utilisateurs dans les réseaux de capteurs sans fil est le processus de vérification de l'identité d'un utilisateur qui souhaite accéder à un réseau de capteurs sans fil. Il est utilisé pour garantir que seules les personnes autorisées peuvent accéder aux données et aux ressources du réseau. Il existe plusieurs méthodes d'authentification des utilisateurs dans les réseaux de capteurs sans fil mais l'authentification par mot de passe est celle qui est la plus utilisée.

Les solutions proposées utilisent la technique d'authentification par mot de passe qu'on peut trouver un peu partout dans différents exemples et applications des réseaux même traditionnels. Certaines de ces solutions utilisent la technique d'authentification par mot de passe faible. Cependant, d'autres solutions centrées sur l'environnement des cartes à puce utilisent la technique d'authentification par mot de passe fort et sont basées uniquement sur les fonctions de hachage et l'opérateur OU exclusif, ce qui facilite leur implémentation dans les RCSF.



Figure 15 : Authentification par mot de passe [F]

La première implémentation basée sur l'authentification par mot de passe fort a été proposée en 2006 par Kirk HM Wong, Juan Zheng et autres. Cette adaptation permet aux utilisateurs légitimes d'accéder au réseau de capteurs selon le fonctionnement suivant. On considère qu'on a un réseau de nœuds avec une station de base qui représente ici la passerelle, des nœuds simples et des nœuds logins. L'utilisateur souhaitant envoyer des requêtes, des données à travers le réseau doit obligatoirement enregistrer ses identifiants (nom d'utilisateur et mot de passe) auprès de la passerelle (ou station de base), s'identifier auprès des nœuds logins qui sont chargés d'authentifier les utilisateurs déjà enregistrés : ceci constitue **l'authentification mutuelle**. Une fois authentifié grâce aux nœuds logins, les utilisateurs pourront accéder aux services dans le réseau. Le protocole d'authentification des utilisateurs comporte trois phases : la phase d'enregistrement, la phase de login et la phase d'authentification.

Beaucoup d'autres travaux plus récents ont suivi également le même principe avec des correctifs apportés au niveau du protocole à cause des vulnérabilités constatées.

III.2 Critères d'évaluation



Figure 16 : Critères d'évaluation des protocoles d'authentification

- La complexité de la communication : les protocoles d'authentification doivent prendre en compte le fait que les nœuds capteurs ont besoin d'espace mémoire pour stocker leurs données et de leur énergie pour assurer leur rôle applicatif.

- T_H : le temps nécessaire pour calculer une fonction de hachage à sens unique,
- T_{XOR} : le temps pour effectuer une opération XOR,
- T_{EXP} : le temps pour calculer une exponentiation modulaire,
- T_{EM} : temps pour exécuter une multiplication scalaire sur la courbe elliptique,
- C_{MH} : le délai de communication multi-sauts entre le LN et la GW,
- *O(1)* : signifie la communication du protocole ne dépend pas de la densité des nœuds.

- La topologie : elle est surtout basée sur le type de nœuds présents dans le réseau qui fait la structure du réseau ; il y'a les nœuds simples et les nœuds logins (LNs) qui font office de chef de cluster d'où l'existence de la topologie plate et celle hiérarchique.

- La scalabilité : ou encore l'évolutivité mesure la flexibilité du protocole en fonction de la taille du réseau, le passage à l'échelle du protocole.

- Le type de clé : symétrique ou asymétrique.

- La résistance aux attaques : résistance contre les attaques les plus fréquentes telles que le Déni de Service (DoS), l'attaque par répétition, attaque par capture de nœud, par usurpation d'identité…

III.3 Comparaison de quelques protocoles

Tableau 1 : Comparaison de quelques protocoles d'authentification

Protocoles (solutions)	*Critères de comparaison*				
	Complexité de communication	Topologie	Scalabilité	Type de clé	Résistance aux attaques
Wong et al. [11]	$7T_H+4T_{XOR}+3C_{MH} = O(1)$	Hiérarchique	Oui	Symétrique	Plus ou moins
Vaidya et al. [2]	$11T_H+4T_{XOR}+3C_{MH} = O(1)$	Hiérarchique	Oui	Symétrique	Oui
Authentification (clé symétrique) [12]	$O(\sqrt{N})$	Plate	Non	Symétrique	Plus ou moins
Authentification robuste [2]	$2nT_H+3T_{EXP} = O(n)$	Plate	Oui	Asymétrique	Plus ou moins
NPCAD [13]	$2T_{EM}+5T_H = O(1)$	Plate	Oui	Asymétrique	Plus ou moins

Ici, on constate que la plupart des clés utilisées sont symétriques étant plus performantes. Le protocole le plus efficace et offrant une bonne sécurité est celui de Vaidya et al. C'est dans ce contexte que nous avons décidé de travailler sur ce protocole. Ayant trouvé la possibilité de l'améliorer, nous proposerons une alternative à ce dernier, pas très différent, mais plus efficace en termes de sécurité.

4

CONTRIBUTION : AMELIORATION D'UN PROTOCOLE D'AUTHENTIFICATION DES RCSF

IV.1 L'authentification par hachage pour sécuriser les RCSF

Dans les réseaux de capteurs sans fil, le hachage (ou "hashing" en anglais) est une technique de traitement de données qui consiste à convertir une entrée de données de taille variable en une sortie de taille fixe, appelée "valeur de hachage" ou "empreinte de hachage". Une fonction de hachage H() applique une série de transformations sur des données en entrée et produit une sortie H(x) plus petite dont la taille peut généralement varier entre 128 et 512 bits selon les algorithmes de hachage.

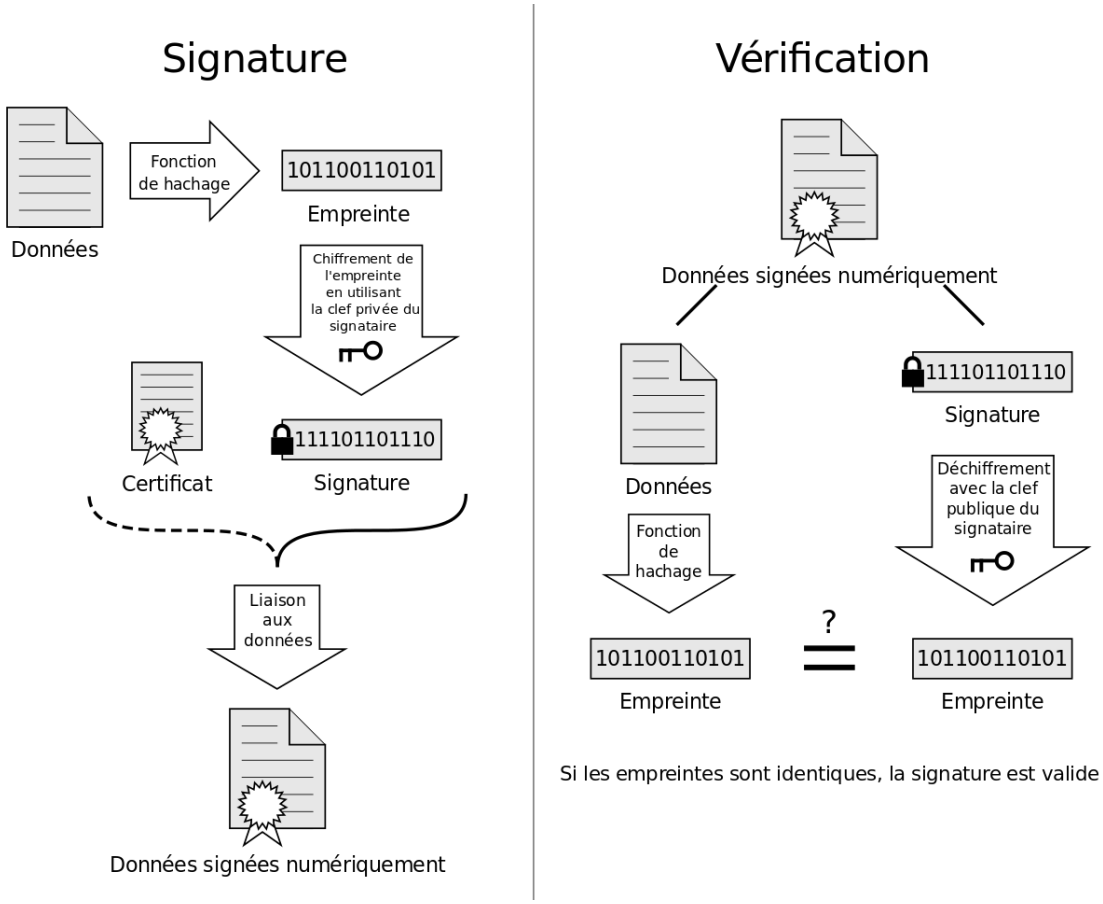


Figure 17 : : Fonction de hachage

En cryptographie, les fonctions de hachage sont surtout utilisées pour optimiser et renforcer les performances des algorithmes de chiffrement et ainsi assurer des services de sécurité tels que le contrôle d'accès (authentification et autorisation) et l'intégrité à travers des relations d'égalité, d'égalité probable, non-égalité etc. Par ailleurs, en cryptographie, la priorité est de sécuriser l'*empreinte* générée par le hachage de toute attaque. Cela nécessite de faire le compromis entre optimisation des ressources et robustesse en termes de sécurité. Ainsi, une fonction de hachage cryptographique est plus exigeante et doit satisfaire un certain nombre de contraintes :

- La résistance aux préimages : il doit être impossible de trouver une donnée d'entrée à partir de son empreinte grâce au caractère de sens unique de la fonction de hachage.

- La résistance aux secondes préimages : il doit être difficile même impossible de trouver pour une empreinte d'une entrée donnée, une autre entrée différente et qui donne la même empreinte.

- La résistance aux collisions : Il doit être difficile, de trouver deux ou plusieurs entrées aléatoires générant la même empreinte. Pour traiter les collisions, la fonction de hachage doit être parfaite, autrement dit, elle doit être mathématiquement une injection de l'ensemble des entrées (ensemble de départ) dans celui des sorties (ensemble d'arrivée).

- La rapidité : Pour une optimisation, normalement le temps de hachage et de chiffrement de l'empreinte doit être inférieur au temps de chiffrement de l'entrée.

IV.2 Description du protocole de Vaidya et Al

Dans cette partie, nous présentons un protocole d'authentification robuste par mot de passe, celui de Vaidya et Al. Contrairement à l'authentification par mot de passe faible, moins coûteuse en stockage mémoire, mais plus coûteuse en calcul (cryptographie asymétrique), cette solution utilise l'authentification par mot de passe fort plus coûteuse en stockage mémoire mais moins coûteuse en calcul (les fonctions de hachage).

La solution de Vaidya et al. [101] est composée de quatre phases : une phase d'enregistrement, une phase de login, une phase d'authentification et une phase de changement de mot de passe. Nous utiliserons pour la suite les notations du tableau suivant.

Tableau 2 : Notations

Symboles	Description
UD	dispositif de l'utilisateur
GW	gateway ou nœud passerelle
LN	nœud login
H()	fonction de hachage à sens unique
$\oplus$	operateur OU exclusif (XOR)
$\|\|$	opérateur de concaténation
Succ_Reg	message d'enregistrement avec succès
Acc_Login	message d'acceptation du login
Succ_Change	message de changement avec succès
x	clé de la passerelle
UID	identité de l'utilisateur
PW	mot de passe choisi par l'utilisateur
TS	temps d'enregistrement d'un nœud
t, T, T_0	temps actuels enregistres par un des nœuds
$\triangle T$	délai de transmission
$\rightarrow$	transmission de message

- 1ère étape : Phase d'enregistrement : durant cette phase, l'utilisateur (UD) est au voisinage de la passerelle GW. Il choisit librement un mot de passe PW et calcule le haché vpw = H(PW). Puis, au temps TS, il envoie son identité UID et le hachage vpw à la passerelle GW en mode sécurisé. Après réception du message, la passerelle GW calcule X = H(UID||x) puis répond à l'utilisateur le message Succ_Reg (X) avec X pour lui notifier que l'enregistrement est effectué avec succès après avoir stocké (UID, vpw, X, TS). L'utilisateur stocke X pour une utilisation future. La GW distribue ensuite les paramètres (UID, X, TS) aux nœuds capteurs de login (LNs) capables de fournir des interfaces aux utilisateurs pour se loguer.

Algorithme : Etapes de la Phase d'Enregistrement (PE)

PE1 - - UD : Calcule vpw = H(PW) ;

PE2 - - UD → GW : UID, vpw ;

PE3 - - GW : Calcule X = H(UID k x) ;

- Stocke UID, vpw, X, TS ;

PE4 - - GW → UD : Succ Reg(X) ;

PE5 - - UD : Stocke X ;

PE5 - - GW →LNs : UID, X, TS ;

PE6 - - LN : Stocke UID, X, TS ;

- 2ème étape : Phase de login : durant la phase de login, l'utilisateur est au voisinage du LN, il calcule A = H(vpw||t), puis soumet (UID, A, t) au LN le plus proche. Après réception de la requête à T_0, le LN vérifie si le UID soumis est non valide et $T_0 - t \geq \triangle T$. Si au moins une condition est vérifiée, le message de login est rejeté, sinon le LN récupéré le paramètre A correspondant et calcule CK = (X ⊕A ⊕ T0), puis il envoie (UID, CK, T_0, t) a la passerelle GW.

Algorithme : Etapes de la Phase de Login (PL)

PL1 - - UD : Calcule A = H(vpw||t) ;

PL2 - - UD → LN : UID, A, t ;

PL3 - - LN : Si UID est valide

- Alors le X correspondant est connu ;

- Sinon rejette le message de login ;

- Si T0 - t≥△T

- Alors rejette le message de login ;

- Sinon récupère A, calcule CK = (X ⊕A ⊕ T0) ;

PL4 - - LN → GW : UID, CK, T0, t ;

- 3ème étape : Phase d'authentification : durant cette phase, la passerelle GW vérifie la validité de UID et t, la requête de login est rejetée s'ils ne sont pas valides. S'ils sont valides, alors la passerelle GW vérifie si T_1-$T_0 \geq \triangle T$ et T_0-$t \geq \triangle T$. Si au moins une des conditions est satisfaite, la requête de login est considérée comme un message répété et est rejetée. Sinon la passerelle récupère le vpw et le paramètre A correspondants, puis calcule A' = H(vpw || t) et C_K' = (X ⊕ A'⊕ T_0). Si $C_K \neq C_K$', le message de login est rejeté, sinon, la GW calcule V_M = H(X||A'||T_1) et envoie un message d'acceptation (Acc_Login, V_M, T_1) au LN. Le LN calcule V'$_M$, et si $V_M = V_M$', il calcule également Y_K = H(V_M || T2) et envoie (Acc_Login, Y_K, T1, T2) à l'utilisateur UD. Apres réception du message au temps T3, l'utilisateur UD vérifie si T_1-$T_0 \geq \triangle T$ et T_0-$t \geq \triangle T$. Si au moins une des conditions est vraie, alors le message Acc login est rejeté, sinon, l'utilisateur

calcule $V''_M = H(X||A||T_1)$ et $Y_K' = H(V''_M || T_2)$, puis vérifie si $Y_K = Y_K'$. Si cette condition est vraie, l'utilisateur UD commence à obtenir les données, sinon le message d'acceptation de login Acc_Login est rejeté.

Algorithme : Etapes de la Phase d'Authentification (PA)

PA1 - - GW : Si UID et t sont valides

- Alors récupère les paramètres (UID, X, TS) ;

- Sinon rejette le message de login ;

- Si $T1 - T_0 \geq \Delta T$ et $T_0 - t \geq \Delta T$

- Alors message de login supposé répété et rejeté ;

- Sinon calcule $A' = H(vpw || t)$;

- calcule $C'_K = (X \oplus A' \oplus T_0)$;

- Si $C'_K \neq CK$

- Alors rejette le message de login ;

- Sinon calcule $V_M = H(X || A' || T_1)$;

- Stocke t ;

PA2 - - GW $\rightarrow$ LN : Acc_Login, V_M, T_1 ;

PA3 - - LN : Si $T_2 - T_1 \geq \Delta T$

- Alors rejette le message de login ;

- Sinon Calcule $V'_M = H(X || A || T_1)$;

- Si $V_M \neq V'_M$

- Alors LN rejette le message de login ;

- Sinon Calcule $Y_K = H(V'_M || T2)$;

PA4 - - LN $\rightarrow$ UD : Acc_Login, Y_K, T_1, T_2 ;

PA5 - - UD : Si $T_1 - T_0 \geq \Delta T$ et $T_0 - t \geq \Delta T$

- Alors rejette le message Acc_Login ;

- Sinon calcule $V''_M = H(X || A || T_1)$;

- calcule $Y'_K = H(V''_M || T2)$;

- Si $Y_K \neq Y'_K$

- Alors rejette le message Acc_Login ;

- Sinon commence à obtenir les données ;

- 4ème étape : Phase de changement de mot de passe : durant la phase de changement de mot de passe, l'utilisateur UD change son mot de passe PW en PW1. Ainsi, il calcule vpw1 = H(PW1) et envoie le triplet (UID, vpw, vpw1) à la passerelle GW en mode sécurisé. La passerelle GW vérifie son UID et vpw, alors met à jour sa base de données. La passerelle envoie ensuite un message de changement effectif avec succès (Succ_Change) à UD en même temps elle distribue les informations de mise à jour à tous les LNs. Après réception, les LNs vérifient la validité du UID avant de mettre à jour leurs données.

Algorithme : Etapes de la Phase de changement de mot de Passe (PP)

PP1 - - UD : Calcule vpw1 = H(PW1) ;

PP2 - - UD → GW : UID, vpw, vpw1 ;

PP3 - - GW : Si UID et vpw existent sur sa liste

Alors met à jour vpw avec vpw1, TS avec TS1 ;

PP4 - - GW → UD : envoie Succ_Change ;

PP5 - - GW → LNs : envoie UID, TS1 ;

- LN : Si UID existe dans sa liste ;

- **Alors** mettre à jour TS avec TS1

IV.3 Vulnérabilités du protocole d'authentification

Le protocole d'authentification proposé par Vaidya et al, même si elle paraît efficace est également vulnérable à bon nombre d'attaques. Nous avons proposé une solution qui consiste à apporter des modifications dans les trois premières phases de ce dernier.

D'abord, au niveau de la phase d'enregistrement, on constate que la topologie de Vaidya et al est conçu de telle sorte que les messages transmis entre les nœuds et/ou la passerelle peuvent faire plusieurs sauts avant d'atteindre la destination. Il serait donc préférable d'avoir une topologie beaucoup plus hiérarchique pour que les nœuds logins soient directement rattachés à la passerelle et éviter qu'un attaquant collecte les données d'enregistrement validées par la passerelle. Cela protègera le réseau de l'attaque par capture de nœuds. Nous montrerons cette proposition par un schéma explicatif.

Ensuite, ce protocole est vulnérable à l'attaque par Déni de Service (DoS) durant sa phase de login. En considérant toujours le scénario de communication de Vaidya et al, la passerelle et les LNs sont la plupart séparés par plusieurs sauts. L'identifiant de l'utilisateur (UID) circule

plusieurs fois dans le réseau. Aussi, durant la phase de login, seuls le UID et le temps t sont vérifiés ; ainsi un attaquant peut intercepter un identifiant et se faire passer pour un nœud légitime en soumettant un faux mot de passe au nœud login qui le retransmettra à la passerelle en passant par tous les nœuds présents sur le chemin. Cela signifie que les nœuds vont transiter de fausses requêtes à travers le réseau ce qui, à la longue va épuiser leur batterie après une perte considérable d'énergie.

Enfin, il faudrait ajouter à la solution proposée le fait qu'un utilisateur n'aura droit qu'à trois sessions pour se connecter afin d'éviter les risques d'épuisement de ressources des nœuds. Après trois tentatives de connexion, les nœuds logins rejettent les requêtes des utilisateurs pour un certain temps (par exemple 5 minutes) afin de pouvoir identifier et arrêter un nœud compromis qui tente d'atteindre le réseau sans autorisation.

IV.4 Solution proposée

Pour la solution proposée, il 'a toujours quatre phases : la phase d'enregistrement, la phase de connexion (login), la phase d'authentification et la phase de changement de mot de passe qui est la seule à ne pas subir de changements avec notre solution.

- 1ère phase : Enregistrement

Dans Vaidya et al, l'utilisateur calcule vpw = H(PW) qu'il envoie avec son identité pour se loguer alors qu'il ne l'utilisera pas après. Il vaudrait mieux choisir son mot de passe et son identité puis les transférer à la passerelle en mode sécurisé. La passerelle, par la suite, hache l'identifiant en calculant X = H(UID || x). Elle notifie le succès de l'enregistrement en répondant à l'utilisateur avec le message Succ_Reg(X). La GW stocke les paramètres (H(PW), UID, X, TS) qu'elle transmet par la suite aux nœuds logins.

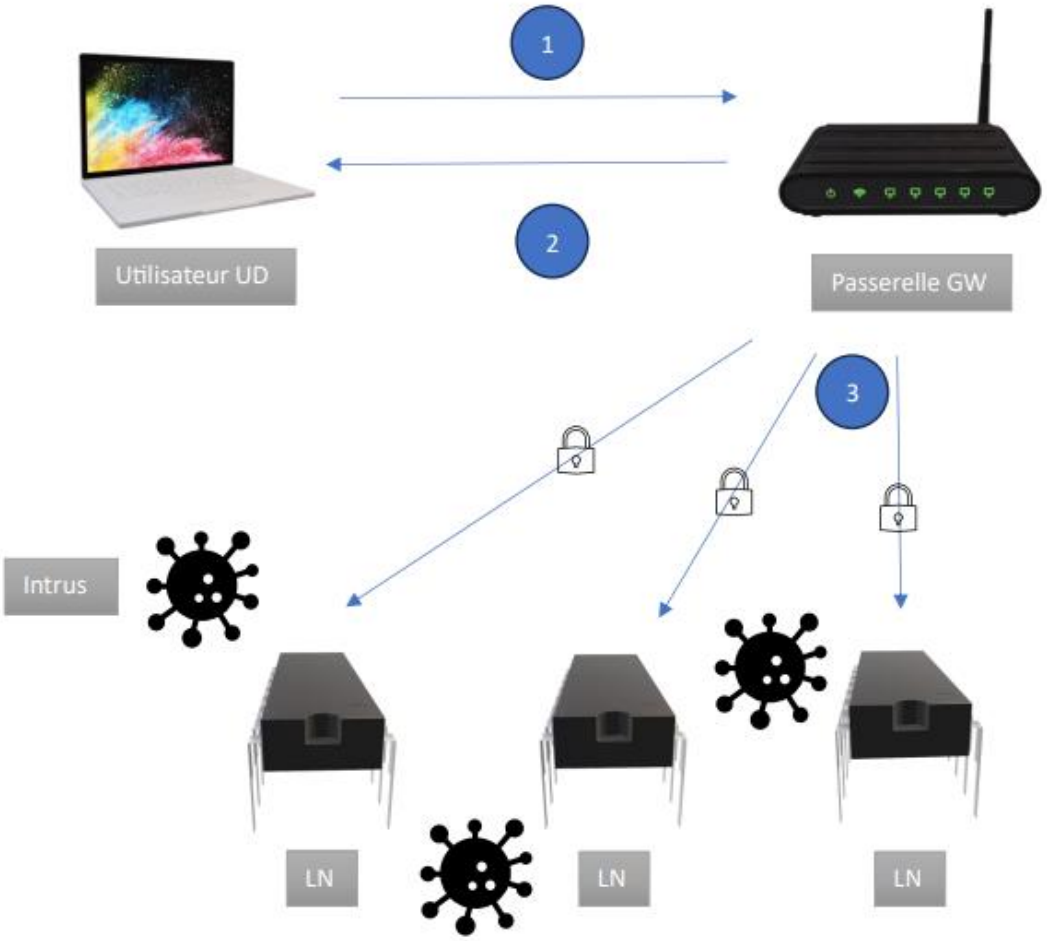


Figure 18 : Phase d'enregistrement

Algorithme : Etapes de la Phase d'Enregistrement (PE)

PE1 - - UD : choisit son mot de passe PW ;

PE2 - - UD → GW : UID, PW ;

PE3 - - GW : calcule X = H(UID || x)

Stocke UID, H(PW), X, TS ;

PE4 - - GW → UD : Succ Reg (X) ;

PE5 - - UD : Stocke X ;

PE6 - - GW → LNs : H(PW), UID, X, TS ;

PE7 - - LN : Stocke H(PW), UID, X, TS ;

- 2ème phase : Connexion

L'utilisateur calcule A= H(H(PW) || t) et envoie (UID, A, t) au nœud login. On initialise le nombre de sessions qu'il a droit et la durée de blocage pour qu'il ne se connecte plus après trois tentatives. Après avoir reçu la requête de l'utilisateur, le LN vérifie si l'identité UID est non valide ou si $A \neq H(H(PW) \| t)$ ou si $T_0 - t \geq \triangle T$. Si c'est le cas, le message est rejeté. Sinon, LN calcule $C_K = (X \oplus A \oplus T_0)$ puis envoie (UID, C_K, T_0, t) à la passerelle GW. Les trois sessions permettent à l'utilisateur qui se trompe sur la saisie de réessayer mais s'il atteint la limite, on se rend compte que c'est un intrus et il est bloqué afin d'éviter de consulter à chaque fois le LN qui perd en énergie.

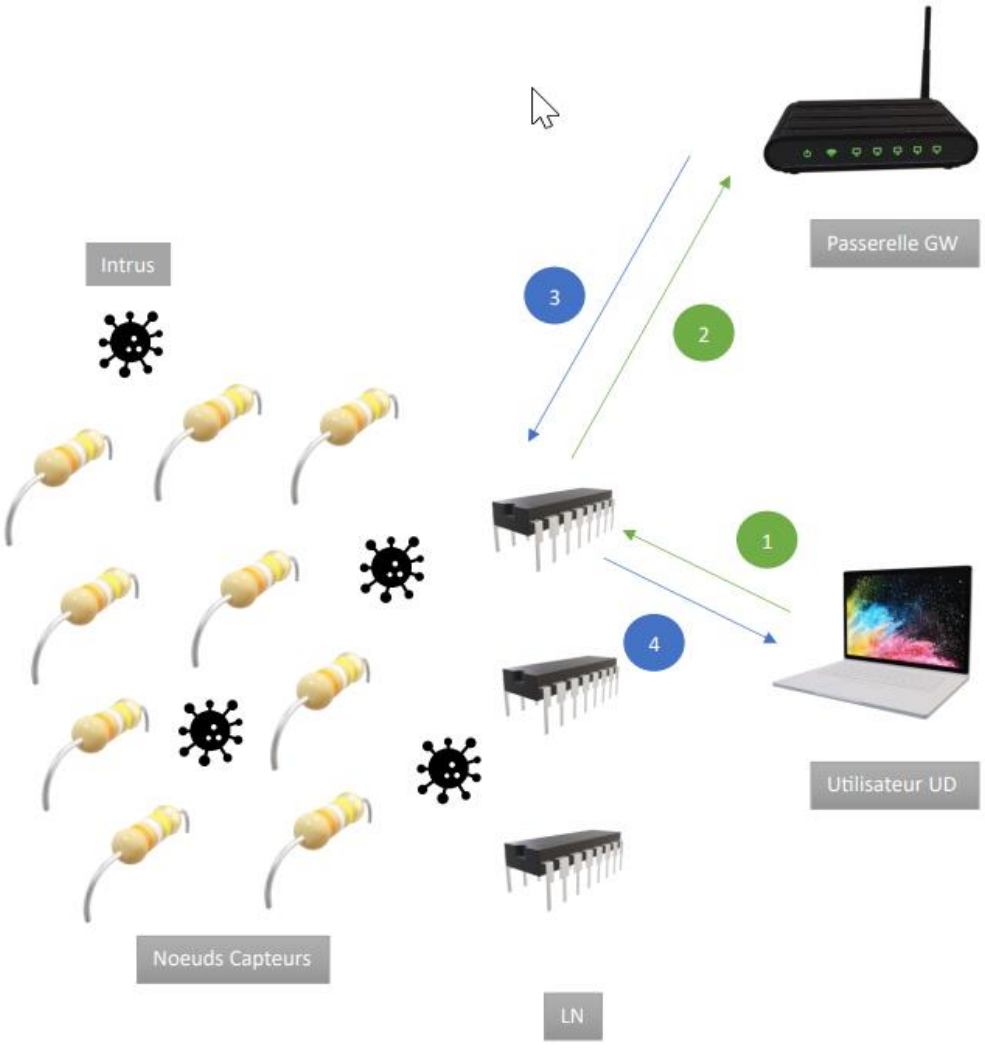


Figure 19 : Phase de Login-Authentification

Algorithme : Etapes de la Phase de Login (PL)

PL1 - - UD : calcule A = H(H(PW) || t) ;

- Sess = 1 ;

- tempsDeBloque = null ;

PL2 - - UD : → LN : UID, A, t ;

PL3 - - LN : Si UID est non valide

- Alors rejette le message de login ;

- Sinon calcule A' = H(H(PW) || t) ;

- Si A ≠ A'

- Alors rejette le message de login ;

- Sinon Si $T_0 - t \geq \triangle T$

- Alors rejette le message de login ;

- Sinon récupère le paramètre A correspondant ;

- calcule $C_K = (X \oplus A \oplus T_0)$;

PL4 - - LN −→ GW : UID, C_K, T_0, t ;

- sess += 1 ;

- Si sess <= 3 ;

- LN vérifie l'utilisateur (UID, A, t) ;

- Sinon tempsDeBloque = temps.actuel + 10 minutes ;

- $3^{ème}$ phase : Authentification

La phase d'authentification est presque la même avec les mêmes étapes sauf au niveau de PA1, la passerelle calcule directement l'empreinte du mot de passe haché H(PW).

Algorithme : Etapes de la Phase d'Authentification (PA)

PA1 - - GW : Si UID et t sont valides

- Alors récupère (UID, X, TS, H(PW)) ;

- Sinon rejette le message de login ;

- Si T1 - $T_0 \geq \triangle T$ et $T_0 - t \geq \triangle T$

- Alors message de login suppose répété et rejeté ;

- Sinon calcule A' = H(H(PW) || t) ;

- calcule $C'_K = (X \oplus A' \oplus T_0)$;

- Si $C'_K \neq C_K$

- Alors rejette le message de login ;

- Sinon calcule $V_M = H(X \| A' \| T_1)$;

- Stocke t ;

PA2 - - GW → LN : Acc_login, V_M, T_1 ;

PA3 - - LN : Si $T_2 - T_1 \geq \triangle T$

- Alors rejette le message de login supposé répété ;

- Sinon calcule $V'_M = H(X \| A \| T_1)$;

- Si $V_M \neq V'_M$

- Alors rejette le message de login ;

- Sinon calcule $Y_K = H(V'_M \| T2)$;

PA4 - - LN → UD : Acc_Login, Y_K, T_1, T_2 ;

PA5 - - UD : Si $T_1 - T_0 \geq \triangle T$ et $T_0 - t \geq \triangle T$

- Alors rejette le message (Acc_Login) ;

- Sinon calcule $V''_M = H(X \| A \| T_1)$;

- calcule $Y'_K = H(V''_M \| T2)$;

- Si $Y_K \neq Y'_K$

- Alors rejette le message (Acc_Login) ;

- Sinon UD commence à obtenir les données ;

- 4ème phase : Changement de mot de passe

Il n'y a pas de changement effectué à ce niveau. Elle est identique à celle de Vaidya et al.

Observations :

Tableau 3 : Comparaison protocoles d'authentification et solution proposée

Protocoles (solutions)	*Critères de comparaison*				
	Complexité de communication	Topologie	Scalabilité	Type de clé	Résistance aux attaques
Solution proposée	15TH+7TXOR+3CMH	Hiérarchique	Oui	Symétrique	Très Bien
Vaidya et al. [2]	$11T_H+4T_{XOR}+3C_{MH} = O(1)$	Hiérarchique	Oui	Symétrique	Oui
Wong et al. [11]	$7T_H+4T_{XOR}+3C_{MH} = O(1)$	Hiérarchique	Oui	Symétrique	Plus ou moins
Authentification (clé symétrique)	$O(\sqrt{N})$	Plate	Non	Symétrique	Plus ou moins
Authentification robuste [2]	$2nT_H+3T_{EXP} = O(n)$	Plate	Oui	Asymétrique	Plus ou moins
NPCAD [13]	$2T_{EM}+5T_H = O(1)$	Plate	Oui	Asymétrique	Plus ou moins

- La solution proposée est légèrement plus coûteuse en termes de consommation énergétique car ayant plus d'opération de hachage et d'opérations OU exclusif mais offre une meilleure sécurité.

- Cette dernière en améliorant le protocole de Vaidya et al offre plus d'efficacité en termes de sécurité, de coût et d'énergie. Comme on l'a dit précédemment, notre solution va permettre d'avoir une structure plus hiérarchisée, également un nœud malveillant sera détecté dès une troisième tentative de connexion (phase de login), ce qui évitera un épuisement d'énergie des capteurs. La solution est efficace donc en termes de coûts de communication et de consommation, compte tenu des ressources limitées des capteurs. Il y a aussi le fait que le réseau est protégé contre un certain nombre d'attaques comme l'attaque par usurpation d'identité et par contournement de nœuds.

CONCLUSION GENERALE

La sécurité est un des enjeux majeurs dans les réseaux de capteurs sans fil en raison de leurs domaines d'applications. Les réseaux de capteurs sont vulnérables contre les attaques externes et internes en raison de leurs caractéristiques uniques, ils sont limités en termes de capacité de calcul, de communication et de mémoire. Le travail consigné dans ce mémoire a été le fruit d'une étude menée dans le contexte des réseaux de capteurs (RCSF en particulier) et ce, relativement au problème de sécurité.

Dans la première partie de notre travail, nous avons fait une étude explicative des réseaux de capteurs sans fil, pour ensuite dans la deuxième partie, aborder la thématique de la sécurité dans ce domaine et les solutions possibles et envisageables dans le contexte des RCSF. C'est dans la troisième partie de notre mémoire que nous avons essayé de faire une comparaison de solutions existantes et enfin d'apporter notre contribution par l'amélioration d'un protocole de sécurité des RCSF dans la dernière partie, à savoir celui de Vaidya et al. ; en proposant une solution que l'on trouve plus efficace et performant en matière de sécurité par rapport aux contraintes de consommation énergétique des RCSF.

Le travail effectué a nécessité plusieurs mois de recherches car le domaine des RCSF étant très large et fastidieux. Notre difficulté majeure a été de déployer notre solution proposée dans sa globalité afin de montrer sa différence et son efficacité par rapport aux autres solutions. Il a été difficile voire impossible de trouver à temps et de comprendre le fonctionnement d'un simulateur assez performant pour effectuer les tests de sécurité que nous voulions implémenter.

Les réseaux de capteurs sans fil constituent un vaste domaine de recherche. En dépit des progrès réalisés dans ce domaine, il y a encore beaucoup de problèmes à résoudre face aux contraintes rencontrées. En perspectives de recherche, nous essayerons d'implémenter ce protocole dans un environnement réel, et éventuellement d'adapter notre proposition à une mobilité des nœuds de capteurs.

BIBLIOGRAPHIE

[1] Pr. Chérif Diallo, “Techniques d’amélioration du routage et de la formation des clusters multi-sauts dans les réseaux de capteurs sans fil. » *Institut National des Télécommunications*, 2010.

[2] Youssou FAYE, « Algorithmes d’authentification et de cryptographie efficaces pour les réseaux de capteurs sans fil. », 2014

[3] Sarika-Choudhary & Nishtha Kesswani, “A Survey: Intrusion Detection Techniques for Internet of Things”, *International Journal of Information Security and Privacy*, January 2019

[4] Messai Mohamed Lamine, « Sécurité dans les Réseaux de Capteurs Sans-Fil », *Université Abderrahmane Mira de Bejaia*, 2008

[5] D.Suneetha & Dr.R.V.Krishnaiah, “Optimal Authentication Scheme for Mobile Communication System”, *International Journal of Information Systems and Computer Sciences*, 2013

[6] Yassine Maleh, Abdellah Ezzati, “Etude et développement d’un protocole symétrique pour sécuriser les communications des RCSF”, *Laboratoire Veille et Technologies Emergente (LAVETE)*, 2015

[7] Hayette Boumerzoug, “Gestion De La Sécurité Dans Les Réseaux De Capteurs Sans Fil”, 2011

[8] Abderrahmane EL AALAOUI, “ Minimisation Avancée de la Consommation d’Energie dans les Réseaux de Capteurs Sans Fil”, 2021

[9] Ismail Mansour, “Contribution à la sécurité des communications des réseaux de capteurs sans fil ”, *Université Blaise Pascal - Clermont-Ferrand II*, 2013

[10] Awatef Ben, Nasri Nejah & Abdennaceur Kachouri, " Contributions à l'optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil", *ResearchGate,* 2013

[11] Kirk HM Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang. "A dynamic user authentication scheme for wireless sensor networks", *IEEE International Conference,* 2006

[12] Satyajit Banerjee and Debapriyay Mukhopadhyay. "Symmetric key based authenticated querying in wireless sensor networks." *In Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*, 2006

[13] Hui-Feng Huang and Kuo-Ching Liu, "A new dynamic access control in wireless sensor networks", *In Asia-Pacific Services Computing Conference*, IEEE, 2008

WEBOGRAPHIE

[A] Réseaux de Capteurs Sans Fils - Anatomie d'un noeud capteur (utc.fr)

[B] Memoire Online - La géolocalisation de réseaux capteurs (algorithme DVHOP) - Mohammed et Hichem MEKIDICHE et RAIS

[C] 2-Domaines d'application des réseaux de capteurs sans fil. | Download Scientific Diagram (researchgate.net)

[D] Coup de projecteur sur les rançongiciels : les modes de chiffrement (emsisoft.com)

[E] PPT - Cryptographie PowerPoint Presentation, free download - ID:2340078 (slideserve.com)

[F] Définition | Mot de passe - Password (futura-sciences.com)