الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

Université Abou Bekr Belkaid
Tlemcen Algérie

جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et systèmes distribués (R.S.D)*

Thème

Implémentation et test d'un protocole de prévention de l'attaque Clone dans un réseau de capteurs sans fil

Réalisé par :

- **Melle KAZI TANI Chahrazad.**
- **Melle BENHADDOUCHE Wiam.**
-

Présenté le 23 juin 2014 devant le jury composé de MM.

- Mr LEHSAINI Mohamed (President)
- Mr BENMAMMAR Badr (Examinateur)
- Mr BENAMAR Abdelkrim (Examinateur)
- Mme LABRAOUI Nabila (Encadreur)

Année universitaire : 2013-2014

REMERCIEMENTS

Si la destination est importante, le parcours ne l'est pas moins. Ces cinq années d'études, nous ont permis de bien comprendre la signification de cette phrase. En effet, le trajet parcouru ne s'est pas réalisé sans défis et sans labeur.

Avant tout, nous remercions Dieu le tout puissant d'avoir été à nos côtés, et de nous avoir donné la force et la patience pour accomplir ce travail.

Au terme de ce travail, nous tenons à remercier, très particulièrement Mme LABRAOUI Nabila d'avoir accepté la lourde tâche d'être la directrice de ce mémoire. Patiente, compréhensive et toujours disponible pour nous aider. Ses conseils et interventions nous ont été d'une grande importance. Nous remercions aussi Mme BOUHAMED Farah pour ses précieux conseils.

Nos remerciements vont aussi aux membres du jury pour l'honneur d'avoir voulu examiner et évaluer cette modeste contribution.

Nos sincères remerciements vont également à tous les enseignants qui nous ont formées durant ces cinq dernières années.

Pour finir, nos dernières pensées vont vers nos familles, et surtout à nos parents, pour les sacrifices et les moyens qu'ils ont mis à notre disposition afin de nous permettre de suivre nos études dans les meilleurs conditions.

DEDICACES

Je voudrais dédier ce modeste travail à toute ma famille et surtout à ma très chère maman qui a veillé ce que je sois ce que je suis devenu maintenant, aucune dédicace ne saurait exprimer l'amour, l'estime et le respect que j'ai toujours eu pour toi. « QUE DIEU TE GARDE et fasse que tu sois toujours fière de moi ».

A mon frère jumeau qui m'a tant soutenu et encouragé dans la vie et surtout pour la réalisation de ce travail.

A mes deux chers grands-parents, la balise qui m'a toujours servie pour braquer sur le quai de réussite.

A mes tantes et mes oncles pour toute l'affection qu'ils m'ont donnée et pour leurs précieux encouragements.

A Mes cousins et cousines et toute ma grande famille.

A mon fiancé pour son soutien, sa compréhension, son attention, sa patience et ces encouragements merci pour tout.

Mon binôme Chahrazad avec qui j'ai partagé de belles années d'études et avec qui j'ai eu l'honneur de les finir.

A mes chers amis partout dans le monde et particulièrement mes amies Sara, Ahlam, Sabéha, Asma et Chahrazad pour tout leur soutien.

A tous ceux qui me sont chers.

Finalement à toute personne que j'ai oubliée de citer son nom, je l'ai fait exprès pour pouvoir écrire ce passage.

Wiam.

DEDICACES

Merci Allah (mon dieu) de m'avoir donné la capacité d'écrire et de réfléchir, la force d'y croire, la patience d'aller jusqu'au bout de mes rêves.

Je dédie ce travail, à tous ceux qui me sont chers,

A m*es parents 'Hami KAZI TANI' & 'Touria BABA AHMED',*

En ma très grande affectation et ma gratitude, Vous vous êtes dépensés pour moi sans compter. En reconnaissance de tous les sacrifices consentis par vous pour me permettre d'atteindre cette étape de ma vie. Vous représentez pour moi le symbole de la bonté par excellence, et l'exemple du dévouement. Aucune dédicace ne saurait exprimer l'amour, l'estime et le respect que j'ai toujours eu pour vous. "QUE DIEU VOUS GARDE et fasse qu'ils soient toujours fiers de moi"

A mon futur mari 'Choukri KAZI AOUAL' pour son soutien, sa compréhension, son attention, sa patience et ses encouragements,

A m*es frères Amine, Nassim et ma sœur Nardjiss qui ont su me guider et être un exemple pour moi,*

A mes belles sœurs 'Lina & Lila' et mon beau-frère 'Ilyes' qui m'ont toujours donnée de bons conseils et soutenus,

A ma *poupée de nièce 'Sonia' et mon cher poupon de neveu 'Anis',*

A t*outes les familles KAZI TANI, BABA AHMED et KAZI AOUAL,*

A m*on amie et mon binôme 'Wiam' avec qui j'ai partagé de belles années d'études et avec qui j'ai eu l'honneur de les finir. A toute sa famille,*

A la mémoire de ma chère grand-mère 'Fatma MESLI' qui a tant attendu ce moment et qui nous a quitté il y a très peu de temps,

A mon encadreur 'Mme Nabila LABRAOUI ',

Enfin je dédie ce travail à tous mes chers amis et professeurs et à tous ceux, qui de près ou de loin ont contribués à la réalisation de mon mémoire de fin d'études.

Chahrazad

RESUME

Souvent déployés dans des environnements sans surveillance, les réseaux de capteurs sans fil peuvent être victimes de plusieurs attaques. L'attaque Clone est l'une des plus dangereuses car non seulement elle passe inaperçue pour le reste du réseau mais elle est en plus le point d'entrée, d'attaques internes qui peuvent avoir des conséquences désastreuses sur le réseau. Pour cela, beaucoup de méthodes et de propositions se sont intéressées pour éviter cette attaque mais l'absence d'une 'solution idéale' fait que plusieurs publications s'y consacrent encore.

Dans ce mémoire, nous présentons un protocole étudié qu'on a choisis qui fait une étude sur la prévention et la détection de l'attaque clone, les résultats d'analyse et d'implémentation ont prouvé l'efficacité de ce protocole et les coûts de communication et de stockage sont compétitifs par rapport aux autres solutions.

Mots clés : réseaux de capteurs sans fil (RCSF), la sécurité dans les RCSF, l'attaque clone.

ABSTRACT

Wireless sensor networks are often deployed in hostile environments, and can be subjected to a multitude of attacks. The clone attack is one of the more insidious because it not only goes undetectable for the rest of the network, but it is the entry point for most internal attacks that can have disastrous consequences on the network.

For this, many methods and proposals are interested to avoid this attack, but the absence of an 'ideal solution' that several publications are still spending. In this thesis, we present a protocol that has chosen that did a study on the prevention and detection of clone attack, the results of analysis and implementation have proven the effectiveness of this protocol and communication costs and storage are competitive compared to other solutions.

Keywords: wireless sensor networks (WSN), security in WSN, Clone attack.

ملخص

شبكات الاستشعار كثيرا ما تنتشر في بيئات معادية مما يعرضها لعدد وافر من الهجمات. الهجوم بالاستنساخ هو أخطرالهجمات، لأنه من جهة لا يمكن ملاحظته من طرف بقية الشبكة و من جهة أخرى هو يعد نقطة الدخول للعديد من الهجمات الداخلية التي يمكن أن يكون لها عواقب وخيمة على الشبكة. ولهذآ الكثير من الطرق و الاقتراحات حظت بالاهتمام لتفادي هدا الهجوم ، ولكن غياب الحل المثالي جعل الكثير من المنشورات تعالج هدا الموضوع.

في هده المدكرة نعرض بروتوكول من اختيارنا الدي يقوم بالدراسة عن الوقاية و الكشف عن الهجمات بالاستنساخ، نتائج التحليل والتطبيق بينت فعالية هدا البروتوكول،وتكاليف الاتصالات والتخزين هي تنافسية بالمقارنة مع الحلول الأخرى.

كلمات البحث: شبكات الاستشعار الاسلكية،الأمن في شبكات الاستشعار الهجوم بواسطة الاستنساخ.

TABLE DES MATIERES

INTRODUCTION GENERALE

Le besoin d'être informé, à tout temps, des évolutions de l'environnement qui nous entoure, a mené l'être humain à perfectionner, chaque fois que c'est nécessaire, les moyens de communication et d'information. L'avènement des réseaux sans fil a élargi considérablement les horizons d'utilisation des équipements de collecte et de transmission des données sans le souci des éléments d'interconnexion classiques comme les câbles.

D'autre part, l'avancé technique a réduit, de plus en plus, la taille et le coût des équipements utilisés. Ainsi, les réseaux de capteurs sans fil ont vu le jour combinant un nombre conséquent de capteurs de faible coût (une zone de couverture très vaste) et un support de transmission fiable.

Les réseaux de capteurs sans fil (RCSF)- Wireless Sensor Networks (WSN) – sont Considérés comme un type spécial de réseaux ad hoc. Les nœuds de ce type de réseaux consistent en un grand nombre de micro-capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. La position de ces nœuds n'est pas obligatoirement prédéterminée. Ils sont dispersés aléatoirement à travers une zone géographique, appelée champ de captage, qui définit le terrain d'intérêt pour le phénomène capté. Les données captées sont acheminées grâce à un routage multi-saut à un nœud considéré comme un "point de collecte", appelé nœud puits (ou sink). Ce dernier peut être connecté à l'utilisateur du réseau via Internet ou un satellite.

En raison du déploiement de ses nœuds en environnements ouverts, de leurs ressources limitées, et la nature broadcast du medium de transmission, les réseaux de capteurs doivent faire face à de nombreuses attaques. Sans mesures de sécurité, un agent malveillant peut lancer plusieurs types d'attaques qui peuvent nuire au travail des réseaux de capteurs sans fil et empêcher leur bon objectif de déploiement. La sécurité est donc une dimension importante pour ces réseaux.

Nous nous intéressons dans ce mémoire à l'une des attaques les plus insidieuses pour les RCSF qui est 'l'attaque clone' ou un attaquant capture un nœud, utilise ses clés

cryptographiques secrètes pour créer plusieurs copies de celui-ci, s'est une attaque qui peut passer inaperçue pour le reste du réseau car le nœud cloné est une copie conforme du nœud légitime, en plus cette attaque peut être le point d'entrée d'attaques internes dangereuses.

Plusieurs recherches se sont intéressées à cette attaque et divers protocoles ont en résulté ainsi que différents articles ont été publiés sur ce sujet. Parmi les premiers protocoles et les plus célèbres, on cite les protocoles de Parno et al. [1] qui ont permis d'introduire la notion de witness et de distribution dans les protocoles de détection des attaques par réplication tout en diminuant la coût de communication et de stockage par rapport à la solution centralisée principalement. Ces protocoles, ont été le point d'inspiration et de référence d'une multitude de protocoles qui ont essayé d'améliorer les rendements et de combler les lacunes.

Nous présentons dans ce mémoire, un protocole proposé par C. Bekara [26], que nous avons choisis pour l'étudier et l'implémenter. C'est un protocole distribué qui repose sur le déploiement par génération et qui fait la prévention de l'attaque clone.

Ce manuscrit est organisé en trois chapitres suivis d'une conclusion générale, à savoir:

Dans le premier chapitre : ***Généralités sur les réseaux de capteurs sans fil(RCSF)***, nous essayons de donner une vue générale sur la notion des capteurs, types de capteurs, de réseaux de capteurs sans fil, leurs caractéristiques et contraintes de conception ainsi que leurs domaines d'applications.

Dans le deuxième chapitre : ***La sécurité dans les réseaux de capteurs***, nous essayons d'aborder l'importance de la sécurité dans les réseaux de capteurs sans fil, en citant quelques attaques les plus connues et les plus dangereuses , en s'intéressant particulièrement sur l'attaque clone qui est la notion principale de notre travail, en expliquant sa gravité sur le réseau , et on termine par l'état de l'art de quelques protocoles centralisés et distribués les plus connus existant de détection pour cette attaque.

Dans le troisième chapitre : ***Implémentation d'un protocole de détection de l'attaque clone,*** nous éxpliquons principallement son fonctionnement , ses hypothéses , son modèle réseau et adversaire , nous citons aussi l'environnement de notre travail et les outils qu'on a utilisés pour faire l'implémentation du protocole étudié, et on termine par donner les couts de

communication et de stockage en mémoire et enfin les scénarios du résultat de notre simulation.

Nous terminons ce travail par une ***Conclusion générale*** dans laquelle nous présentons ce qu'on a appris à travers ce sujet, nous donnons des perspectives envisagées pour ce travail.

Chapitre 1

GENERALITES SUR LES RESEAUX DE CAPTEURS SANS FIL

SOMMAIRE

1. INTRODUCTION

Les progrès récents dans la technologie des systèmes micro-électromécaniques(Micro Electro- Mechanical Systems MEMS), des communications sans fil et de l'électronique numérique ont permis le développement de petits dispositifs peu coûteux, de faible puissance et qui peuvent communiquer entre eux appelés : « capteurs » [6]. Ils coopèrent entre eux pour former une infrastructure de communication appelée réseau de capteurs .Un réseau de capteur sans fil ou RCSF est un type particulier de réseaux mobiles ad hoc ou MANET (Mobile Ad hoc Network) .Il est caractérisé par un grand nombre de micro-capteurs déployés sur une zone géographiquement vaste, afin de collecter et de transmettre des informations sur un évènement ou plusieurs, d'une façon autonome [5]. (Figure1.1). L'affranchissement de la communication par ondes radio a permis à ces réseaux d'être présents dans plusieurs domaines tels que : le secteur industriel mais aussi pour les organisations civiles où la surveillance et la reconnaissance de phénomènes physiques est une priorité. En effet, un réseau de capteurs peut être mis en place dans le but de surveiller une zone géographique plus ou moins étendue pour détecter l'apparition de phénomènes ou mesurer une grandeur physique (température, pression, vitesse...) [3].

Un RCSF est un réseau non filaire et sans infrastructure, comme illustre la figure suivante (Figure1.1) :

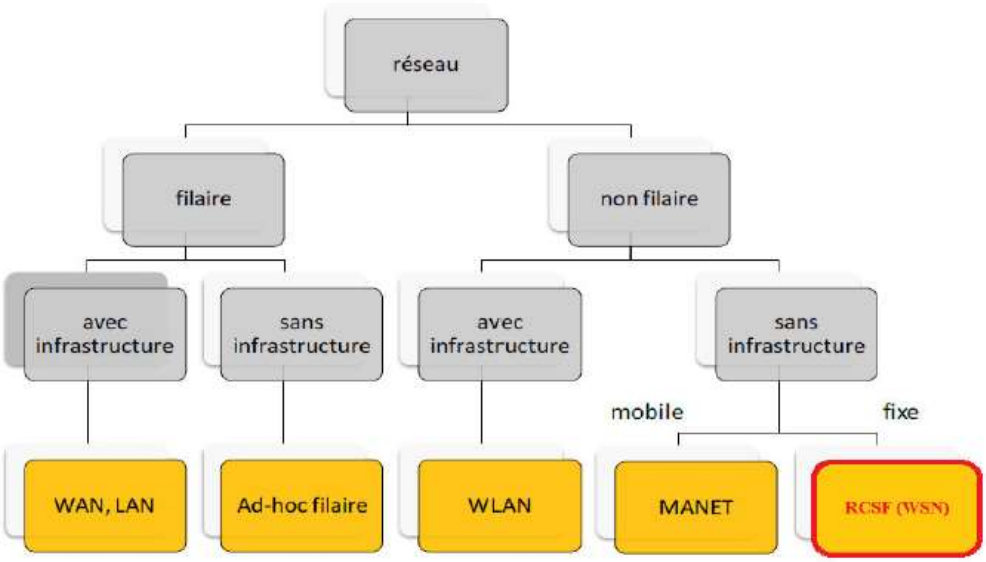

FIGURE 1. 1: CLASSIFICATIONS DES RESEAUX DE COMMUNICATIONS [5]

Nous présentons dans ce chapitre, une présentation sur les réseaux de capteurs, nous allons principalement décrire leurs architectures, composants, modèles, types ainsi que l'architecture de communication, caractéristiques et domaines d'application.

2. NŒUD CAPTEUR

Les capteurs sont de petits dispositifs électroniques « sensors » une sorte de petits calculateurs capable de capter une information, la modifiée, la stockée et la transmettre à une station de base ou à un autre capteur [8].

2.1 ARCHITECTURE D'UN CAPTEUR SANS FIL

Nous distinguons les deux parties qui composent un capteur :

2.2 ARCHITECTURE HARDWARE (MATERIELLE)

Le nœud de capteur est composé principalement de quatre unités: l'unité d'acquisition (de captage), l'unité de traitement (calcul), l'unité de communication (transmission) et une source d'énergie (voir la Figure 1.2) [4].

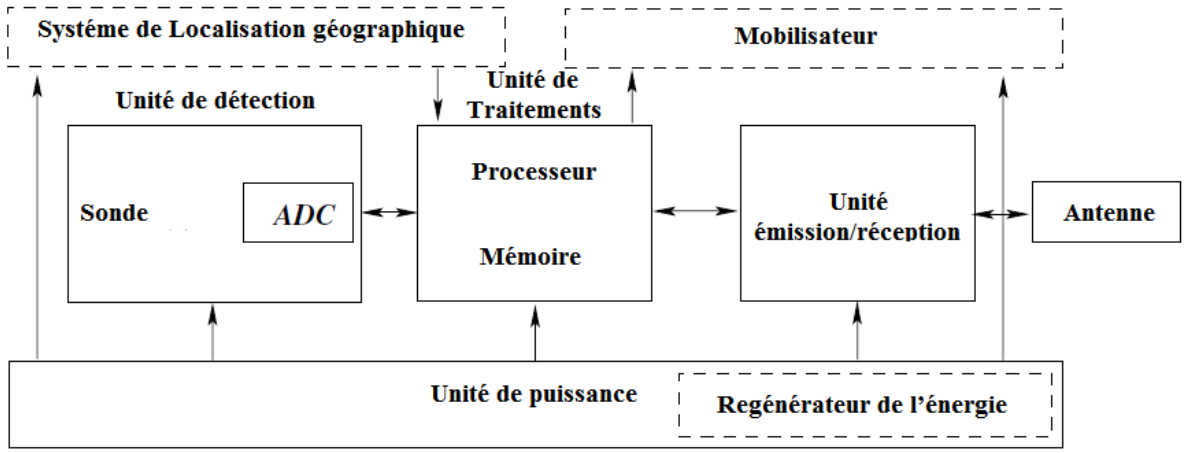

FIGURE 1. 2 : ARCHITECTURE D'UN NŒUD CAPTEUR [5]

Unité de capture (Sensing unit) : composée d'un dispositif de capture physique qui prélève l'information de l'environnement local et un convertisseur analogique/numérique

appelé ADC (Analog to Digital Converter) qui va convertir l'information relevée et la transmettre à l'unité de traitement [4].

Unité de traitement (Processing unit) : est composée de deux interfaces : une interface pour l'unité d'acquisition et une autre pour l'unité de transmission. Cette unité est également composée d'un processeur et d'une mémoire, elle acquiert les informations en provenance de l'unité d'acquisition et les stocke en mémoire ou les envois à l'unité de transmission [2].

Unité de transmission (Transceiver unit) : responsable de la transmission et de la réception des données via un support de communication radio. Ce dernier peut être de type optique (comme dans les capteurs Smart Dust) ou de type radio fréquence (MICA2) [4].

Unité d'énergie (Power unit) : responsable de la gestion de l'énergie et de l'alimentation de tous les composants du capteur (par exemple, en mettent en veille les composants inactifs). Elle consiste généralement en une batterie qui est limitée et irremplaçable, ce qui rend l'énergie comme principale contrainte pour un capteur [2].Notant que la transmission consomme beaucoup d'énergie par rapport à l'unité de calcul.

2.3 ARCHITECTURE SOFTWARE

En plus des plateformes matérielles et des standards, plusieurs plateformes logicielles ont été également développées spécifiquement pour les réseaux de capteurs sans fil. La plateforme la plus répandue est le **TinyOS,** qui est un système d'exploitation open source conçu pour les RCSF [5].

En plus de TinyOS, plusieurs plateformes logiciel et systèmes d'exploitation ont été introduits récemment, comme **LiteOS**ou **CONTIKI** par exemple.

Tandis que plusieurs systèmes d'exploitation avec des capacités supplémentaires sont devenus disponibles, TinyOS est toujours employé couramment dans la recherche sur les RCSF, une des raisons principales de cette popularité est le vaste espace de code établi dans toutes les solutions développées [5].

2.4 TYPE DE CAPTEURS

Il existe actuellement un grand nombre de capteurs, avec des fonctionnalités diverses et variées. La plupart des capteurs dépendent de l'application pour laquelle ils ont été conçus (capteurs aquatiques, sous-terrain, etc.) [14].

Depuis un peu plus de 10 ans, la technologie des capteurs sans fil a beaucoup évoluée. Les modules deviennent de plus en plus petits et les durées de vie prévues augmentent. Aujourd'hui, le marché de nœuds a été ouvert à l'industrie. Le fournisseur le plus connu est *Crossbow Inc*. avec son offre de capteurs Mica2 et MicaZ [1] (Figure 1.3).

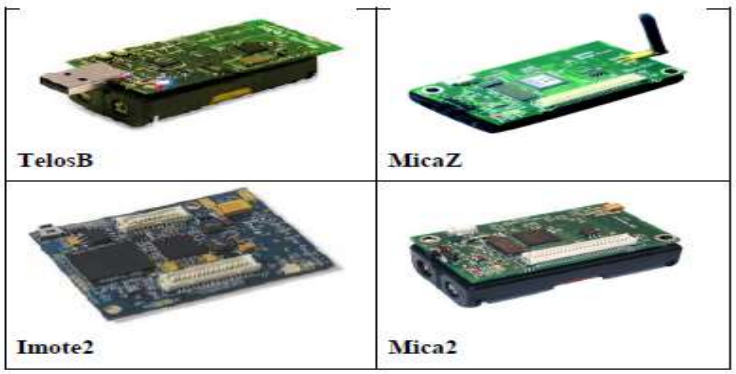

FIGURE 1. 3 : QUELQUES MODELES DE CAPTEURS SANS FIL [1]

2.5 CARRACTERISTIQUES PRINCIPALES D'UN CAPTEUR

Deux entités sont fondamentales dans le fonctionnement d'un capteur: l'unité d'acquisition qui est le cœur physique permettant la prise de mesure et l'unité de communication qui réalise la transmission de celle-ci vers d'autres dispositifs électroniques. Ainsi, chaque capteur possède un rayon de communication (Rc) et un rayon de sensation (Rs).

La Figure 1.4 montre les zones définies par ces deux rayons pour le capteur. La zone de communication est la zone où le capteur peut communiquer avec les autres capteurs. D'autre part, la zone de sensation (ou de détection) est la zone où le capteur peut capter l'événement [7].

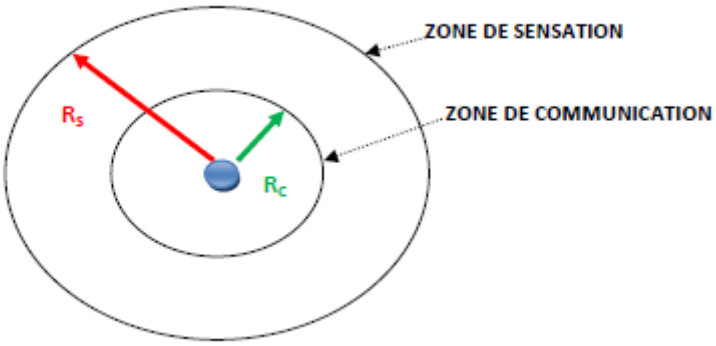

FIGURE 1. 4: RAYONS DE COMMUNICATION ET DE DETECTION D'UN CAPTEUR [7]

3. RESEAUX DE CAPTEURS SANS FIL

3.1 DEFINITION

Un RCSF est composé d'un ensemble de nœuds capteurs. Ces nœuds capteurs sont organisés en champs « sensor Fields » (voir figure 1.5). 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 [13].

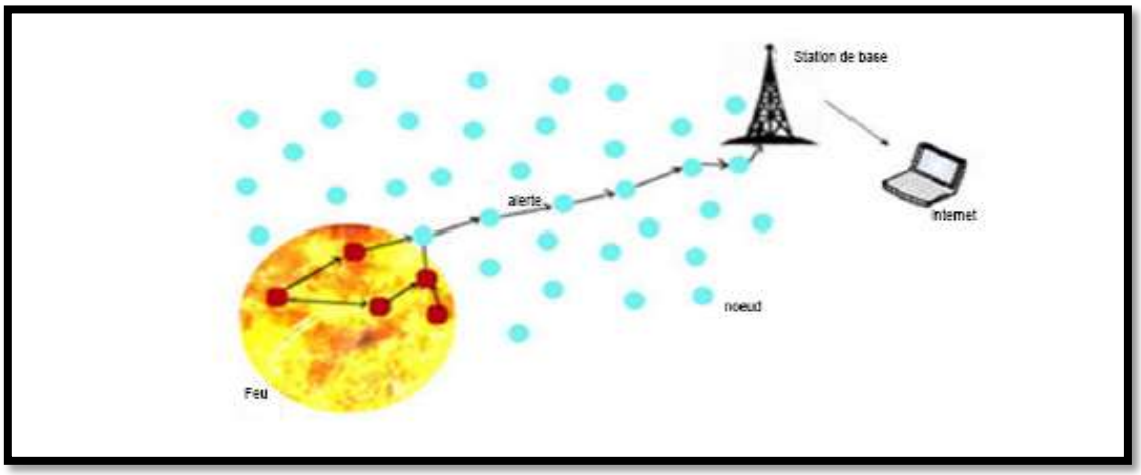

FIGURE 1. 5 : ARCHITECTURE D'UN RCSF : EXEMPLE D'UNE APPLICATION DE DETECTION DE FEU DE FORET [15]

4. DOMAINES D'APPLICATION DES RCSF

La miniaturisation des micro-capteurs, le coût de plus en plus faible et la large gamme de capteurs disponibles (thermique, optique, vibrations, etc.) ainsi que le support de communication sans fil utilisé, permettent l'utilisation des réseaux de capteurs dans plusieurs domaines parmi lesquels [2] :

- ✓ **Domaine militaire**

Comme pour de nombreuses autres technologies, le domaine militaire a été le moteur initial pour le développement des réseaux de capteurs. Le déploiement rapide, le coût réduit, l'auto-organisation et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Actuellement, les RCSF peuvent être une partie intégrante dans le commandement, le contrôle, la communication, la surveillance, la reconnaissance, etc.

- ✓ **Domaine médical**

Les réseaux de capteurs sont également largement répandus dans le domaine médical. Cette classe inclut des applications comme : fournir une interface d'aide pour les handicapés, collecter des informations physiologiques humaines de meilleure qualité, facilitant ainsi le diagnostic de certaines maladies, surveiller en permanence les malades et les médecins à l'intérieur de l'hôpital.

- ✓ **Domaine architectural**

Transformation des bâtiments en environnements intelligents capables de reconnaitre des personnes, interpréter leurs actions et y réagir.

- ✓ **Domaine environnemental**

Dans ce domaine, les capteurs peuvent être exploités pour détecter les catastrophes naturelles (feux de forêts, tremblements de terre, etc.), détecter des émanations de produits toxiques (gaz, produits chimiques, pétrole, etc.) dans des sites industriels tels que les centrales nucléaires ou pétrolières.

- ✓ **Domaine commercial**

Parmi les domaines dans lesquels les réseaux de capteurs ont aussi prouvé leur utilité, on trouve le domaine commercial. Dans ce secteur nous pouvons énumérer plusieurs applications comme : la surveillance de l'état du matériel, le contrôle et l'automatisation des processus d'usinage, etc. [2].

- ✓ **L'industrie**

Les industriels s'intéressent au potentiel des capteurs pour diminuer les coûts du contrôle et de la maintenance des produits, de la gestion de l'inventaire et de la télésurveillance après-vente. En particulier, l'intégration de la technologie RFID avec les réseaux de capteurs est une des directions prometteuses de recherche dans l'industrie [1].

- ✓ **Les domaines urbains et domotiques**

Les capteurs entrent de plus en plus dans nos vies quotidiennes. Dans le milieu urbain, les capteurs sont déjà utilisés pour la localisation des bus, pour des tickets électroniques et pour la sécurité. Une des applications est la surveillance du trafic routier avec les réseaux de capteurs déployés sur les autoroutes. De plus, les maisons, les bâtiments, les bureaux équipés de capteurs intelligents permettent de construire des systèmes où l'information est omniprésente [1].

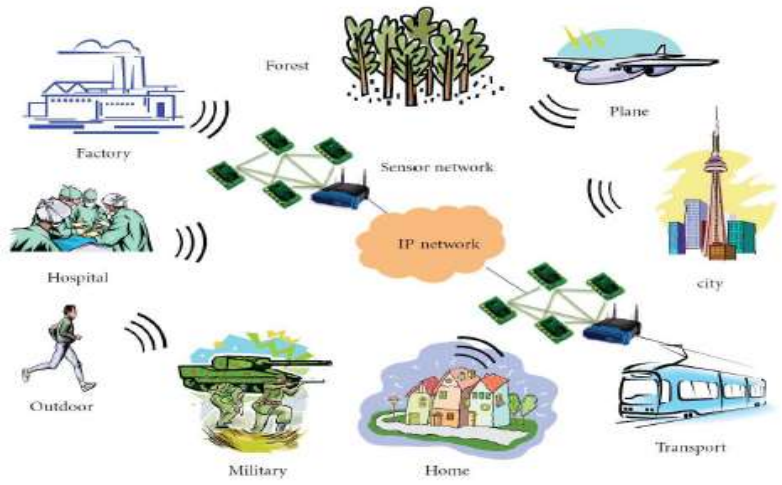

FIGURE 1. 6 :QUELQUES DOMAINES D'APPLICATION POUR LES RCSF[11]

5. CARACTERISTIQUES ET CONTRAINTES DE CONCEPTION D'UN RCSF

La conception et la mise en place des RCSF sont influencées par plusieurs contraintes qui peuvent être des contraintes conceptuelles ou matérielles. Ces facteurs importants servent comme directives pour le développement des algorithmes et protocoles utilisés dans les réseaux de capteurs ; ils sont considérés également comme métriques de comparaison de performances entre les différents travaux dans le domaine [11].

5.1 CONTRAINTES CONCEPTUELLES

La conception des RCSF, leurs protocoles et algorithmes sont guidés par plusieurs facteurs :

- ***La tolérance aux pannes***

La défaillance ou le blocage de certains nœuds dans un réseau de capteurs peut être engendrés par plusieurs causes, notamment l'épuisement d'énergie, l'endommagement physique ou les interférences liées à l'environnement. Ces problèmes ne devraient pas affecter le reste du réseau. C'est le principe de la tolérance aux pannes.

- ***L'extensibilité (passage à l'échelle)***

L'une des caractéristiques des RCSF est qu'ils peuvent contenir des centaines voire des milliers de nœuds capteurs. Suivant l'application, ce nombre peut encore augmenter jusqu'à des millions de capteurs. Les nouveaux schémas doivent pouvoir garantir un bon fonctionnement avec ce nombre élevé de capteurs. Ils doivent aussi exploiter la nature fortement dense des réseaux de capteurs.

- ***Environnement***

Les nœuds capteurs doivent être conçus d'une manière à résister aux différentes et sévères conditions de l'environnement : forte chaleur, pluie, humidité…

- ***Média de transmission***

Les nœuds communicants sont reliés sans fil. Ce lien peut être réalisé par radio, signal infrarouge ou un média optique [11].

- ***Contrainte d'énergie, de stockage et de calcul***

La caractéristique la plus critique dans les réseaux de capteurs est la modestie de ses ressources énergétiques car chaque capteur du réseau possède de faibles ressources en termes d'énergie, de calcul et de stockage. Afin de prolonger la durée de vie du réseau, une minimisation des dépenses énergétiques est exigée chez chaque nœud [12].

- ***Agrégation de données***

Dans les RCSF, les données produites par les nœuds capteurs voisins sont corrélées spatialement et temporellement. Ceci peut engendrer la réception par la station de base d'information redondante. Réduire la quantité d'informations redondantes transmises par les capteurs permet de réduire la consommation d'énergie dans le réseau ainsi d'améliorer sa durée de vie. L'une des techniques utilisée pour réduire la transmission d'informations redondantes est l'agrégation des données, appelée aussi fusion des données.

5.2 CONTRAINTES MATERIELLES

Parmi les contraintes matérielles liées aux RCSF, on peut citer :

- ***Dimension***

La taille réduite des capteurs peut présenter de nombreux avantage, elle permet un déploiement flexible et simple du réseau. Cependant, la puissance des batteries utilisées pour alimenter les nœuds capteurs est limitée par la petite taille de ces derniers.

- ***Puissance de calcul***

Les processeurs des réseaux de capteurs sont différents de ceux d'une machine classique car ils utilisent souvent des microcontrôleurs de faibles fréquences [11].

6. CONCLUSION

Nous avons présenté dans ce chapitre quelques définitions de base sur les RCSF ainsi que leurs domaines d'applications. Les réseaux de capteurs sans fil ne cessent de prendre une place très appréciée au sein de la communauté de recherche vu leurs déploiement assez simple et leurs applications qui se développent chaque jour pour élargir leurs horizons. Initialement, réservés pour les applications militaires, les RCSF ont réussi à conquérir d'autres domaines civils plus larges et plus pratiques changeant le quotidien des êtres humains. Cependant, les contraintes relatives au hardware du capteur, l'élément clé du réseau rendent la conception du réseau une tâche difficile, et nécessite beaucoup de travail sur le volet des softwares [5].

Dans le chapitre suivant, nous allons aborder le problème de la sécurité en mentionnant quelques attaques dans les RCSF et plus précisément l'attaque clone.

Chapitre 2

LA SECURITE DANS LES RESEAUX DE CAPTEURS SANS FIL

SOMMAIRE

1. INTRODUCTION

Parmi les caractéristiques majeures des nœuds de capteurs, nous distinguons la limitation de leurs ressources en termes de capacité de calcul, d'espace de stockage des données et la faible portée radio. Les ressources limitées de ces nœuds et les environnements hostiles dans lesquels ils pourraient être déployés, rendent ce type de réseaux très vulnérable aux attaques. Dans ce contexte, une grande communauté de chercheurs tente de proposer des mécanismes de sécurité pour la prévention et la détection de tout type d'attaque, en tenant compte des contraintes de ce type de réseaux [4].

La conception des applications citées dans le premier chapitre suppose que tous les nœuds engagés sont coopératifs et dignes de confiance. Cependant, ceci n'est pas le cas dans les déploiements du monde réel, où les nœuds sont exposés à différents types d'attaques qui peuvent carrément endommagé le bon fonctionnement du réseau. Ces attaques exploitent essentiellement l'incertitude du canal de communication et le déploiement aléatoire des nœuds capteurs dans des zones difficiles à surveiller.

Garantir la sécurité de ce type de réseau est une tâche difficile. Le cas échéant, utiliser des protections physiques est dans beaucoup de situations quasiment impraticables. Capturer des nœuds est alors une possibilité intéressante pour les attaquants [1].

Dans ce chapitre nous allons passer en revue les différentes attaques contre les réseaux de capteurs sans fil, et plus particulièrement l'attaque clone (attaque par réplication).

2. OBJECTIFS DE SECURITE DANS LES RCSF

La sécurité des informations transitant dans les RCSF doivent répondre à plusieurs prés requis :

Disponibilité du réseau : Le réseau doit pouvoir être disponible à tout instant, c'est à dire que l'envoi d'information ne doit pas être interrompu, de même que la circulation de l'information ne doit pas être stoppée [16].

Cette propriété reste difficile à assurer dans les RCSF étant donné les contraintes qui pèsent sur ces réseaux, à savoir : topologie dynamique, ressources limitées des nœuds de transit ainsi que des communications sans fil pouvant être facilement brouillées ou perturbées [1].

Authentification : L'authentification des capteurs est nécessaire pour s'assurer que l'identité déclarée par un capteur est bien celle du capteur déclarant. En l'absence d'un mécanisme permettant d'authentifier clairement un nœud du réseau, de nombreuses attaques peuvent se mettre en place comme l'attaque Sybil [16].

Intégrité des données : Les données circulant sur le réseau ne doivent pas pouvoir être altérées au cours de la communication. Il faut donc s'assurer que personne ne puisse capturer et modifier les données du réseau. De la même manière il faut vérifier que les données n'ont pas subi d'altération due à un disfonctionnement du matériel, qui est un risque important sur des capteurs sensibles aux altérations d'états [16]. L'intégrité peut être assurée par l'utilisation des fonctions de hachage cryptographiques qui permettent d'obtenir pour chaque message une empreinte numérique [1].

La confidentialité : la confidentialité reste un point important, étant donné la communication sans fil des RCSF. Elle consiste à préserver le secret des messages échangés et ne pas les révélés aux adversaires. La confidentialité peut être assurée par l'usage de la cryptographie à clé symétrique ou asymétrique [1].

Fraîcheur des données : la fraîcheur des données permet de savoir si la donnée est récente ou non. Cela signifie qu'il faut s'assurer que la donnée transmise correspond à un état présent. La fraîcheur des données garantit ainsi que ces données ne reflètent pas un état passé qui n'a plus cours [17].

Auto organisation : Les capteurs du réseau doivent être capables, après avoir été déployés, de s'auto organiser et surtout de se sécuriser eux-mêmes, sans autres interventions extérieures [17].

Localisation sécurisée : Le besoin de se localiser et de connaître la position des autres nœuds peut être primordial dans de nombreux cas pour déjouer d'éventuelles attaques jouant sur les distances [16].

3. LES ATTAQUES DANS LES RCSF

Nous décrivons dans cette section, une liste non exhaustive mais représentative des attaques les plus courantes, actives ou passives, que nous pouvons trouver dans les RCSF.

ECOUTE PASSIVE: cette attaque consiste à écouter le réseau et à intercepter les informations circulant dans le medium sans modifier les données ou le fonctionnement du réseau. Elle est difficile à détecter.

ANALYSE DU TRAFIC: c'est une attaque qui met en jeu des mécanismes d'écoute passive et de surveillance du réseau [16]. L'analyse du trafic peut permettre à un attaquant de connaître la position des stations de base ou des nœuds d'agrégation de données en repérant les lieux où le plus grand nombre de paquets transitent [17].

Brouillage radio : Un attaquant utilise les même fréquences qu'un RCSF ce qui conduit à empêcher les nœuds de communiquer car le medium sera saturé par le brouillage radio [17]. Un réseau sans accès au médium est un réseau hors service [16].

HELLO FLOODING: Les protocoles de découverte dans les réseaux ad-hoc utilisent des messages de type "HELLO" pour découvrir ses nœuds voisins et pour s'insérer dans un réseau. Dans une attaque dite de HELLO Flooding, un attaquant utilise ce mécanisme pour consommer l'énergie des capteurs et empêcher leurs messages d'être routés, comme l'illustre la figure 2.1 ci-dessous [17].

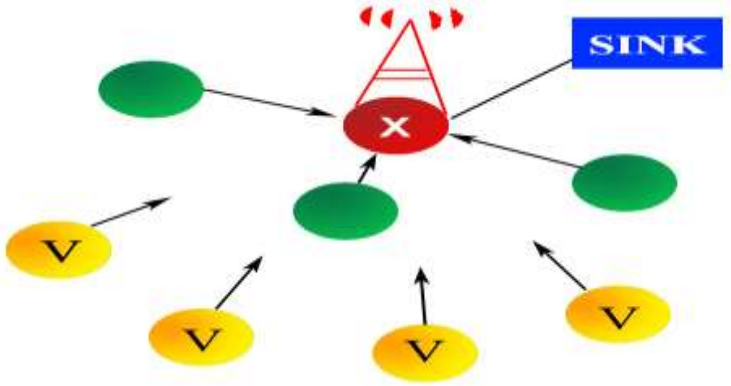

FIGURE 2. 1 : ATTAQUE DE TYPE HELLO FLOODING [16]

INJECTION DE MESSAGES: L'attaquant va chercher par divers moyens (utilisation de nœuds malicieux, envoi de paquets sur la même fréquence radio, réplication de données, etc....) à injecter des messages dans le réseau. Cette injection de messages peut avoir pour effet de perturber le réseau, le saturer ou le tromper en envoyant de fausses informations [16].

ATTAQUE DU TROU NOIRE: L'intrus dans cette attaque se place dans un endroit stratégique dans le réseau c'est-à-dire qu'il prétend être dans le plus court chemin vers la station de base ou le cluster-Head en générant une puissance élevé de transmission. Ce nœud malicieux va modifier les tables de routage, ensuite toutes les informations qui passent par ce dernier ne seront jamais transmises, elles seront supprimées.

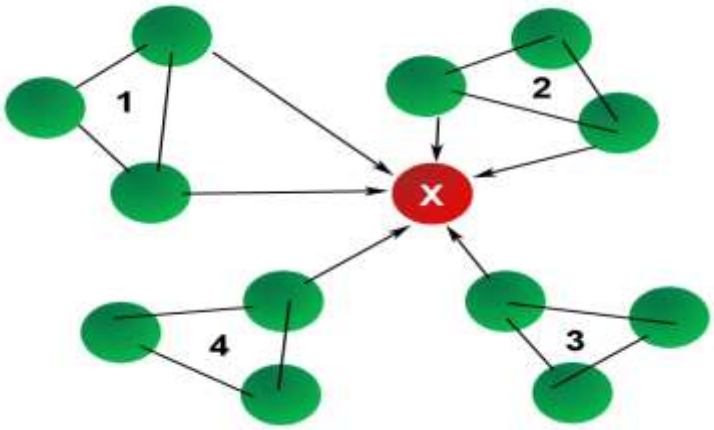

FIGURE 2. 2 : ATTAQUE DU TROU NOIRE(*BLACK HOLE ATTACK*) [16]

La figure 2.2 représente un trou noir mis en place par un nœud malicieux X qui a modifié le routage pour que les clusters 1, 2, 3 et 4 fassent passer l'information par lui pour

communiquer entre clusters. Dans ce cas de figure, le trou noir X ne retransmettra aucune information, empêchant toute communication entre les différents clusters [16].

ATTAQUE DU TROU GRIS: C'est une variante de l'attaque précédente dans laquelle l'attaquant empêche la transmission de certains paquets. Par exemple, les paquets de routage ne sont pas retransmis alors que les paquets de données le sont.

ATTAQUE DU TROU DE VER (TUNNELING): Cette attaque nécessite l'insertion d'au moins deux nœuds malicieux dans les réseaux. Ces derniers sont reliés entre eux par une connexion puissante (filaire ou radio), ce qui permet de tromper les autres nœuds sur les distances qui les séparant.

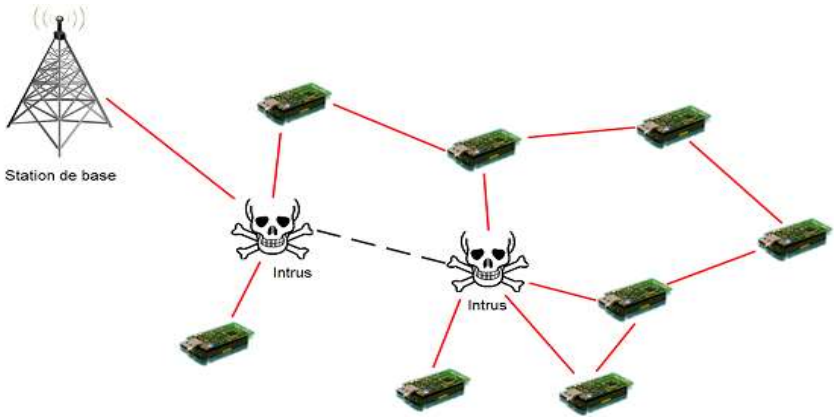

FIGURE 2. 3: ATTAQUE DU TROU DE VER [17]

L'ATTAQUE SYBIL : Dans cette attaque, un nœud malveillant peut avoir plusieurs identités ceux qui lui permettront de gagner un avantage important pour une élection de nœud maître.

4. ATTAQUE CLONE

Les nœuds sont de petits dispositifs non blindés, qui travaillent sans surveillance et sont généralement déployés dans des endroits éloignés assimilés comme des zones hostiles. Pour cela, les RCSF sont très sensibles aux attaques malveillantes comme l'écoute passive, système d'intrusion, le déni de service (DoS), etc. La plus dangereuse des attaques est l'attaque clone nommée également attaque par réplication.

Dans cette attaque, un adversaire capture au moins un des nœuds légitimes, il va le compromettre, ensuite il va reproduire un très grand nombre de copies ou des répliques ayant

la même identité du nœud capturé et enfin il va déployer ces clones dans des emplacements stratégiques dans le réseau.

La détection de cette attaque est très difficile puisque le nœud répliqué est une copie conforme du nœud légitime du réseau. Ainsi aucun nœud légitime dans le réseau ne peut s'apercevoir si c'est un nœud répliqué ou non.

FIGURE 2. 4 : ETAPES DE L'ATTAQUE CLONE D'UN NŒUD CAPTEUR[27]

Les étapes de cette attaque sont comme suit (Figure2.4) :

Etape1 : Les nœuds sont déployés aléatoirement dans le réseau.

Etape2 : L'adversaire capture au moins un des nœuds légitimes déployé dans le réseau.

Etape3 : L'adversaire va compromettre le nœud en collectionnant toutes les informations nécessaires (son identité, ses clés cryptographiques secrètes…).

Etape4 : Il va reproduire des nœuds conformes (des clones) du nœud légitime.

Etape5 : L'adversaire va déployer les clones dans des endroits stratégiques dans tout le réseau.

5. LES PROTOCOLES DE DETECTION DEL'ATTAQUE PAR REPLICATION

Afin d'assurer la sécurité dans les RCSF, plusieurs chercheurs se sont intéressés à trouver des protocoles efficaces pour la détection des multiples attaques qui menacent ces réseaux en utilisant différentes approches (centralisées ou distribuées) que ce soit dans les RCSF statiques ou mobiles.

Nous présentons dans ce qui suit quelques protocoles de détection des attaques par réplication spécifique à chaque approche pour les RCSF stationnaires.

5.1 TECHNIQUES CENTRALISEES

Dans les approches centralisées, la station de base est considérée comme un centre puissant qui est responsable de la convergence de l'information et de la prise de décision. Parmi les protocoles utilisant cette technique, nous citons :

5.1.1 LA DETECTION DE L'ATTAQUE CLONE DANS LES RCSF EN TEMPS REEL

Xing et al. Ont proposé la détection des attaques clones dans les RCSFen temps réel [23]. Dans cette approche, chaque nœud calcule une empreinte digitale, en intégrant les informations de voisinage grâce à un code superposé. Chaque nœud stocke les empreintes digitales de tous ses voisins. Chaque fois qu'un nœud envoie un message, cette empreinte doit être inclues dans le message et donc les voisins peuvent vérifier l'empreinte digitale.

Les messages envoyés par les nœuds répliqués qui ont été déployés dans d'autres endroits seront détectés et supprimés car l'empreinte n'appartient pas à la même communauté [27].

5.1.2LE PROTOCOLE SET

Choi et al. Ont proposé une approche de détection de l'attaque clone dans les RCSF appelé SET (Le réseau est divisé en sous-ensembles exclusifs au hasard) [24]. Chacun des sous-ensembles a un chef de file et les membres sont à un saut de leurs chefs de sous ensemble. Les racines multiples sont décidées au hasard pour construire plusieurs sous arbres et chaque sous-ensemble est un nœud du sous arbre. Chaque chef de sous-ensemble recueille de l'information du membre et l'a transmet à la racine de l'arborescence. L'opération

d'intersection est réalisée sur chaque racine de l'arborescence pour détecter les nœuds dupliqués. Si l'intersection de tous les sous-ensembles d'un sous arbre est vide, il n'y a pas de nœud clone dans ce sous arbre. Dans la phase finale, chaque racine transmet son rapport à la station de base (SB). La SB détecte les nœuds clones en calculant l'intersection de deux des sous arbres reçus [27].

5.2 TECHNIQUES DISTRIBUEES

Dans les techniques distribuées, il n'existe aucune autorité centrale donc c'est un mécanisme de détection spécial (mécanisme de diffusion) dans lequel la détection est effectuée par un nœud distribué localement. L'envoi de la demande de localisation et n'ont pas la station de base mais à un nœud sélectionné de façon aléatoire appelé nœud témoin.

5.2.1 N2NB (DIFFUSION DU NŒUD DANS LE RESEAU)

Cette approche consiste à ce que chaque nœud diffuse sa déclaration signée de sa position géographique et sauvegarde les déclarations de ses voisins directs et si on remarque qu'un nœud refuse de diffuser ses coordonnées, il sera sanctionner. Si un nœud reçoit une déclaration dupliquée par rapport aux valeurs enregistrées, il signale qu'il y a l'attaque par réplication par le mécanisme d'inondation. Ce protocole a un cout de communication très cher de O (n^2) ce qui va influencer sur la durée de vie de la batterie du capteur.

5.2.2 DM (DETERMINISTIC MULTICAST)

Parno et al. Ont proposé cette approche pour la détection distribuée de l'attaque clone dans les RCSF stationnaire [1]. Ce protocole permet le partage des coordonnées géographiques signées seulement avec un sous ensemble limité de nœuds appelé : témoins (witness) qu'ils sont choisis de manières aléatoire. Les nœuds témoins $F(a)$ sont calculés par la fonction F qui est publique et par l'identité du nœud a. Si un nœud reçoit une information dupliquée ou un attaquant fait une copie d'un nœud légitime et les témoins reçoivent deux positions géographiques avec la même identité cela implique une preuve des nœuds répliqués. Si un attaquant trouve la fonction F donc tout le réseau sera dirigé par l'adversaire.

5.2.3 RM (RANDOMIZED MULTICAST)

Parno et al. Ont proposé cette approche pour la détection distribuée de l'attaque clone dans les RCSF stationnaire [1]. Chaque nœud génère un secret (un message signé) à l'aide de sa clé privée, après il diffuse localement ce message à ses voisins d'un saut. Chaque voisin, avec une probabilitép, vérifie l'authenticité du message et vérifie que les nœuds se trouvent dans sa plage de communication. Ce dernier envoie la demande de localisation à ses g nœuds témoins (g sont choisis aléatoirement). Lors de la réception des messages signés, les g témoins vérifient l'authenticité du message et les stockent. Si un des gnœuds reçoit deux positions différentes avec un ID enregistré, il va les signalés pour les supprimer.

5.2.4 (SPACE-TIME)-RELATED PAIRWISE KEY PRE DISTRIBUTION SCHEME

Fei et al. Ont proposé un protocole (espace-temps) lié par un régime de pré-distribution de paires de clés basé sur un polynôme) [25] (PSPP-PKPS, for short PSPP) pour les RCSF, qui concernent le matériel de chiffrement d'un nœud avec son temps de déploiement et l'emplacement.

Dans le PSPP, le matériel de chiffrement d'un nœud ne peut travailler qu'à son emplacement initial de déploiement. Si un nœud quitte son emplacement de déploiement, son matériel de chiffrement ne sera plus valable. En utilisant cette idée, leurs régime offre une résistance contre l'attaque clone [27].

5.2.5LE PROTOCOLE MCD (MOBILE ASSISTED CLONE DETECTION SCHEME)

Dans [18], les auteurs ont présenté un nouveau protocole MCD « Mobile assisted Clone Detection scheme » pour la détection des attaques par réplication, qui est un protocole hybride, utilisant à la fois les capteurs statiques et mobile « patrouille » dans le même réseau ainsi que deux approches différentes de conception qui sont : l'approche distribuée pour la détection des répliques et l'approche centralisée pour la révocation des clones. Ce protocole a introduit une notion très peu utilisée dans les réseaux de capteurs sans fil qui est « les pots de miel » ou « honeypots » afin de servir de leurre et de retarder l'attaquant.

L'utilisation de niveaux de détection hiérarchiques ainsi que d'un robot patrouille pour faire la tournée de tous les nœuds du réseau pour détecter les répliques a permis de réduire les

couts de communication et de stockage par rapport aux protocoles existants sans pour autant affecter l'efficacité et la probabilité de détection qui selon les auteurs avoisinerai les 100%.

6. CONCLUSION

La sécurité dans les approches centralisées s'appuie sur un seul point de vulnérabilité et dans les approches décentralisées sur les nœuds témoins ainsi que d'autres propositions.

Nous avons cité quelques protocoles et il existe bien d'autres approches pour la détection de cette attaque.

Dans le chapitre suivant, nous allons faire l'étude d'un protocole de détection de l'attaque par réplication proposé par C. Bekara [26], qui fait surtout la prévention contre cette attaque.

Chapitre3

IMPLEMENTATION D'UN PROTOCOLE DE PREVENTION DE L'ATTAQUECLONE

SOMMAIRE

1. INTRODUCTION

Les capteurs sont de petits appareils avec une faible capacité de stockage en mémoire, fourniture d'énergie limité qui est en général ni rechargeable ni remplaçable, faible capacité de calcul. Ces nœuds travaillent sans surveillance dans des zones hostiles. Tous ces faits, rendent les RCSF cible à l'attaque clone ainsi que d'autres. Le déploiement des RCSF au cours des dernières années exige plusieurs considérations de sécurité.

L'attaque clone est connue sous l'attaque la plus insidieuse et la plus nuisible dans un RCSF, parce qu'un attaquant compromet un nœud du réseau puis rempli tous ce dernier par des copies du nœud cloné en utilisant tous ses secrets (clés cryptographiques). Le but de cette attaque est d'avoir le contrôle sur le réseau, en compromettant seulement quelques nœuds légitimes.

Différents protocoles pour la détection des nœuds clonés ont été proposés dans la littérature [1] [22], mais malheureusement, la plupart d'entre eux ne sont pas adaptés pour les RCSF, en raison de leurs frais de calcul et de transmission lourde due à l'utilisation de la cryptographie à clé publique, et en raison de leur dépendance à l'égard des coordonnées des nœuds de localisation, ce qui signifie que les capteurs sont des GPS activé, ou qu'ils doivent faire confiance à certains nœuds de balise placées sur le périmètre du réseau pour calculer leurs emplacements exacts [26].

Dans ce chapitre, nous présentons un protocole pour la sécurisation et la prévention contre les attaques par réplication dans les RCSF statiques où un nœud cloné déployé peut être détectée une fois qu'il tente d'établir des paires de clés avec les nœuds voisins du réseau, protégeant ainsi les nœuds légitimes de communiquer avec elle ou de relayer ses paquets, et la protection de notre réseau.

Ce protocole ne repose pas sur des nœuds témoins de la réalisation de la détection de l'attaque clone, il utilise uniquement la cryptographie symétrique [26].

2. PRESENTATION D'ALGORITHME

Dans ce chapitre, nous présentons un protocole proposé par Bekara et al. [26] pour la sécurisation et la prévention contre l'attaque par réplication dans les RCSF statiques, qui ne nécessitent aucune connaissance sur l'emplacement des nœuds, et introduit aucune surcharge importante sur la contrainte des ressources du capteur. Nous donnons l'acronyme PPAC (Protocole de Prévention contre l'Attaque Clone) au protocole étudié [26].

2.1 CONTEXTE

Dans ce qui suit, nous décrivons les hypothèses, le modèle réseau, les notations utilisées, et le modèle de l'adversaire.

2.1.1 HYPOTHESES

✓ Tout d'abord, nous supposons que la station de base (SB) est une entité puissante dans le réseau, qui ne peut pas être compromise.

✓ Deuxièmement, nous supposons que les capteurs sont statiques, une fois qu'ils sont déployés ils ne quittent pas leurs emplacements.

✓ Troisièmement, nous supposons un déploiement basé sur un groupe de nœuds, où les capteurs sont déployés progressivement dans les générations successives (groupes). Dans ce protocole, les nœuds de la même génération pourraient être déployés n'importe où dans le réseau aléatoirement. Par conséquent, ce protocole n'est pas fondé sur une connaissance préalable sur l'emplacement de déploiement de nœuds et ces derniers n'ont pas besoin d'avoir des connaissances sur leurs positions géographiques.

✓ Quatrième, nous supposons qu'une fois qu'un nœud est déployé dans le réseau, il a besoin au maximum d'un temps *Tes*t pour établir la connexion par paires de clés avec ses voisins. De plus, un attaquant a besoin au moins d'un temps T_{comp} pour mettre en péril un nœud après qu'il est déployé dans le réseau, avec $Tcomp > Test$. Cette supposition est présente dans plusieurs protocoles de gestion de clés pour RCSF comme [28], [29] et [30].

Ceci est probable pour être vrai, parce qu'un attaquant doit d'abord avoir un accès physique à un capteur, pour se connecter et utilise ensuite quelques outils de programmation pour extraire les clés secrètes du capteur.

2.1.2 LE MODELE DE DEPLOIEMENT DU RESEAU

La SB déploie des nœuds dans des générations multiples numérotées successivement de 1 à n, où n est le nombre maximal de générations déployées. Nous prenons $n < 2^{16}$-1, donc chaque numéro de génération est la longueur exactement de deux octets.

L'ordre de déploiement doit être respecté G1..., Gi, Gi+1..., Gn, Chaque nœud appartient à une génération unique. Une génération j + 1 est déployée après les nœuds qui ont déjà été déployé dans la génération précédente j. On finit l'établissement par leurs clés par paires.

Parce que les nœuds ne sont pas mobiles dans notre réseau, il est logique que seuls les nœuds de la génération nouvellement déployé qui demandent la clé de la mise en place avec leurs voisins, qui peuvent appartenir soit à la même génération, ou de générations antérieures déployées. Les nœuds de générations précédentes ne peuvent pas demander l'établissement des clés, et même si elles demandent, leurs demandes doivent être rejetées.

Notation	**Signification**
u, v	Deux nœuds du RCSF
Idu	Identifiant unique de 4 octets dunœud$u$ dans le réseau
Nu	Une valeur d'occasion croissante produite par le nœud u
Fu	L'action du polynôme secrète du nœud u
$Kuv = Kvu$	La clé de paires secrète établie entre u et v
$MACK(M)$	Le code d'authentification de message de M en utilisant la clé secrète K
H	Une fonction de hachage à sens unique, avec une longueur de sortie de 4 octets
$A\|\|b$	A concaténé avec b
$\|x\|$	La longueur d'octets de l'argument x

TABLEAU 3. 1: LES NOTATIONS UTILISEES [26]

Sur la base de cette hypothèse, nous pouvons affirmer que n'importe quelle clé qui demande l'établissement provient de:

- soit d'un nœud à partir de la génération nouvellement déployé;
- Ou un nœud déployé par un attaquant, qui est un nœud cloné ayant l'Id et les clés cryptographiques secrètes d'un nœud compromis.

Pour des raisons de sécurité, nous supposons que tout nœud u récemment déployé met un minuteur à la valeur *Test* tout de suite après le déploiement. Une fois le minuteur expire, le nœud u arrête le processus de création de clé avec tout nœud déployé de l'ancienne génération, et rejette toute demande d'établissements de clé provenant d'un nœud de la même génération nouvellement déployé.

3.1.3 LE MODELE D'ADVERSAIRE

Nous considérons que l'adversaire a la capacité de capturer et de compromettre un nombre limité de nœuds légitimes du réseau. Après qu'il compromette un nœud légitime, l'adversaire clone le nœud en chargeant sa clé secrète cryptographique sur plusieurs nœuds de capteurs génériques, et déployer les nœuds clonés dans certains endroits stratégiques du réseau. une fois que les nœuds clonés sont déployés par l'adversaire, ils vont d'abord essayé d'établir des liens sécurisés avec leurs voisins, en vue d'envoyé des paquets, et participer à l'exploitation du réseau comme tout autre nœud légitime dans le réseau, . Une fois que les nœuds clonés sont intégrés dans le réseau, l'adversaire et les nœuds clonés peuvent collaborer à des différentes attaques contre le réseau. Nous estimons également que n'importe quel nœud cloné a au moins un ou plusieurs nœuds légitimes de son quartier.

Pour plus de clarté, nous énumérons les symboles et notations utilisés dans le **Tableau 3.1**.

3. DETAILS DU PROTOCOLE

Maintenant, nous décrivons le protocole étudié pour la prévention de l'attaque clone. La base de ce protocole, est l'utilisation du polynôme symétrique pour l'établissement de la clé par paires, ce modèle de déploiement est basé sur un groupe défini.
L'idée principale de ce protocole, est de lier chaque nœud déployé à l'unique génération dans laquelle il appartient, par l'utilisation du polynôme symétrique, pour que même si les nœuds

multipliés sont créés. Ces derniers appartiennent aussi à la même génération que le nœud compromis.

Dans ce protocole, seuls les nœuds nouvellement déployés (nœuds qui appartiennent à la nouvelle génération) ont pu établir des clés par paires avec leurs voisins. Tous les nœuds du réseau connaissent le numéro de la génération déployée la plus élevée. Comme conséquence, un attaquant peut mettre en péril un vieux nœud déployé (qui appartient à une ancienne génération), ne peut pas réussir à remplir le réseau avec des nœuds clonés, parce que ces derniers ne parviendront pas à établir les clés par paires avec leurs voisins.

3.1 INITIALISATION

Initialement (avant le déploiement des nœuds), la station de base (SB) génère un polynôme aléatoire à deux variables symétrique [26].

$$f(x,y)=\sum_{i,j=0,\ldots,t} aij \times +x^i y^j \ (mod Q') \qquad (1)$$

Ou Q' est un grand nombre premier, $1 \leq a_{ij} \leq Q'-1, t$ est le degré du polynôme et un paramètre de sécurité. Nous supposons que | x | = | y | = 4 octets.

Pour toute G_i génération nouvellement déployé, la SB charge chaque nœud $u \in G_i$sa part du polynôme secret unique:

$$fu(y) = f\ (\ H\ (\ i\ ||\ Idu\ ), y\ ) \qquad (2)$$

Notez qu'il est impossible que deux nœuds différents peuvent avoir la même part du polynôme secret, si un nœud ne peut jamais mentir sur sa véritable identifiant ou le nombre réel de génération auquel il appartient. En effet, supposons que $u \in G_i$et$v \in G_j$, avec$i \neq j$. $f_u(y) = f_v\ (y)$ Est possible, seulement et seulement si $H\ (i||Id_u) = (j||Id_v)$, ce qui signifieque$i||Id_u = j||Id_v$. Le numéro de Chaque génération est la longueur exactement de 2 octets et chaque identifiant de nœud est la longueur exactement de 4 octets, de sorte que $|i||Id_u| = |j||Id_v| = 6\ octets$.Grâce à notre extension de station bien formaté identificateur (2 octets de numéro de génération, 4 octets ID de nœud), à partir d'un identificateur de nœud étendu$i||Id_u$, c'est impossible de trouver un autre identificateur de nœud distincte $j||Id_v$ où $i \neq j$ou $Id_u \neq Id_v$.

3.2 DESCRIPTION DU PROTOCOLE

Supposons que la SB déploie les générations précédentes (dire les premières générations i $(1,2,\dots,i)$, et vient de déployer la génération$i+1$. Dans notre protocole, les nœuds connaissent le plus haut numéro de génération déployé$i+1$. Soit $u \in Gj$est un nœud nouvellement déployé. Il n'est évident que, par un nœud légitime, $u \in G_{i+1}$ Le nœud u cherche à établir les liens sécurisé avec ses voisins directs en diffusant localement un message 'Bonjour':

$$u \rightarrow *: Bonjour, j, Id_u N_u \qquad (3)$$

Où Nu est utilisé pour garantir la réponse. Soit$v \in Gz$, où $z \leq i+1$, un nœud voisin de $u$réceptions de son message. Pour le nœud v décide de servir le nœud u .Le nœud v suit deux étapes:

1) vérifie si$\boldsymbol{j = i+1}$, pour vérifier si u appartient à la génération nouvellement déployé. Si la vérification échoue, il rejette simplement la demande du nœud$u$, car ce dernier est normalement déjà déployé.

2) Si v vérifie que$\boldsymbol{j = i+1}$, alors:

- Si v appartient à la génération $\boldsymbol{z \leq i}$,alors v calcule $K_{vu} = f_v(H(i+1||Id_u))$ et renvoie au nœud u le message suivant:

$$v \rightarrow u: \ z, Id_v, N_v, MACK_{K_{vu}}(z, Id_v, N_v, N_u) \qquad (4)$$

- Si $\boldsymbol{j = z = i+1}(u, v \in G_{i+1})$, alors:

- Si la temporisation est réglée par le nœud$v$ (pour le test de la valeur), n'a pas expiré, faire la même chose (traitement comme dans le cas précédent).

- Si le délai est expiré, il rejette la demande, en raison du nœud u qui est soupçonné d'être malveillant.

Dès la réception du message du nœudv' s, le nœud $u$calcule$K_{uv} = f_u(H(z||Id_{v)})$, et vérifie l'authenticité du message. Si le message n'est pas authentifié, le nœud v rejette tout simplement le message. Si le message est authentifié, le nœud u définit K_{uv} comme clé par

paires partagée avec v , et envoie à v le message suivant à conclure et authentifier mutuellement la clé processus de mise en place:

$$u \rightarrow v:\ ok, MAC_{K_{uv}}(ok, N_v)\ (5)$$

En recevant la réponse par le nœud$u\ '\ s$, le nœud v vérifie l'authenticité des messages en utilisant K_{vu}et, si cela est fait avec succès, Le nœud v définit K_{vu} comme clés par paires partagées avec$u$, autrement (échec de l'authentification, ou réponse non reçu), il effaceK_{vu}.

A la fin de cette phase, une clé par paires est établi entre deux nœuds valides, ou l'établissement de clé par paires échoue au cas où un des deux nœuds est soupçonné d'être un nœud cloné ou un faux nœud d'identifiant non - existant. Le protocole décrit, garantit que n'importe quelle demande d'établissement de clés servie, provient d'un nœud appartenant à la génération nouvellement déployée$i\ +\ 1$.

4. ANALYSE DE SECURITE DU PROTOCOLE

Requête de nœud	Réponse de nœud
Nouveau	Nouveau
Nouveau	Ancien
Ancien	Nouveau
Ancien	Ancien

TABLEAU 3. 2 : SCENARIOS IDENTIFIES POUR L'ETABLISSEMENT DES CLES SELON LA GENERATION DES NŒUDS CONCERNES [26]

Dans le protocole PPAC et sous les hypothèses précédentes, un attaquant est hautement improbable pour déployer les nœuds clonés, et convaincre leurs voisins de leur validité.

Le **Tableau 3.2** résume les différents scénarios des tentatives de déploiement d'un nœud cloné. Comme un nœud répliqué doit d'abord établir les clés avec ses voisins en vue de s'intégrer dans le réseau.

Quatre cas d'attaques sont possibles qu'ils peuvent être définis selon la génération sur laquelle appartient le nœud multiplié, si ce dernier est un nœud de requête ou un nœud répondant dans le processus d'établissements par clés par paires.

Tout d'abord, nous allons voir comment le protocole PPAC gère les deux derniers cas, Ancien - Nouveau et Ancien- Ancien où un nœud clone u d'une ancienne génération déployé demande l'établissement de clés avec un nœud d'une génération plus récente,ou une génération plus ancienne. Seuls les nœuds de la génération nouvellement déployée sont en mesure de demander l'établissement de clés avec leurs voisins. Par conséquent, un nœud clone u d'une ancienne génération déployé ($u \in Gi$), ne peut pas initier l'établissement de clés avec un autre nœud déployé$(v \in Gj)\ ou\ j > i$. En outre, le mécanisme garantie que tous les nœuds du réseau ont la même vue sur le nombre le plus élevé de la génération déployée, de sorte que le nœud cloné $u \in Gi$ ne peut pas demander l'établissement de clés avec un nœud$v \in Gj$ où $j \leq i$.

Deuxièmement, nous allons voir comment le protocole PPAC gère le premier cas Nouveau - Nouveau, où un attaquant compromet un nœud nouvellement déployé et demande l'établissement des clés avec un autre nœud nouvellement déployé de la même génération. En limitant la durée de la phase d'établissements des clés pour les nœuds nouvellement déployés, même si un attaquant compromet un nœud nouvellement déployé dans une période de temps T_{comp}, où T_{comp} > Test, l'attaquant ne peut pas établir des liaisons sécurisées avec d'autres nœuds de la même génération, tout simplement parce que les nœuds qui ont répondu rejettent la demande.

4.1 REVOCATION DU NŒUD ET DETECTION D'INTRUSION

Comme décrit ci-dessus, dans les trois cas possibles d'établissements des clés, une attaque active est toujours détectée. En outre, un attaquant silencieux (intrus) est également détecté quand il essaie de répondre aux demandes d'établissements de clé de nœuds nouvellement déployées, et les nouveaux nœuds sont alors avisés. En conséquence, on connaît l'identité du nœud compromis, donc les nœuds voisins du nœud multiplié peuvent lancer une révocation distribuée contre cela, ou notifier la SB qui émet un message de révocation dans le réseau pour révoquer à la fois le nœud compromis et ses clones.

5. CALCULS ET COUTS EN MEMOIRE

Dans cette section, nous allons examiner les calculs et les coûts de mémoire du protocole étudié.

Pour le coût de la mémoire, chaque nœud stocke son identificateur étendu (numéro de génération, l'ID du nœud), sa part polynôme et les clés par paires établies. Un identificateur est prolongé de longueur de 6 octets. Une part de polynôme est représentée par des coefficients t+1, plus le modulo Q'. Si nous choisissons un modulo Q ' de 8 octets et t=100, chaque nœud doit 816 octets de mémoire pour stocker sa part polynôme. Chaque paire de clés établie a besoins de 8 octets en mémoire.

Pour le coût de calcul, chaque nœud doit évaluer sa part polynôme pour chaque établissement de clé. Comme il est décrit dans [20], l'évaluation d'une part polynôme nécessite t multiplications modulaires et t additions modulaires dans un $F_{Q'}$ champ fini. Cependant, le processeur d'un capteur ne manipule pas des mots de 64 bits (8 octets).

Par conséquent, dans un processeur d'UC de 16 bits, évaluant un polynôme de t-degré partagent $f_u(y)$ sur un domaine fini F_Q, où Q' est un nombre premier de 64 bits et y est la longueur (de 6 octets) de 48 bits, exige 4 × T des additions modulaires et 8+24 × (T - 1) des multiplications modulaires.

Grâce à l'utilisation de la cryptographie seulement à clé symétrique, ce protocole a des calculs pour effectuer des opérations de chiffrement ou d'authentification, alors Parno et al. [1], les Protocoles qui reposent sur l'utilisation de la cryptographie à clé publique, et même moins de Zhang et al. [22], les protocoles basés sur des courbes elliptiques cryptographies.

Même en produisant les paires de clés, le protocole de génération de clé à base de polynôme a moins de calcul au-dessus, parce que nous n'avons aucune exponentiation modulaire comme dans la cryptographie à clé publique traditionnelle et nous n'avons aucune multiplication de point scalaire comme dans la cryptographie de courbe elliptique.

Pour le coût de la mémoire en raison des matériaux de clés initialement stockées, notre protocole peut avoir un coût supplémentaire que les autres protocoles. En effet, comme décrit ci-dessus, chaque nœud doit stocker un matériel de clé (part polynôme) de 800 centaines d'octets. Dans les protocoles proposés par Parno et al. Et dans le cas, où nous utilisons la clé publique sur les courbes elliptiques cryptographies, chaque nœud doit stocker au moins 163 bits (21 octets) clé privée, Le modulo principal Q qui est de longueur au moins de 163

bits aussi, son certificat de longueur de 86 octets et le certificat de la BS qui est la longueur de 86 octets aussi. Cependant, les protocoles de Parno et al consomment de l'énergie lourde pendant la transmission, parce que chaque nœud doit diffuser dans le réseau son certificat de 86 octets ainsi que son emplacement revendique qui permettait la vérification de sa signature, la signature est de longueur approximativement de 42 octets. Dans le protocole Zhang., chaque nœud stocke un modulo principal Q de 163 bits (sur lequel les courbes elliptiques sont définies), sa clé est basée sur l'identité de 42 octets privée, la clé privée basée sur l'emplacement de 42 octets, et sa position, dont la longueur dépend du type des coordonnées utilisé.

Protocoles	Coût de communication	Coût de mémoire
Xing et al. Scheme [23]	C· (1 + ratio)	O (d) + min $(M, \omega \cdot \log 2\ M)$
SET [24]	O (n)	O (g)
N2NB [1]	O (n^2)	$O(1)$
DM [1]	$(g \log \sqrt{n}/d)$	$O(g)$
RM [1]	(n^2)	$O(\sqrt{n})$
MCD [18]	O (n)	$O(1)$
PPAC [26]	***O(√n)***	***O(1)***

TABLEAU 3. 3 : ANALYSE DE PERFORMANCE ASYMPTOTIQUE [27].

Le Tableau 3.3 illustre la comparaison en termes de cout de communication et du cout en mémoire entre le protocole étudié PPAC et les autres solutions existantes. Nous remarquons à travers ce tableau que le protocole PPAC possède le meilleur cout de communication et de mémoire parmi les autres solutions proposées.

6. RESULTATS DE L'IMPLEMENTATION

Nous avons utilisé dans l'implémentation de ce protocole le simulateur TOSSIM ainsi que l'utilisation des capteurs afin de visualiser le fonctionnement du protocole PPAC d'une manière plus réaliste.

L'objectif principal de cette implémentation est de modéliser le protocole PPAC afin de déterminer son efficacité, ses points faibles ainsi que les perspectives envisagées.

6.1 CHOIX TECHNIQUES

L'implémentation de ce protocole a nécessité l'utilisation de différents outils logiciels bien spécifiques au domaine des réseaux de capteurs sans fil, tels que NesC comme langage et TinyOS comme système d'exploitation, et le simulateur TOSSIM, ainsi que des outils matériels qui sont les capteurs telosB.

Un aperçu de ses outils est décrit dans ce qui suit :

6.1.1 LE SYSTEME D'EXPLOITATION TinyOS 2.x

Selon [8] TinyOS est un système d'exploitation en open source développé et suivi par l'université de Berkeley. Ce système d'exploitation a été conçu pour les réseaux de capteurs sans fil car un capteur n'a pas assez de mémoire pour supporter un système d'exploitation comme Linux ou Windows qui prennent beaucoup de place. Il respecte une architecture basée sur les associations de composants, réduisant ainsi la taille du code nécessaire à sa mise en place, respectant ainsi la contrainte de mémoire des capteurs.

TinyOS est basé sur la gestion de taches et d'événements. Les événements sont prioritaires sur les taches et seul un événement peut arrêter une tache. Il y a donc deux niveaux de priorités : basse pour les taches et haute pour les événements.

L'outil de développement de TinyOS est compatible avec Linux et Windows, sa programmation est simple et portable sur de nombreuses plateformes (Mica, Telos...), cependant il n'est pas possible de faire des allocations dynamiques, des pointeurs sur fonctions et la mémoire n'est pas protégée ce qui implique la possibilité de crash et de corruption de la mémoire.

6.1.2 LE LANGAGE DE PROGRAMMATION NesC

Le système d'exploitation TinyOS s'appuie sur le langage NesC. Celui-ci propose une architecture basée sur des composants, permettant de réduire considérablement la taille mémoire du système et de ses applications. Chaque composant correspond à un élément matériel (LEDs, timer, ADC …) et peut être réutilisé dans différentes applications. Ces applications sont des ensembles de composants associés dans un but précis. Les composants peuvent être des concepts abstraits ou bien des interfaces logicielles aux entrées sorties matérielles de la cible étudiée (carte ou dispositif électronique) [3].

6.1.3 LE SIMULATEUR TOSSIM

Avant sa mise en place, le déploiement d'un RCSF nécessite une phase de simulation afin de s'assurer du bon fonctionnement de tous les protocoles de communication qu'il utilise. En effet, pour de grands réseaux, le nombre de capteurs peut atteindre plusieurs milliers et entraine donc un coût financier relativement important. Ainsi, il faut réduire au maximum les erreurs de la conception. Malgré cela, il reste des facteurs réels qui ne peuvent être pris en compte par la simulation, tels que les contraintes physiques (perturbations électromagnétiques, inondations, etc.) ou les aléas (détériorations dues à un animal, etc.). Pour arriver à simuler le comportement des capteurs au sein d'un RCSF, un outil très puissant a été développé et proposé pour TinyOS sous le nom de TOSSIM. Le principal but de TOSSIM est de créer une simulation très proche de ce qui se passe dans les RCSF dans le monde réel. Une économie d'effort et une préservation du matériel sont possibles grâce à cet outil.

Pour une compréhension moins complexe de l'activité du réseau, TOSSIM utilise avec le langage python [19].

LE LANGAGE Python

Python est un langage de programmation objet, multi-paradigme et multiplateformes. Il favorise la programmation impérative structurée et orientée objet. Il est doté d'un typage dynamique fort, d'une gestion automatique de la mémoire par ramasse-miettes et d'un système de gestion d'exceptions ; il est ainsi similaire à Perl et Tcl.

Le langage Python vous permet d'interagir avec le simulateur TOSSIM en cours dynamique, comme un puissant débogueur [19].

6.2 MISE EN PLACE DE LA PLATEFORME

6.2.1 INSTALLATION LOGICIELLE

Cette étape nous a permis de nous familiariser avec les capteurs telosb et le langage NesC, le simulateur TOSSIM ainsi que l'installation du système d'exploitation TinyOS 2.X sous Ubuntu, ce qui n'a pas été une tâche facile.

6.2.2 INSTALLATION MATERIELLE

Consiste en la réalisation de la plateforme implémentant notre protocole (voir la figure 3.1), Nous utilisons pour cela sept capteurs telosB chacun représentant un rôle bien spécifique comme décrit ci-dessous :

FIGURE 3.1 PLATROME D'EXECUTION DU PROTOCOL

- Le capteur de l'id= 4 est flashé avec le programme principal qui traite tous les cas possible du protocole PPAC.
- Le capteur de l'id= 7 appartient à la nouvelle génération.
- Les capteurs id=5 et id=6 appartiennent à la même génération que le capteur 4.
- Les capteurs id=1, id=2, id=3 appartiennent à l'ancienne génération.

Gestion des Leds

Nous utilisons pour l'exécution de ce protocole tout en faisant appel d'une part à la bibliothèque « *printf* » de TinyOs pour afficher le déroulement du processus d'exécution et d'autre part à un mécanisme de gestion de Leds tel que décrit dans le tableau 3. 4.

Les scénarios	Les leds
Nœud d'une nouvelle génération	Led1
Nœud d'une ancienne génération	Led0
Nœud de la même génération	Led2

TABLEAU 3.4: GESTION DES LEDS

Ce programme utilise les interfaces:

- Boot : permet d'initialiser tous les composants au démarrage, elle est fournie par la configuration MainC qui est le cœur de l'application.
- Leds : utilisée pour la manipulation des leds, fournie par LedsC.
- Timer : c'est une interface de synchronisation qui permet de gérer le timer d'émission, de test et d'allumage des leds.
- Split control : contrôle l'antenne radio.
- AMSend : pour l'envoie du paquet.
- Packet : pour accéder aux données du message.
- AMPacket : fournie l'adresse locale et la fonctionnalité d'accès au paquet.
- Receive : pour la réception des messages.

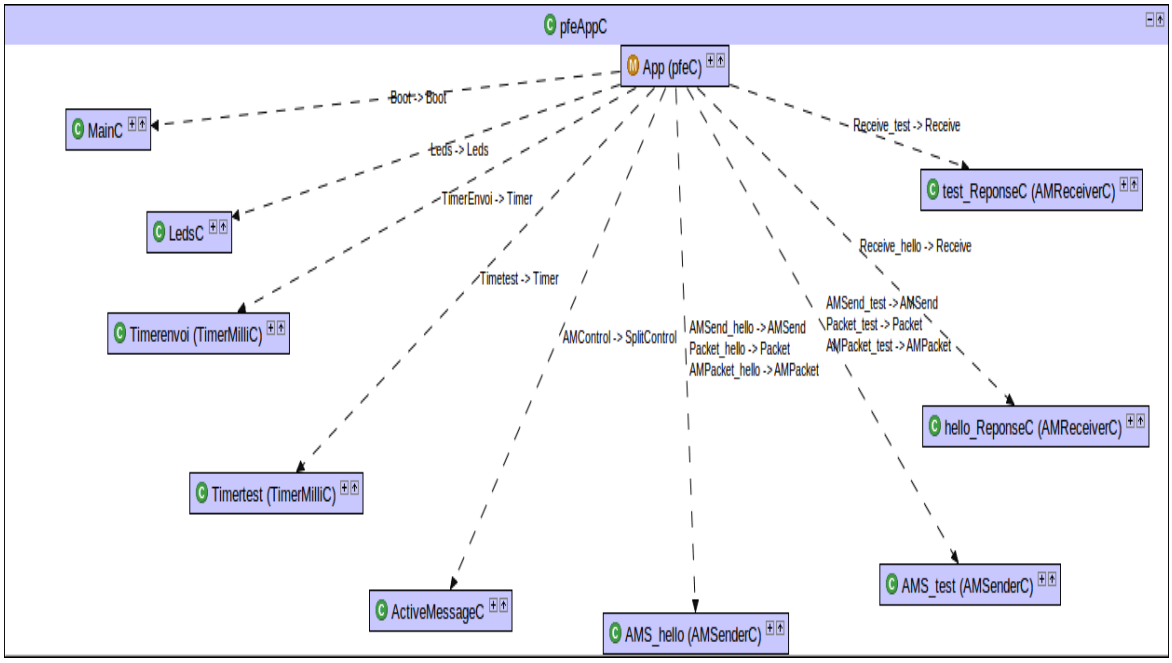

FIGURE 3. 2 : REPRESENTATION GRAPHIQUE DU PROGRAMME

6.3QUELQUES EXECUTIONS

La topologie :

Nous avons fait la simulation avec 14 nœuds, la topologie qui illustre notre travail se trouve dans la figure 3.3

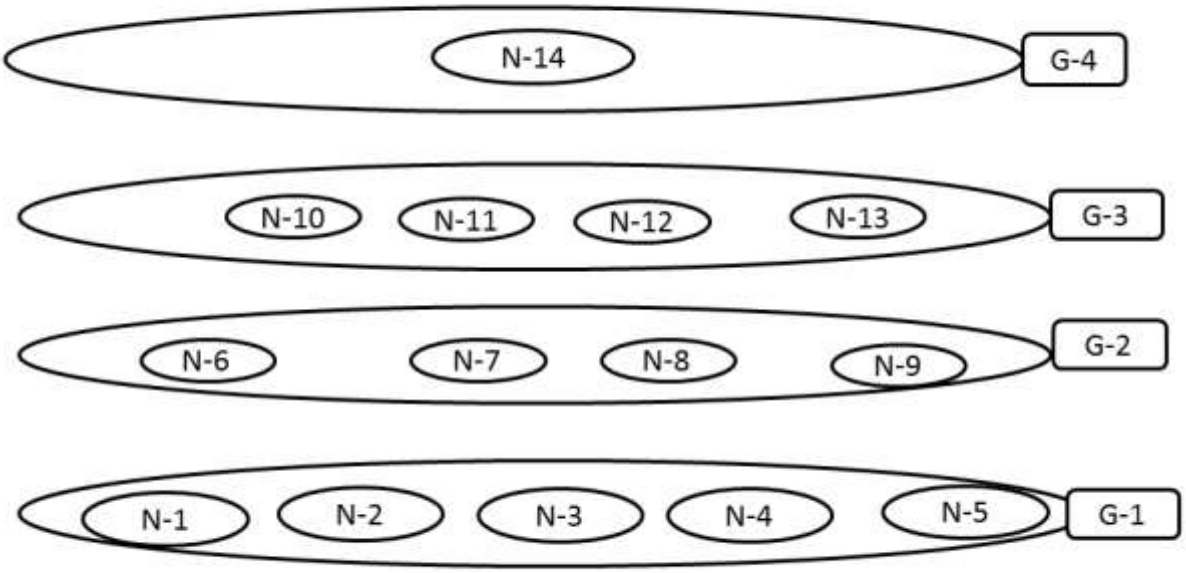

Figure 3.3 : Représentation de la topologie utilisée dans la simulation

Nous allons vous présentez les cas (scénarios) de simulation qu'on a étudiez pour ce protocole :

Scénario1 : Nouvelle génération

Quand un nouveau nœud veut rejoindre le réseau, il diffuse le message bonjour avec son identifiant et son numéro de génération, un de ses voisins des anciennes générations va lui répondre pour établir avec lui un lien sécurisé, et à la fin il sera déployé dans le réseau.

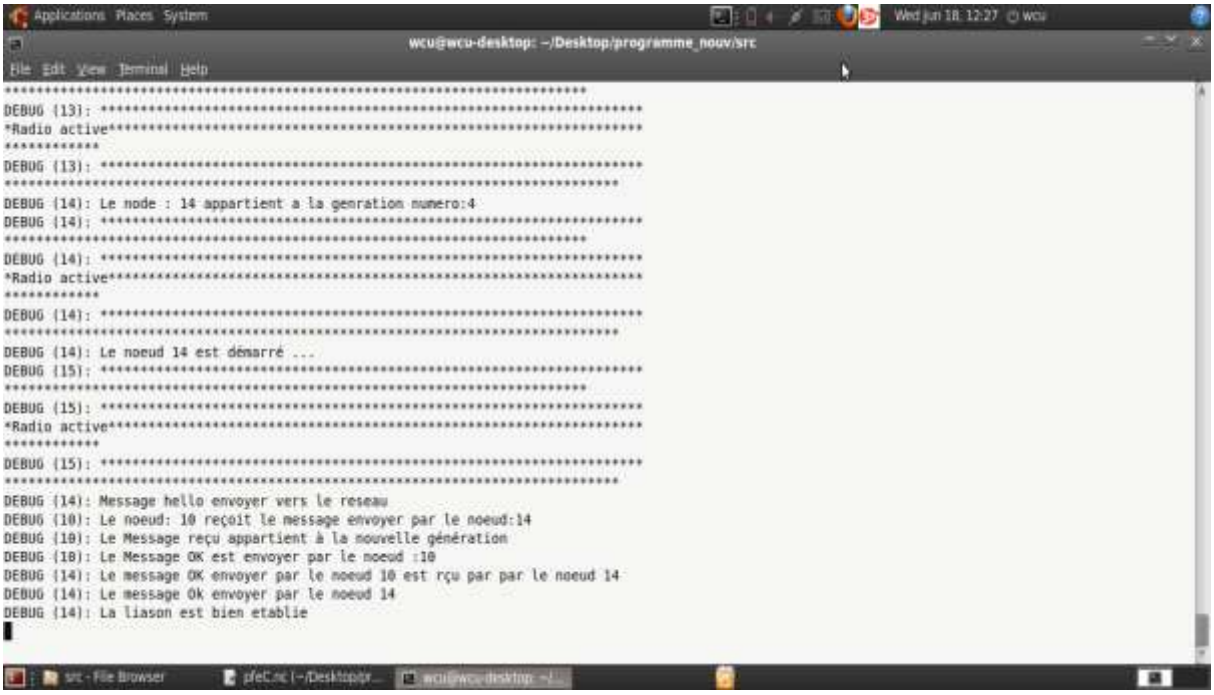

FIGURE 3. 4 : RESULTAT DE SIMULATION D'UN NŒUD D'UNE NOUVELLE GENERATION

Scénario2 : Ancienne génération

Quand un nœud appartient à une ancienne génération et veut rejoindre à nouveau le réseau sa demande sera rejeter automatiquement car il est normalement déjà déployé.

Figure 3. 5 : RESULTAT DE SIMULATION D'UN NŒUD D'UNE ANCIENNE GENERATION

Scénario3 : Même génération

Quand un nœud de la même génération va rejoindre le réseau on distingue deux situation : un clone ou nœud légitime .Dans ses deux dernier un temporisateur va démarrer.

Comme on a supposé une fois qu'un nœud est déployé dans le réseau, il a besoin au maximum d'un temps T_{test} pour établir une paire de clés avec ses voisins. De plus, un attaquant a besoin au moins d'un temps T_{comp} pour mettre en péril un nœud après qu'il sera déployé dans le réseau, avec $T_{comp}>T_{test}$. On va régler un temporisateur avec un temps T_{test}.

Situation1 : nœud clone

Un attaquant qui possède toutes les informations d'un nœud légitime diffuse un message bonjour avec son identifiant et son numéro de génération et il attend la réponse d'un de ses voisins, une fois que le message sera reçu par un de ses voisins et il trouve qu'il est avec lui dans la même génération, il lui répond avec un message test et il démarre en même temps un temporisateur. Une fois que le message sera reçu par le clone il renvoi un code pour qu'il confirme son légitimité, ce processus va prendre beaucoup de temps car $T_{comp}>T_{test}$, Donc le temporisateur sera terminer et le voisin rejette simplement la demande du nœud clone, ainsi que la liaison ne sera jamais établie.

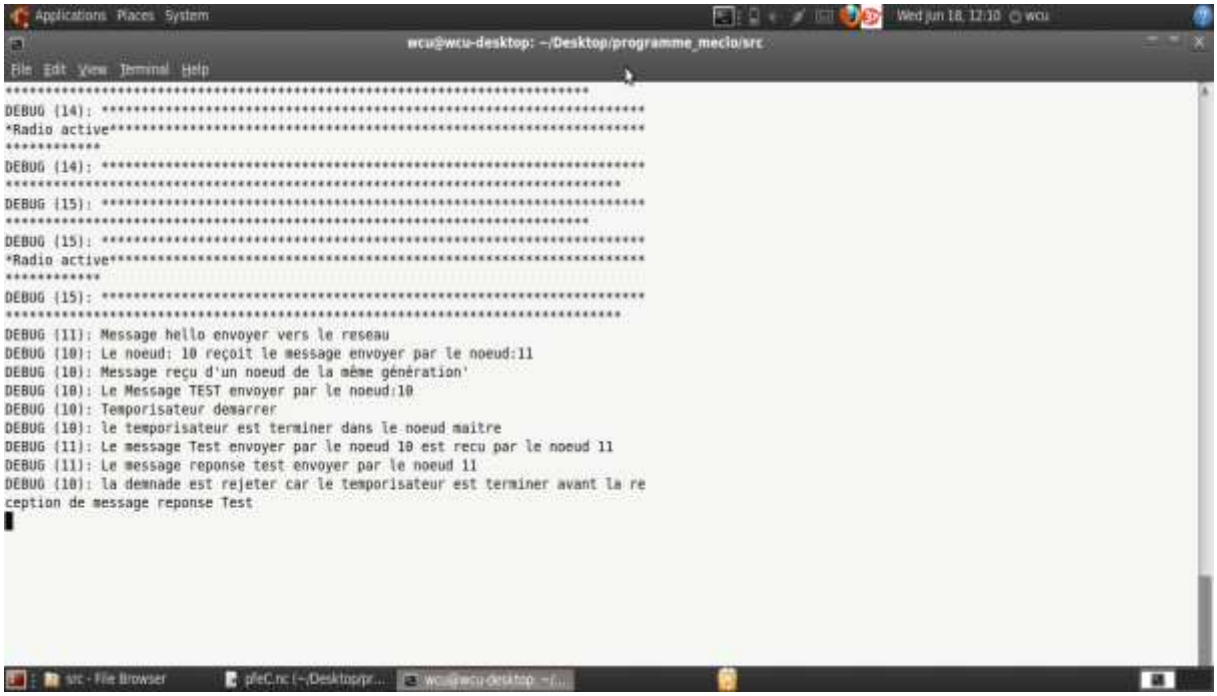

Figure3. 6 : RESULTAT DE SIMULATION D'UN NŒUD CLONE

Situation2 : nœud légitime

Un nœud légitime veut rejoindre le réseau il diffuse un message Bonjour à ses voisins avec son identifiant et son numéro de génération. Une fois qu'un de ses nœuds voisin reçoit le message Bonjour, il va lui répondre avec un message test, lorsque le nouveau nœud reçoit ce dernier message il établit un lien sécurisé avec le nouveau nœud.

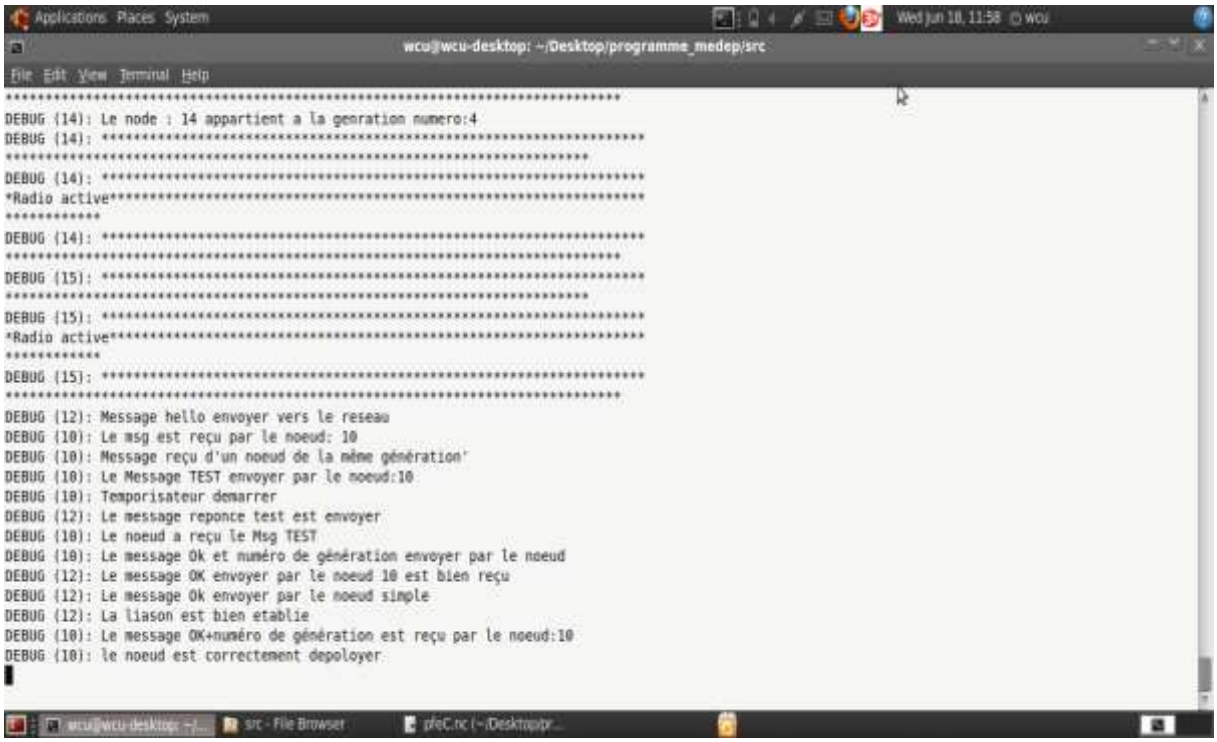

Figure3. 6 : RESULTAT DE SIMULATION D'UN NŒUD LEGITIME

7. QUELQUES PROBLEMES ET SOLUTIONS PROPOSEES POUR LE PROTOCOLEPPAC

Nous allons voir comment ce protocole gère le second cas, où un nœud de la génération nouvellement déployé demande l'établissement de clé avec un nœud d'une génération déployée plus ancienne. Deux cas sont à distinguer :

-Tout d'abord, le nœud nouvellement déployé (nœud demandeur) est un nœud clone d'un nœud compromis qui appartient à la génération nouvellement déployé.

- Deuxièmement, le nœud répondant est un nœud clone d'un nœud compromis qui appartient à une génération plus ancienne.

7.1 PROBLEMES

Pour le premier cas, *malheureusement*, notre algorithme ne gère pas cette situation. Ce cas est **difficile à détecter**, car le nœud cloné ressemble à un nœud légitime appartenant à la génération la plus élevée déployée.

Le deuxième cas est **également difficile à détecter**, car le nœud nouvellement déployé a une demande pour l'établissement de clés, et il n'a aucun moyen de vérifier si le nœud est un nœud répliqué ou non.

Le problème est encore plus difficile si le nœud clone reste inactif ou silencieux jusqu'à ce qu'un nouveau nœud est déployé.

A cette époque, le nœud cloné pourrait devenir actif et établir un lien sécurisé avec le nœud nouvellement déployé simplement en répondant à sa demande.

Dans ce scénario, le nœud cloné ne demande pas à ses voisins l'établissement de clés, il ne peut pas être détecté, de sorte que le nœud nouvellement déployé ne peut être empêchée.

7.2 IDEE D'AMELIORATION

Pour le premier cas, *une solution* pourrait être proposée c'est qu'un nœud déployé n'accepte plus d'établir des liens sécurisés avec des nœuds d'une même génération nouvellement déployée que pendant une période de temps Tmax après le déploiement d'une nouvelle génération, où test <Tmax<Tcomp.

Les nœuds savent à tout moment, le nombre le plus élevé de la génération déployé, et quand une nouvelle génération sera déployé. Par conséquent, chaque nœud déjà déployé définit une minuterie pour la valeur Tmax<Tcomp lorsque le temps de déploiement d'une nouvelle génération est atteint. Un attaquant a besoin d'au moins un temps Tcomp afin de compromettre un nœud nouvellement déployé car nous sommes pratiquement assurés qu'un attaquant ne va pas établir des liaisons sécurisées avec des nœuds de générations plus âgées, car ces nœuds rejettent sa demande.

Pour le deuxième cas, *une solution* à ce problème est que les nœuds voisins qui sont déployés à la fois du nœud nouvellement déployé et le nœud cloné détectent l'existence d'un nœud voisin, mais ils n'ont pas de liens sécurisés avec lui, ils concluent que le nœud est un nœud malveillant (nœud cloné).

En conséquence, un message d'information sera envoyé par eux au nœud nouvellement déployé qui efface tous les clés établies avec le nœud cloné.

8. CONCLUSION

Nous avons présenté dans ce chapitre un protocole qui prévient et détecte les nœuds clonés, en supposant que les nœuds de ce RCSF ne connaissent pas leurs coordonnées géographiques et que ses petits appareils ne sont pas en mesure d'effectuer des opérations cryptographiques à clés publiques, ainsi que ces derniers ne tiennent pas en compte d'autres entités de confiance que la SB.

Ce protocole utilise le principe de générations basé sur l'établissement de paires de clés, il fait surtout la prévention et la protection contre l'attaque par réplication, où seuls les nœuds de la génération nouvellement déployée qui demande l'établissement de clés. En outre, le mécanisme proposé pour la détermination de la plus haute génération déployée garantit que les nœuds répondront qu'aux demandes des nœuds nouvellement déployés, ainsi la durée limitée de l'établissement des clés rendra pratiquement impossible qu'un adversaire réussie de capturer un nœud, ce qui ne lui permettra pas de construire des copies du nœud capturé. De plus, ce protocole supporte la détection des attaquants silencieux.

CONCLUSION GENERALE

Ce projet était une occasion de découvrir un nouveau monde (les réseaux de capteurs sans fil). Ces derniers constituent un axe de recherche très fertile et peuvent être appliqués dans plusieurs domaines différents ‘militaire, médical, environnemental, surveillance, etc.’. Cependant, il reste encore de nombreux problèmes à résoudre dans ce domaine afin de pouvoir les utiliser dans les conditions réelles. L’un des problèmes qu’on peut rencontrer dans ce genre de réseaux nous citons la problématique de la sécurité, elle est causée par le fait que les réseaux de capteurs sans déployés dans des environnements inaccessibles et hostiles. Et pour cela, le réseau sera exposé à plusieurs types d’attaques internes et externes. Ce mémoire avait pour objectif de bien comprendre l’attaque clone, qui est une attaque interne et très dangereuse, car un malveillant peut capturer un nœud, le dupliquer autant de fois qu’il le désire et utiliser ces répliques afin d’avoir un accès au réseau et mener d’autres attaques plus nuisibles ou plus profitables.

Dans ce travail, nous avons présenté d’abord une présentation sur les nœuds capteurs, leurs types , leurs contraintes ainsi que leurs domaines d’application, ensuite, durant la phase d’étude bibliographique, nous nous sommes intéressées aux RCSF stationnaires , et à plusieurs solutions ou approches centralisées et distribuées les plus connues qu’elles ont été proposées par les chercheurs contre cette attaque , en précisant les avantages et les inconvénients de ces protocoles proposés.

Après cette étape, nous avons choisis le protocole proposé par C. BEKARA [26]. C’est un protocole distribué, différent des autres parce qu’il s’appuie sur le principe des générations (anciennes, et nouvelles ainsi que sur la même génération), c’est-à-dire quand un nouveau nœud veut rejoindre le réseau, il faut faire des tests pour s’assurer que ce n’est pas un clone. Ce protocole fait beaucoup plus la prévention contre cette attaque, il a aussi un faible cout de communication et de mémoire par rapport à d’autres protocoles existants avec un taux de détection élevé.

Finalement, pour tester les performances du protocole choisis, nous avons fait la simulation et nous avons développé une plateforme constituée de capteurs telosB, ce qui nous a permis de tester le fonctionnement de notre programme et de démontrer son efficacité.

Perspectives

Pour avoir le meilleur protocole, ou bien pour trouver une solution parfaite contre cette attaque, il faut améliorer les résultats en termes de communication, de stockage en mémoire, et aussi d'élever le taux de détection par rapport aux protocoles déjà existants.

Ce projet nous a permis d'acquérir des connaissances en programmation évènementielle. Il nous a aussi fait découvrir un nouveau langage de programmation, le NesC et le simulateur TOSSIM, ainsi que la plateforme de programmation adéquate qui est TinyOs.

Comme perspective, il serait intéressant des perspectives envisagées pour ce travail, c'est d'utiliser la simulation pour avoir une vue générale sur le comportement du protocole à grandes échelles, avec la présence d'un grand nombre de clones afin de bien visualiser son fonctionnement et de pouvoir calculer les métriques d'évaluation du protocole.

BIBLIOGRAPHIE

[1] B. Parno, A. Perrig and V. Gligor, Distributed Detection of Node Replication Attacks in Sensor Networks, Proceedings of the IEEE Symposium on Security and Privacy, Berkley, Californie, USA, pp. 49-63, Mai 2005.

[2] K. BADER, Détection d'intrusions dans les réseaux de capteurs sans fil, Rapport de Stage 2009-2010.

[3] M. BADET, W. BONNEAU, Mise en place d'une plate-forme de test et d'expérimentation, Projet tutoré, 2005-2006.

[4] S.A.H. SEDJELMACI, Mise en œuvre de mécanismes de sécurité basés sur les IDS pour les réseaux de capteurs sans fil, Thèse de doctorat, Février 2013.

[5] K.BOUCHAKOUR, Routage hiérarchique sur les réseaux de capteurs sans fil : Protocol KhLCH (K-hop Layered Clustering Hierarchy), Thèse de magister, 2012.

[6] M.LEHSAINI, Diffusion et couverture basées sur le clustering dans les réseaux de Capteurs : application à la domotique, Thèse de doctorat, 2009.

[7] F.BOUHAMED, Détection des attaques par réplication dans un réseau de capteur Sans fil, Thèse de master, 2012.

[8] H.GUYENNET, D.MARTINS, Implémentation de mécanismes de sécurité Efficaces pour les réseaux de capteurs, Thèse de master, 2010.

[9] C.T.KONE, Conception de l'architecture d'un réseau de capteur sans fil deGrande dimension, Thèse de doctorat, 2011.

[10] C. DURAN-FAUNDEZ, Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie, Thèse de doctorat, 2009.

[11] Y.YOUNES, Minimisation d'énergie dans un réseau de capteurs, Thèse deMagister, 2012.

[12] A.SELATNA, Implémentation d'une application orientée surveillance pour lesRéseaux de capteurs, Thèse de master, 2012.

[13] Y.CHALLAL, Réseaux de capteurs sans fils, Support de cours, 2008.

[14] D.MARTINS, Sécurité dans les réseaux de capteurs sans fil, Stéganographie et réseaux de confiance, Thèse de doctorat, 2010.

[15] W.ZNAIDI, Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil, Thèse de doctorat, 2010.

[16] D.MARTINS, Sécurité dans les réseaux de capteurs sans fil (Stéganographie et réseaux de confiance), Thèse de doctorat, 2010.

[17] W.I.TAHRAOUI, A. BELHASSENA, Parallélisassions du chiffrement basé sur l'ECC dans les réseaux de capteurs sans fil, Thèse de Master, 2012.

[18] F.KHEDIM and N.LABRAOUI. Détection des Attaques par Réplication dans un Réseau de Capteurs Sans Fil. Conférence Nationale sur les Technologies de l'Information et les Télécommunications CNTIT'13, 10-11 Décembre 2013.

[19] B.SAHRAOUI, Etude d'un protocole de routage basé sur les colonies de Fourmis dans les réseaux de capteurs sans fil, Thèse de master, 2013.

[20] D. Liu and P. Ning, Establishing Pairwise Keys in Distributed Sensor Networks, In the Proc. of the 10th ACM Conference on Computer and Communication Security, Washington DC, USA, pp. 52-61, Octobre 2003.

[21] N. LABRAOUI, La sécurité dans les réseaux sans fil ad hoc: Agrégation de données et Localisation, Thèse de doctorat, 2012.

[22] W. Zhang, W. Liu, W. Lou and Y. Fang, Securing sensor networks with location-based keys, IEEE Wireless Communication and Networking Conference, New Orleans, USA, pp. 1909-1914, Mars 2005.

[23] K.Xing, X. Cheng, F. Liu, andD.H.C.Du, Real-time detection of clone attacks in wireless sensor networks, in Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08), pp. 3–10, Beijing, Chine, Juillet 2008.

[24] H. Choi, S. Zhu, and T. F. L. Porta, SET: detecting node clones in sensor networks, in Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm '07), pp. 341–350, Septembre 2007.

[25] F. Fei, L. Jing, and Y. Xianglan, Space-time related pairwise key predistribution scheme for wireless sensor networks, in Proceedings of the International Conference onWireless Communications,Networking andMobile Computing (WiCOM '07), pp. 2692–2696, Shanghai, China, Septembre 2007.

[26] C. Bekara and M. Laurent-Maknavicius, A new protocol for securing wireless sensor networks against nodes replication attacks, in Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '07),White Plains, NY, USA, Octobre 2007.

[27] W.Z. Khan, M.Y. AalSalem, M.N.B.M.Saad and Y. Xiang, Detection and Mitigation of Node Replication Attacks in Wireless Networks : A Survey, International journal of Distributed Sensor Networks, Mars 2013.

[28] B. Dutertre, S. Cheung and J. Levy, Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust, SDL Technical Report SRI-SDL-04-02, SRI International, 2004.

[29] S. Zhu, S. Setia, S. Jajodia,LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks, In Proc. of the 10th ACM Conf. on Computer and Communications Security, Washington DC, USA, pp. 62-72, Octobre 2003.

[30] T. Dimitriou and I. Krontiris, A Localized, Distributed Protocol for Secure Information Exchange in Sensor Networks, In Proc. of the 19th IEEE International Parallel and Distributed Processing Symposium, Denver, Colorado, USA, Avril 2005.

[31] A. Perrig, R. Szewczyk, V. Wen, D. Cullar and J. D. Tygar, Spins: Security protocols for sensor networks, In Proc. of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Rome, Italie, pp. 189-199, 2001.

ANNEXE : CODE SOURCE

Nous mettons à votre disposition quelques parties du code source des programmes qu'on a utilisé dans ce projet :

***pfeC.nc*(le fichier module➔ notre programme principal)**

```
#include <Timer.h>
#include "msg.h"
//#include "/opt/tinyos-2.x/tos/lib/printf.h"
/* ------------------------------------------------*/
* Définition des Interfaces
* Boot              Démarrage
* Leds              Gestion des leds
* Timer Gestion d'un timer
* AMControl     Contrôle interface radio
* Interfaces emission et réception trames
* ------------------------------------------------*/
modulepfeC {
uses interface Boot;
uses interface Leds;
uses interface Timer<TMilli> as TimerEnvoi;
uses interface Timer<TMilli> as Timetest;

/* Modules d'émission radio
*   uses interface SplitControl as AMControl;
/* Modules d'émission msg hello  */
uses interface Packet as Packet_hello;       /* Accès aux données du message */
uses interface AMPacket as AMPacket_hello; /* idem                              */
uses interface AMSend as AMSend_hello;            /* Envoi du paquet                  */
/* Modules d'émission msg test    */
uses interface Packet as Packet_test;        /* Accès aux données du message */
uses interface AMPacket as AMPacket_test; /* idem                              */
uses interface AMSend as AMSend_test;   /* Envoi du paquet                  */
```

```
/* Modules de réception Réponse            */
uses interface Receive as Receive_hello;
uses interface Receive as Receive_test;
}
implementation {
/* ---------------------------------------------
* Définition des variables
* ---------------------------------------------*/
uint16_t gene_n = 0;                /* compteur round                  */
uint16_t id;
boolbusy = FALSE;                   /* Booléen si la radio est occupée */
message_tpkthello ,pkttest,pktok;   /* Trames                          */
uint32_t tabespion[5];
```

pfeAppC*(Le fichier de configuration)*

```
#include <Timer.h>
#include "msg.h"
#pour raccorder les composants de notre programme
configurationpfeAppC {
}
implementation {
componentsMainC;
componentsLedsC;
componentspfeC as App;
components new TimerMilliC() as Timerenvoi;
components new TimerMilliC() as Timertest;
componentsActiveMessageC;
/* Gestion émission des données  */
components new AMSenderC(AM_HELLO_MSG)   as AMS_hello;
components new AMSenderC(AM_TEST_MSG)   as AMS_test;
/* Gestionréception des données  */
components new AMReceiverC(AM_HELLO_MSG) as hello_ReponseC;
```

```
components new AMReceiverC(AM_TEST_MSG) as test_ReponseC;
/* Association des Composants aux interfaces */
App.Boot ->MainC.Boot;
App.Leds ->LedsC;
App.TimerEnvoi ->Timerenvoi;
App.Timetest ->Timertest;
App.AMControl ->ActiveMessageC;
/* TRAME envoi                    */
App.AMSend_hello ->AMS_hello;
```

***msg.h*(l'entête)**

```
#ifndef MSG_H
#define MSG_H
typedefnx_structhello_msg {
nx_uint16_t id_node;
nx_uint16_tgenera;
        } hello_msg_t;
        enum {
AM_HELLO_MSG = 7,
AM_TEST_MSG = 9,
CODE_TEST =12345
        };
typedefnx_structtest_msg {
nx_uint16_tidm;
nx_uint16_t code;
nx_uint16_tcodea;
nx_uint16_tcodek;
        } test_msg_t;
```

test.py **le fichier qui contient le script python pour dérouler la simulation de notre programme**

```
#! /usr/bin/python
from TOSSIM import *
```

```
            import sys
            t = Tossim([])
            r = t.radio()
r.add(11, 10,-34.0)
r.add(10, 11,-34.0)
num_node = 13
t.addChannel("app", sys.stdout)
            #t.addChannel("node", sys.stdout)
            #t.addChannel("espion", sys.stdout)
             noise = open("noise.txt", "r")
lines = noise.readlines()

for line in lines:

str = line.strip()

if (str != ""):

val = int(str)

fori in range(1, num_node+1):

t.getNode(i).addNoiseTraceReading(val)

fori in range(1, num_node+1):

print "Creating noise model for ",i;
```

LISTE DES FIGURES

LISTE DES TABLEAUX

RESUME

Souvent déployés dans des environnements sans surveillance, les réseaux de capteurs sans fil peuvent être victimes de plusieurs attaques. L'attaque Clone est l'une des plus dangereuses car non seulement elle passe inaperçue pour le reste du réseau mais elle est en plus le point d'entrée, d'attaques internes qui peuvent avoir des conséquences désastreuses sur le réseau. Pour cela, beaucoup de méthodes et de propositions se sont intéressées pour éviter cette attaque mais l'absence d'une 'solution idéale' fait que plusieurs publications s'y consacrent encore.

Dans ce mémoire, nous présentons un protocole étudié qu'on a choisis qui fait une étude sur la prévention et la détection de l'attaque clone, les résultats d'analyse et d'implémentation ont prouvé l'efficacité de ce protocole et les coûts de communication et de stockage sont compétitifs par rapport aux autres solutions.

Mots clés : réseaux de capteurs sans fil (RCSF), la sécurité dans les RCSF, l'attaque clone.

ABSTRACT

Wireless sensor networks are often deployed in hostile environments, and can be subjected to a multitude of attacks. The clone attack is one of the more insidious because it not only goes undetectable for the rest of the network, but it is the entry point for most internal attacks that can have disastrous consequences on the network.

For this, many methods and proposals are interested to avoid this attack, but the absence of an 'ideal solution' that several publications are still spending. In this thesis, we present a protocol that has chosen that did a study on the prevention and detection of clone attack, the results of analysis and implementation have proven the effectiveness of this protocol and communication costs and storage are competitive compared to other solutions.

Keywords: wireless sensor networks (WSN), security in WSN, Clone attack.

ملخص

شبكات الاستشعار كثيرا ما تنتشر في بيئات معادية مما يعرضها لعدد وافر من الهجمات. الهجوم بالاستنساخ هو أخطرالهجمات، لأنه من جهة لا يمكن ملاحظته من طرف بقية الشبكة و من جهة أخرى هو يعد نقطة الدخول للعديد من الهجمات الداخلية التي يمكن أن يكون لها عواقب وخيمة على الشبكة. ولهذآ الكثير من الطرق و الاقتراحات حظت بالاهتمام لتفادي هدا الهجوم ، ولكن غياب الحل المثالي جعل الكثير من المنشورات تعالج هدا الموضوع.

في هده المدكرة نعرض بروتوكول من اختيارنا الدي يقوم بالدراسة عن الوقاية و الكشف عن الهجمات بالاستنساخ، نتائج التحليل والتطبيق بينت فعالية هدا البروتوكول،وتكاليف الاتصالات والتخزين هي تنافسية بالمقارنة مع الحلول الأخرى.

كلمات البحث: شبكات الاستشعار الاسلكية،الأمن في شبكات الاستشعار الهجوم بواسطة الاستنساخ.