Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Laboratoire STIC

UNIVERSITE ABOU BEKR BELKAID TLEMCEN
FACULTE DE TECHNOLOGIE
DEPARTEMENT DE TELECOMMUNICATIONS

MEMOIRE

Pour l'obtention du diplôme de

MASTER en

Réseaux Mobiles et Services de Télécommunication

Réalisé par

OTMANI Amina **BENDJELLOULI Leila**

THEME

Implémentation et sécurisation d'un RCSF pour la surveillance de la température.

Soutenu en Mai 2016 devant le Jury :

Abdelmalek Abdelhafid	Maitre de conférences à l'université de Tlemcen	Président
Mousaoui Djilali	Maitre de conférences à l'université de Tlemcen	Examinateur
Kadri Benamar	Maitre de conférences à l'université de Tlemcen	Encadreur

Année universitaire 2015-2016

Remercîment

Nous remercions tout d'abord le dieu tout puissant de nous armés de force et de courage pour mener à terme ce projet.

Nos sincères remerciements reviennent à monsieur Kadri Benamar, notre promoteur, pour sec conseils instructifs et pour son aide précieuse qui nous a conduits à l'aboutissement de ce modeste travaille.

Messieurs Mousaoui Djilali et Abdelmalek Abdlehafid, nous ont honorés de leur présence au jury de ce modeste travail.

Nos profonds remerciements vont également à toutes les personnes qui nous ont aidés et soutenue de près ou de loin.

Enfin, nous ne pouvons empêcher de remercier tout le corps enseignants de L'université Abou Bakr Belkaid De Tlemcen pour la qualité de l'enseignement qu'ils nous ont offerts et d'avoir bâti l'édifice intellectuel que nous sommes d'ores et déjà.

Dédicace

Je dédie ce modeste travail aux personnes que je sens chères pour moi, à ce qui m'ont soutenu, m'ontencouragé durant toute ma période d'étude et pour leur sacrifices consentis : A ma mère et mon père,que Dieu, le tout puissant, vous préserve et vous procure santéet longue vie.

A mes chères sœurs : Amel, Wissam et l'adorée Alae.

A mon chère frère Mohamed Read.

A ma chère cousine Houda et toute sa famille

A mon binôme : Amina Otmani et toute sa famille.

A mes amies, surtoutNadjet, Samira,ImenHidayet et Soumia.

A tous les membres de ma promotion réseau mobile et service de télécommunication RMST 2015 /2016.

A tous mes professeurs.

Bendjellouli Leila

Dédicace

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 du rêve.

Je dédie se travail :

A celle qui m'a donné la vie, ma comblé d'amour d'affection et d'encouragement pour que je devienne la femme que je suis aujourd'hui. A l'être le plus chère à mon cœur, ma mère.

A mon chère qui m'a éclairé le chemin de ma vie par son grand soutien et son encouragement et les énormes sacrifices qu'il m'a consenti durant mes études et qui a toujours aimé me voire réussir.

Je les remercie pour tout ce qu'ils mon fait, et j'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

A mon très cher mari (Youcef),A Tes sacrifices, ton soutien moral et matériel m'ont permis de réussir mes études. Ce travail soit témoignage de ma reconnaissance et de mon amour sincère et fidèle.

Puisse Dieu, vous procure santé, bonheur et langue vie.

A mon frère (Yassine) A ma petite sœur (Assia) qui sont les plus proches personnes à moi.

A ma grande mère ainsi que mes oncles, tantes, cousins et cousines et toute ma famille.

A ma deuxième famille, lafamillede mon mari.

Son oubliée tous mes amies surtout mon binôme Leila et tous sa famille.

En fin à tous ceux qui ont contribué d'une maniéré ou d'une autre à l'élaboration de ce travail.

OtmaniAmina

Table de matière

Chapitre 4 : déploiement d'un RCSF sécurisé

Table de figure

Liste de tableau

Introduction générale

AU cours de ces dernières années, le développement technologique des réseaux de communication sans fils, a connu un essor important grâce aux avancés technologiques dans divers domaines, tels que la micro-électronique et sa miniaturisation. C'est ainsi que de nouvelles voies d'investigation ont été ouvertes, avec l'émergence des réseaux de capteurs sans fil des réseaux a hôtes autonomes et à infrastructure non prédéfinie utilisés dans des domaines très variés tels que la détection de flux de radiation, le suivi d'objets en déplacement et leur positionnement.

Les réseaux de capteurs sans fil (RCSF)- Wireless Sensor Networks (WSN) – sont Considérés comme un type spécial de réseaux ad hoc.

Le développement des RCSFs était originalement motivé par les applications militaires (surveillance des champs de bataille, localisation de l'ennemie…). Néanmoins, leurs performances remarquables en termes de fiabilité et de faible coût ont permis de proliférer leur utilisation dans le domaine d'application civil (surveillance d'environnement, l'industrie, la domotique, la santé…).

Les nœuds de ce type de réseaux sont conçus pour être déployés d'une manière dense dans des endroits hostiles et difficiles d'accès, d'où la nécessité de limiter au maximum leurs dimensions physiques qui s'obtiennent impérativement au détriment des capacités de calcul de traitement et de ressources énergétiques. 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.

En raison des caractéristiques de ces réseaux de capteurs, ils 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.

L'objectif de notre étude de l'aspect sécurité dans ce type réseau. Pour cela, nous avons organisé notre travail en 4 chapitres comme suit :

Le premier chapitre 1 : nous parlerons en général sur les réseaux de capteurs sans fil et leurs caractéristiques.
Le deuxième chapitre 2 : nous citons les différents attaque qui peut découler les RCSFs, et nous avant donner quelque solution qui permet d'offrir la sécurité pour n'importe quelle système de communication.
Le troisième chapitre 3 : nous avant étudier des solutions adaptées à RCSFs.
Le quatrième et le dernier chapitre 4 : nous proposons une solution pour assurer un certain niveau de sécurité et nous terminons par une implémentation de notre programme.


Chapitre 1

Introduction :

Les récents progrès et les nombreuses avancées technologiques dans les domaines de la micro-électronique et les progrès atteints dans les domaines d'intégration et de la miniaturisation ont permis la fabrication d'entités miniaturisées, communément appelées capteurs, faibles en cout et de plus en plus performantes, capables de se disposer dans l'environnement de manière aisée sans altération du paysage ambiant. Egalement, le progrès des technologies de communication sans fil a permis aux capteurs d'être plus autonomes ce qui favorise un déploiement facile et rapide dans des endroits difficile d'accès ou complètement inaccessibles. Sur un champ de captage, les capteurs coopèrent entre eux sans aucune intervention externe (humaine, infrastructure de base…etc.) pour former une infrastructure de communication dite réseau de capteurs sans fil

Un réseau de capteurs sans fil est composé de plusieurs milliers de capteurs communicants via des liaisons sans fil placés dans des endroits précis ou dispersés aléatoirement sur une zone à surveiller, capables de collecter, traiter et s'auto-organiser afin de transmettre des informations sur leur environnement

Dans ce chapitre, nous présenterons les réseaux de capteurs sans fil, leurs architectures de communication, leurs applications. Nous discuterons également les principaux facteurs et contraintes qui influencent la conception des réseaux de capteurs sans fil.

I. Réseaux Adhoc :

Un réseau sans-fil ad hoc (ou MANET, pour Mobile Ad hoc NETwork) est formé par un ensemble d'hôtes qui s'organisent seuls et de manière totalement décentralisée, formant ainsi un réseau autonome et dynamique ne reposant sur aucune infrastructure filaire.
Ces hôtes peuvent être fixes ou mobiles. Selon ces hypothèses, tous ensemble d'objets munis d'une interface de communication adéquate est susceptible de spontanément former un tel réseau.
Aucune infrastructure n'étant disponible, ces objets ont donc à découvrir dynamiquement leur environnement.
Un réseau ad hoc étant avant tout un réseau sans-fil, les objets communiquent entre eux par le biais d'une interface radio. Ces communications sont donc soumises aux phénomènes physiques qui régissent les ondes radio, telle qu'une forte atténuation du signal avec la distance. Ainsi, seuls les hôtes suffisamment proches les uns des autres sont capables de communiquer directement ensemble, et les communications de longue distance doivent s'effectuer par le biais d'un mécanisme nommé multi-sauts : cela signifie simplement que certains objets doivent relayer les messages de proche en proche jusqu'à ce que leur acheminement soit effectué. L'utilisation d'une antenne radio omnidirectionnelle implique également qu'un message envoyé par un émetteur quelconque est reçu par tous les récepteurs suffisamment proches de lui.

La figure I.1 illustre un réseau sans-fil classique tel que l'on peut par exemple en trouver dans les gares et les aéroports. L'infrastructure y est composée de deux points d'accès P1 et P2 reliés grâce à une liaison filaire classique, et qui servent de points d'entrée aux hôtes du réseau. Lorsque l'objet A désiré communiquer avec l'objet D, il envoie les messages à P1 qui les fait suivre à P2, ce dernier les envoyant à D.

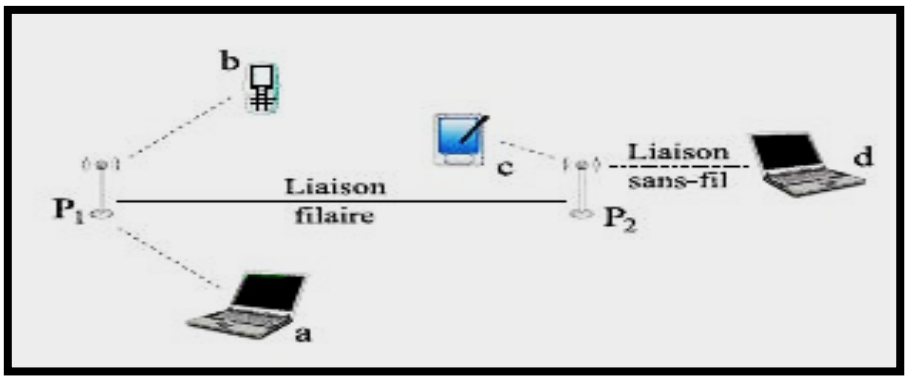


Figure I.1 : Réseau sans-fil classique

La figure I.2 illustre un réseau ad hoc pour lequel aucune infrastructure n'est nécessaire pour que les hôtes puissent communiquer ensemble. L'objet C doit donc servir de relais afin qu'a puisse communiquer avec D.

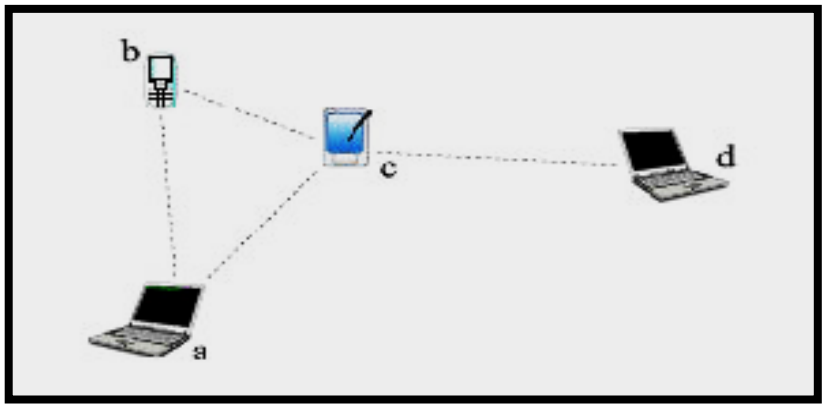


Figure I.2 : Réseau sans-fil adhoc.

Les applications de ces réseaux sont multiples, et concernent principalement les zones où une infrastructure filaire est indisponible ou non désirable. C'est par exemple le cas dans les zones sinistrées par un désastre naturel, où les secours ont un grand besoin de communication. C'est aussi le cas lorsque la rapidité et la discrétion sont des facteurs déterminants : on ne peut raisonnablement imaginer le déploiement d'une infrastructure de communication complète lors de manœuvres militaires en territoire ennemi. D'autres cas plus légers d'utilisation peuvent également survenir. Ainsi, pour des raisons de coût, il n'est, par exemple, pas possible de mettre en place une infrastructure filaire le temps d'une réunion en plein air. Dans tous ces exemples, l'utilisation d'un réseau ad hoc peut s'avérer indispensable. **[1]**

II. Réseaux de capteurs sans-fil (RCSF)

II.1 Définition d'un capteur :

UN capteur est un dispositif transformant l'état d'une grandeur physique observée en une grandeur utilisable, telle qu'une tension électrique (qui sera à son tour traduite en une donnée binaire exploitable et compréhensible par un système d'information).

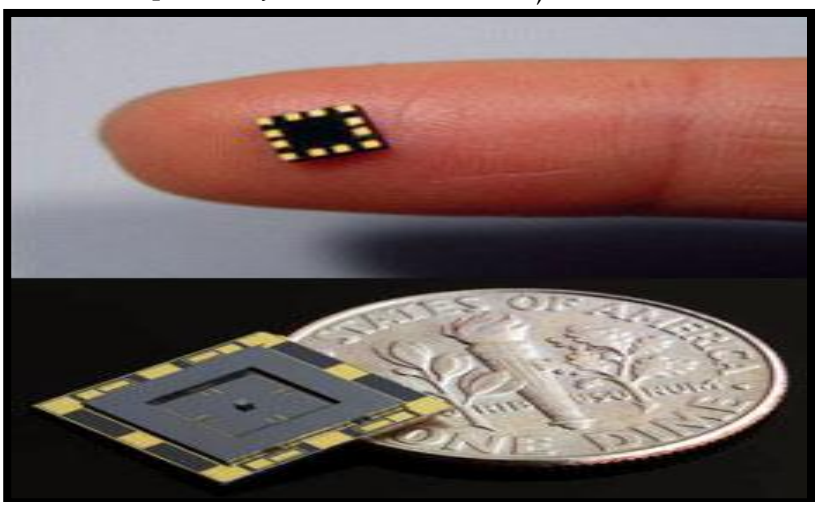


Figure I.3 : différent capteurs [7]

1I.2 Définition d'un Réseaux de capteur sans fil :

Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Les nœuds capteurs sont des capteurs intelligents "smart sensors", capables d'accomplir trois tâches complémentaires : le relevé d'une grandeur physique, le traitement éventuel de cette information et la communication avec d'autres capteurs. L'ensemble de ces capteurs, déployés pour une application, forme un réseau de capteurs. Le but de celui-ci est de surveiller une zone géographique, et parfois d'agir sur celle-ci (il s'agit alors de réseaux de capteurs-actionneurs). On peut citer comme exemples un réseau détecteur de feu de forêt, ou un réseau de surveillance de solidité d'un pont après un tremblement de terre.

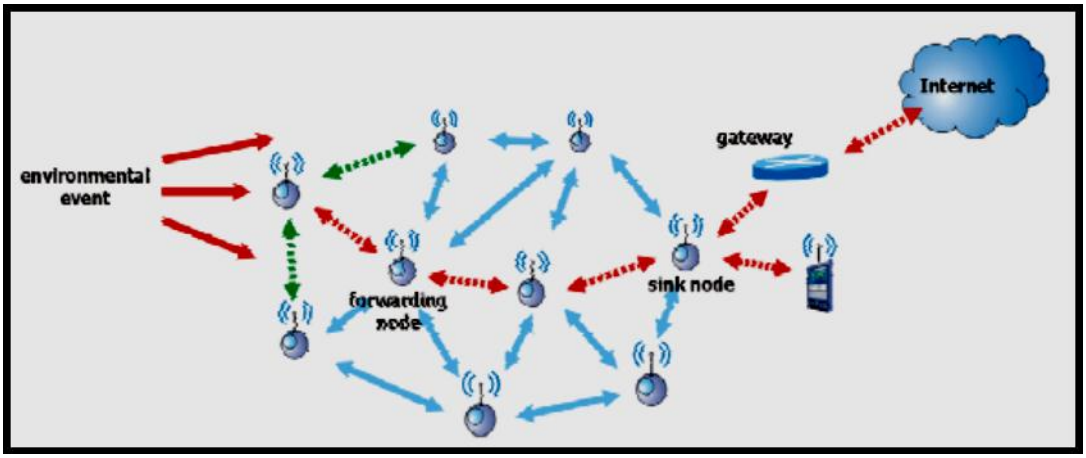


Figure I.4 : réseau de capteur

Le réseau peut comporter un grand nombre de nœuds (des milliers). Les capteurs sont placés de manière plus ou moins aléatoire (par exemple par largage depuis un hélicoptère) dans des environnements pouvant être dangereux. Toute intervention humaine après le déploiement des nœuds capteurs est la plupart du temps exclue, le réseau doit donc s'autogérer. Afin que les nœuds capteurs travaillent d'une façon coopérative, les informations recueillies sont partagées entre eux par voie hertzienne. Le choix du lien radio plutôt que du lien filaire permet un déploiement facile et rapide dans un environnement pouvant être inaccessible pour l'être humain. **[2-3]**

III. Les types des réseaux capteurs :

Il existe actuellement un grand nombre de capteurs, avec des fonctionnalités diverses et variées. La plupart de ces capteurs dépendent de l'application et l'environnement pour lesquels ils ont été conçus **[7].** Il existe cinq types de réseaux de capteurs : terrestre, souterrain, multimédia, mobile et sous-marin.

III.1 Les réseaux capteurs terrestres :

Dans un réseau de capteurs terrestre, la communication fiable dans un environnement dense est très importante. Les nœuds capteurs terrestres doivent être capables de communiquer efficacement les données vers la station de base. **[8]**

➢ Domaine d'application :

- Applications militaires : serviraient à indiquer la position de troupes militaires sur le terrain
- Applications domestiques : En plaçant sur le plafond ou dans le mur (la présence d'un gaz, la luminosité...)
- détecter des incendies.
- surveiller des catastrophes naturelles.
- détecter des pollutions.
- Applications médicales
- Applications de transport… etc

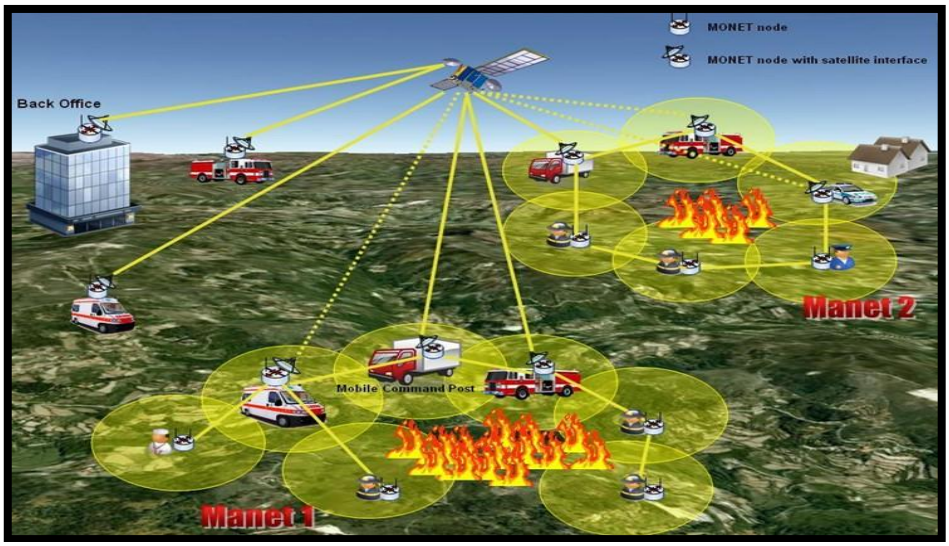


Figure I.5 : Domaine d'application des capteurs terrestres

III.2 Les réseaux capteurs souterrains :

Les réseaux de capteurs souterrains se composent d'un nombre des nœuds capteurs enfouis sous terre ou dans une grotte ou une mine utilisés pour surveiller les conditions souterraines. Les nœuds sink additionnels sont situés au-dessus du sol pour relayer l'information à partir des nœuds capteurs vers la station de base. **[8]**

➢ Domain d'utilisation :

- Applications militaires.
- Applications environnementales
- Applications agricoles.
- Les recherches géologiques.

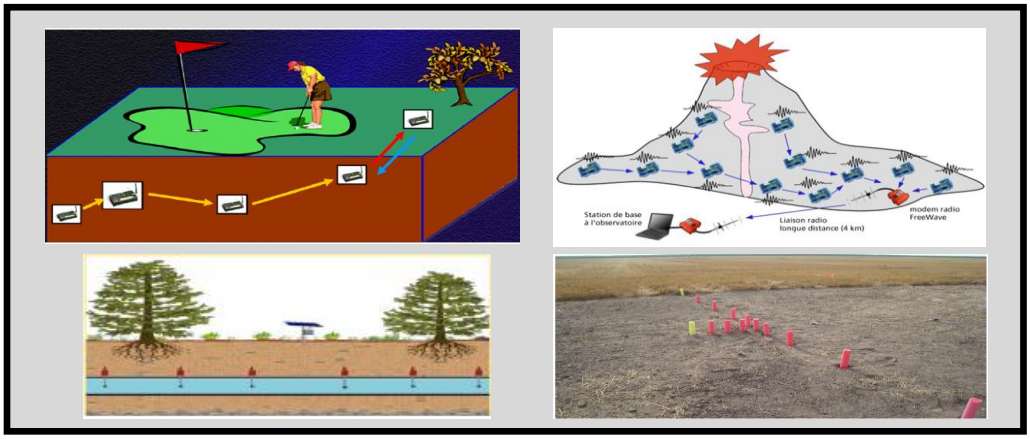


Figure I.6 : Les applications des capteurs souterraines

III.3 Les réseaux capteurs multimédias :

Les réseaux de capteurs multimédias ont été proposés pour permettre la surveillance et le suivi des événements dans la forme de multimédia comme la vidéo, l'audio et l'image. **[9]**

Figure I.7 : Les applications des capteurs multimédias

III.4 Les réseaux de capteurs mobiles :

Les réseaux de capteurs mobiles sont constitués d'un ensemble de nœuds capteurs qui peuvent se déplacer par leurs propres moyens et d'interagir avec l'environnement physique.

Figure I.8 : Les RCSF mobiles

III.5 Les réseaux de capteurs sous-marins :

Le réseau de capteur sans fil aquatique est une technologie dédiée aux applications marines (dans l'eau). Ce type de réseau est composé d'un nombre variable de capteurs et de véhicules sous-marins autonomes, déployés pour effectuer des tâches de surveillance ou de collecte de données dans une zone définie. [11]

- **Domain d'utilisation :**

Applications UWSN gagnent rapidement en popularité pour permettre des avancées dans le domaine de la surveillance des océans et des systèmes de l'observatoire, la surveillance en haute mer, le suivi des différentes entités de l'environnement aquatique, et déterrer des ressources. UWSNs trouvent leur application dans des domaines comme le pétrole et l'extraction de gaz, les déversements de pétrole, la surveillance militaire et de reconnaissance, la détection des mines, la surveillance de la pollution, les catastrophes naturelles comme le tsunami et la prévision des ouragans, des récifs coralliens et de surveillance de l'habitat de la vie marine, et de la pisciculture.

Figure I.9 : photo des différentes applications

IV. La pile protocolaire dans un RCSF

Le rôle de cette pile consiste à standardiser la communication entre les participants afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles.

Ce modèle comprend 5 couches qui ont les mêmes fonctions que celles du modèle OSI ainsi que 3 couches pour la gestion de la puissance, la gestion de la mobilité et la gestion des taches.

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction.

Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur. **[6]**

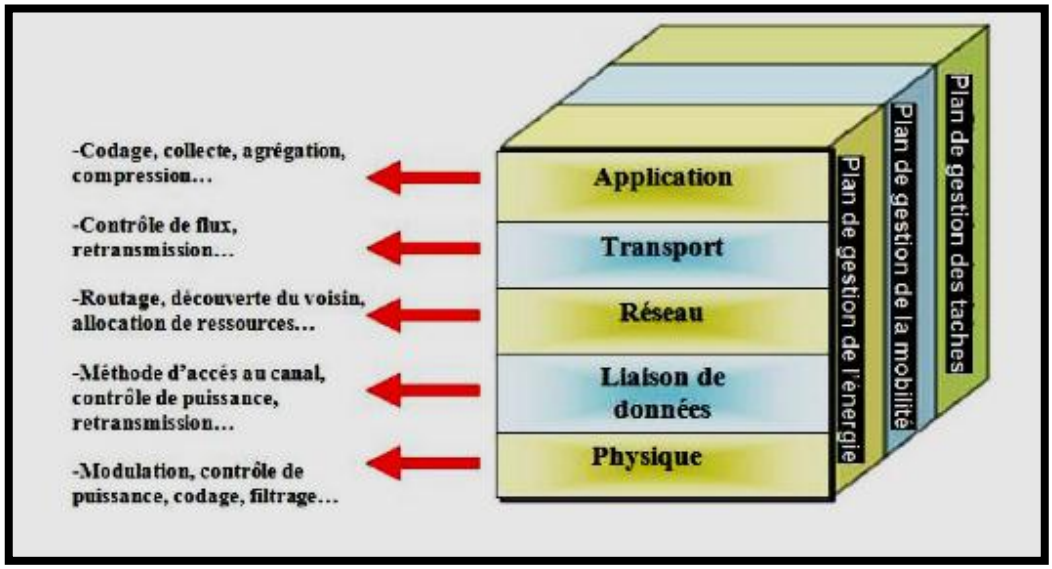


Figure I.10 : Pile protocolaire dans les réseaux de capteurs.

Suivant la fonctionnalité des capteurs, différentes applications peuvent être utilisées et bâties sur la couche application. La couche transport aide à gérer le flux de données si le réseau de capteurs l'exige. Elle permet de diviser les données issues de la couche application en segments pour les délivrer, ainsi elle réordonne et rassemble les segments venus de la couche réseau avant de les envoyer à la couche application. La couche réseau prend soin de router les données fournies par la couche transport. Le protocole MAC (Media Access Control) de la couche liaison assure la gestion de l'accès au support physique. La couche physique assure la transmission et la réception des données au niveau bit.

En outre, les plans de gestion de l'énergie, de la mobilité et des tâches surveillent la puissance, le mouvement et la distribution des tâches, respectivement, entre les nœuds capteurs. Ces plans de gestion sont nécessaires, de sorte que les nœuds capteurs puissent fonctionner ensemble d'une manière efficace pour préserver l'énergie, router des données dans un réseau de capteurs mobile et

partager les ressources entre les nœuds capteurs. Du point de vue global, il est plus efficace d'utiliser des nœuds capteurs pouvant collaborer entre eux. La durée de vie du réseau peut être ainsi prolongée. [13]

V. Les architectures :

V.1 L'architecture d'un nœud capteur :

Un nœud capteur contient quatre unités de base :

- l'unité de captage,
- l'unité de traitement,
- l'unité de transmission,
- et l'unité de contrôle d'énergie. (voir le chapitre4)

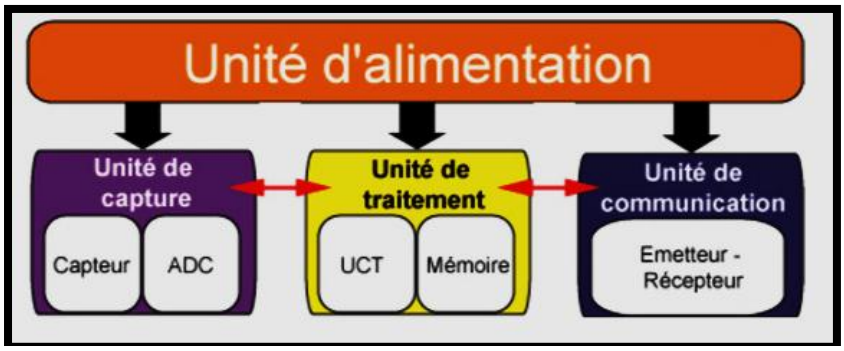


Figure I.11 : Architecture d'un capteur sans fils

Il peut contenir également, suivant son domaine d'application, des modules supplémentaires tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire). On peut même trouver des micro-capteurs, Un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le micro-capteur en cas de nécessité.

V.2 L'architecture d'un RCSF

Un réseau de capteurs sans-fil est composé d'un ensemble de dispositifs très petits nommés nœuds capteurs et d'une ou de plusieurs stations de base appelées « Sink nodes » ou nœuds puits qui sont considérés comme l'interface entre le réseau de capteurs et l'utilisateur final.

Les nœuds capteurs, dont le nombre peut atteindre des dizaines de millions d'éléments pour certaines applications, sont des entités caractérisées par leur cout très réduit, leur taille minuscule généralement en quelques millimètres de volume et leurs ressources limitées en calcul, en mémoire et notamment en énergie. Ils sont déployés sur une zone de capture, soit aléatoirement (largage par avion ou par hélicoptère par exemple) ou d'une manière déterministe en choisissant leurs emplacements, dans le but de collecter des données de leur environnement telles que les grandeurs physiques comme l'intensité de la luminosité, la température, l'humidité, les vibrations…etc., et de

les router vers la station de base. Ils participent en conséquence à un partage organisé d'informations par des traitements coopératifs. [5]

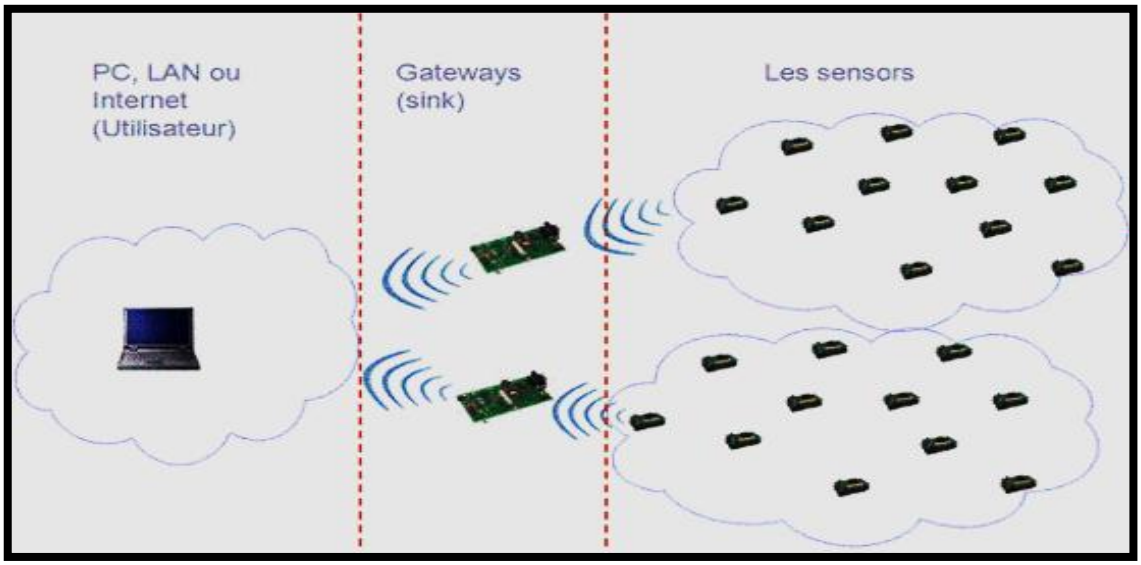


Figure I.12 : l'architecture d'un RCSF [6]

La station de base, jouant à la fois le rôle de collecteur final et de passerelle vers d'autres réseaux, sert à collecter l'ensemble des informations provenant des nœuds capteurs et de les transmettre par d'autres moyens (réseau filaire, internet, satellite…etc) à un utilisateur final. De plus, l'utilisateur final peut utiliser la station de base comme une passerelle pour diffuser ses requêtes sur le réseau.

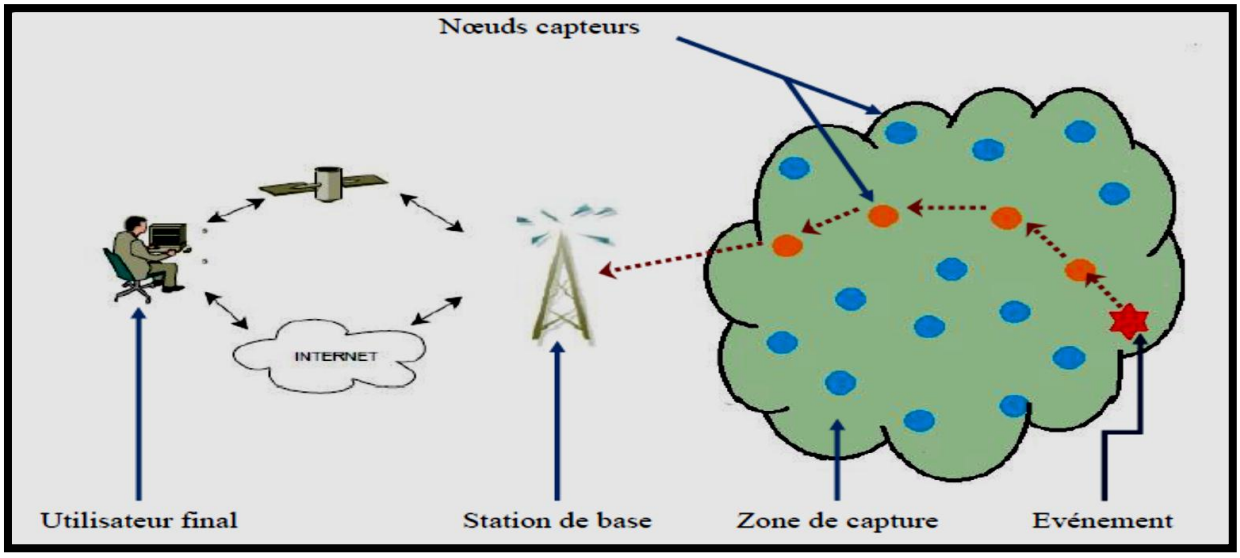


Figure I.13 : exemple d'un RCSF [5]

Il existe deux types d'architectures pour les réseaux de capteurs sans fil :

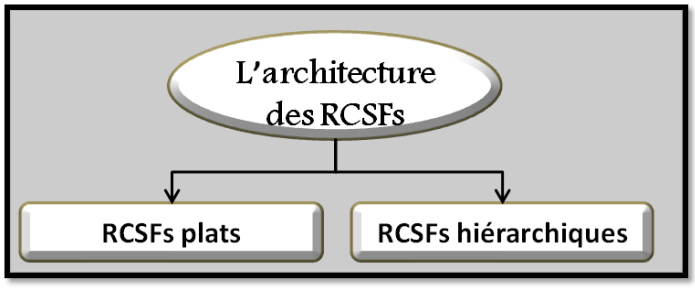


Figure I.14 : types d'architectures RCSFs

V.2.1 Les réseaux des capteurs sans fils plats :

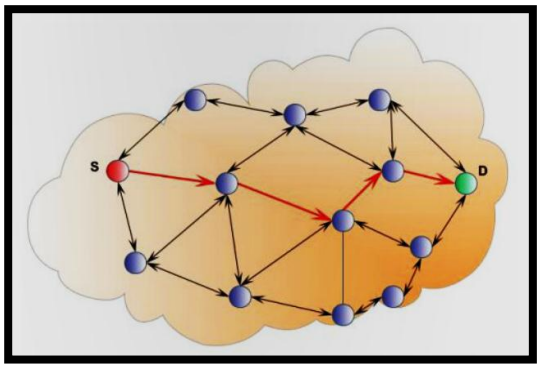


Figure I.15 : RCSFs plats

Un réseau de capteurs sans fil plat est un réseau homogène, ou tous les nœuds sont identiques en termes de batterie et de complexité du matériel, excepté le Sink qui joue le rôle d'une passerelle et qui est responsable de la transmission de l'information collectée à l'utilisateur final. Selon le service et le type de capteurs, une densité de capteurs élevée (plusieurs nœuds capteurs/m2) ainsi qu'une communication multi-saut peut être nécessaire pour l'architecture plate. En présence d'un très grand nombre de nœuds capteurs, la scalabilité devient critique. Le routage et le contrôle d'accès au médium (MAC) doivent gérer et organiser les nœuds d'une manière très efficace en termes d'énergie.

V.2.2 Les réseaux de capteurs hiérarchiques :

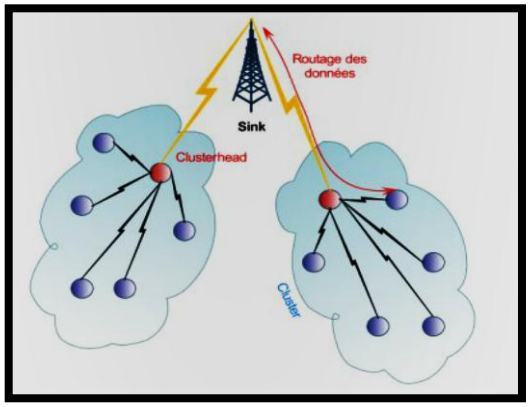


Figure I.16 : RCSF hiérarchiques

Une architecture hiérarchique était proposée pour réduire le coût et la complexité de la plus part des nœuds capteurs en introduisant un ensemble de nœuds capteurs plus coûteux et plus puissant, ceci en créant une infrastructure qui décharge la majorité des nœuds simples à faible coût de plusieurs fonctions du réseau. L'architecture hiérarchique est composée de multiples couches : une couche de capteurs, une couche de transmission et une couche de point d'accès. **[14]**

VI. Caractéristiques des RCSF

Un réseau de capteurs sans fil possède plusieurs caractéristiques dont :

- Ressources limitées des capteurs en calcul, en mémoire et en énergie.
- Durée de vie limitée.
- Mode de communication direct ou en multi-sauts.

- Densité importante des capteurs qui peuvent atteindre des dizaines de millions pour certaines applications.
- Possibilité de découper le réseau en clusters et d'utiliser les capteurs comme calculateurs ou des agrégateurs.
- La coopération entre les nœuds capteurs pour les taches complexes.
- Absence d'un identifiant global pour les capteurs.
- Deux modes de fonctionnement : « Un à plusieurs » où la station de base diffuse des informations aux différents capteurs et « Plusieurs à un » où les nœuds capteurs diffusent des informations à la station de base. **[2]**

VII. Système d'exploitation TinyOS

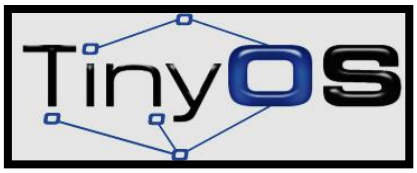


Figure I. 17 : Logo de TinyOS.

TinyOS est un système d'exploitation intégré, modulaire, destiné aux réseaux de capteurs miniatures. Cette plate-forme logicielle ouverte et une série d'outils développés par l'Université de Berkeley est enrichie par une multitude d'utilisateurs. En effet, TinyOS est le plus répandu des OS pour les réseaux de capteurs sans-fil. Il est utilisé dans les plus grands projets de recherches sur le sujet (plus de 10.000 téléchargements de la nouvelle version). Un grand nombre de ces groupes de recherches ou entreprises participent activement au développement de cet OS en fournissant de nouveaux modules, de nouvelles applications,... Cet OS est capable d'intégrer très rapidement les innovations en relation avec l'avancement des applications et des réseaux eux même tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs. La librairie TinyOS comprend les protocoles réseaux, les services de distribution, les drivers pour capteurs et les outils d'acquisition de données. TinyOS est en grande partie écrit en C mais on peut très facilement créer des applications personnalisées en langages C, NesC, et Java.

VIII. Les problématiques :

Il y'a plusieurs problèmes dans les RCSF, en citant :

VIII.1 L'absence d'infrastructure

Les réseaux de capteurs sont constitués de plusieurs capteurs minuscules ou nœuds ayant une caractéristique essentielle résidant dans l'absence d'infrastructure fixe et ayant une topologie changeante due à la mobilité des capteurs et pose le problème des communications sans fil entre les autres capteurs ainsi que le problème de l'épuisement de leurs batteries. **[15]**

VIII.2 Environnement de déploiement

Dans la majorité des applications, les nœuds capteurs sont déployés dans des zones distantes, hostiles et sans aucune surveillance ni intervention humaine. Les capteurs doivent être conçus pour résister aux différentes conditions climatiques telles que la chaleur, l'humidité, le froid, la pression …etc.

VIII.3 Topologie du réseau

L'ajout de nouveaux capteurs sur la zone de captage ou la défection d'un ou de plusieurs nœuds capteurs du réseau peut causer une instabilité de la topologie du réseau. **[5]**

VIII.4 Routage des données

Le routage dans les RCSF est un routage multi-sauts. Un nœud consomme de l'énergie soit pour transmettre ces données soit pour relayer les données des autres nœuds.

Pour limiter le nombre de communications coûteuses en énergie, les réseaux de capteurs sans fil utilisent des protocoles de routage efficaces. Une solution souvent utilisée est la clusterisation, qui divise le réseau en plusieurs clusters. Dans chacun de ces clusters, un nœud maître (cluster-head) est élu et aura pour mission de récupérer les informations des nœuds du cluster dont il a la charge pour les transmettre aux autres clusters et inversement.

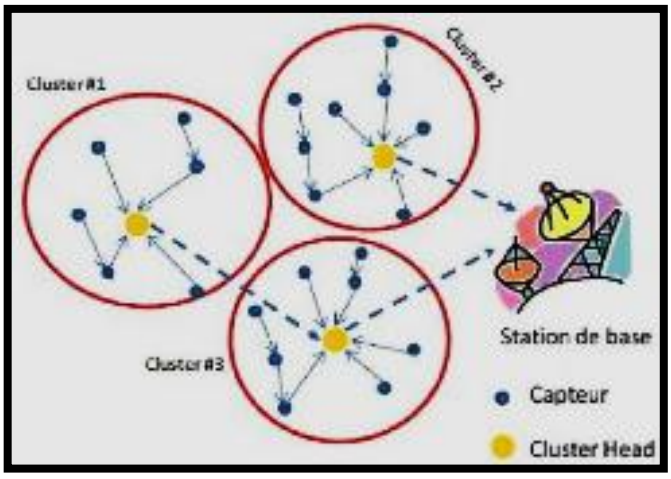


Figure 1.18 : exemple d'un RCSF utilise les 3 clusters

Le choix du nœud maître sera fait en désignant par exemple les nœuds avec l'énergie la plus importante, pour augmenter la vie du réseau.

D'autres problèmes de routage doivent aussi être pris en compte pour limiter le nombre de communications comme les problèmes d'implosion ou de chevauchement

Dans ce contexte, une mauvaise politique de routage peut avoir des conséquences graves sur la durée de vie du réseau.

VIII.5 Faible puissance de calcul

Malgré les progrès récents dans la fabrication de capteurs de plus en plus puissants, les capteurs actuels souffrent d'un manque de puissance de calcul (par exemple seulement 16 Mhz de puissance et 128Koctets de mémoire programmable pour un capteur MicaZ).

Cette faible puissance ne permet pas d'utiliser des algorithmes complexes dans les réseaux de capteurs sans fil, et particulièrement dans la cryptographie poussée.

De plus la vocation des capteurs sans fil est d'être en très grand nombre et leur utilisation dans des applications avec un nombre de nœuds élevé nécessite l'utilisation des capteurs bons marchés, ce qui impliquent des capteurs avec une puissance de calcul très faible.

La faiblesse de la puissance de calcul est aussi préjudiciable pour le temps de réponse du réseau. Si l'on demande à un capteur d'effectuer de nombreux calculs, sa réactivité va sensiblement se détériorer. **[17]**

VIII.6 Les Pannes :

Le réseau doit être capable de maintenir ses fonctionnalités sans interruption en cas de défaillance d'un de ses capteurs. Cette défaillance peut être causée par une perte d'énergie, dommage physique, interférence de l'environnement ou compromission des nœuds …etc.

Ces pannes ne doivent pas affecter le fonctionnement global du réseau. La tolérance aux pannes se définie alors comme la capacité du réseau à continuer à fonctionner normalement sans interruption même après le dysfonctionnement d'un ou de plusieurs de ses nœuds capteurs. **[5]**

VIII.7 La consommation d'énergie

Les capteurs sont conçus pour fonctionner durant des mois voire des années. Ainsi, la capacité énergétique des capteurs doit être utilisée efficacement afin de maximiser la durée de vie du réseau. A noter qu'une fois qu'un nœud capteur a épuisé son énergie, il est considéré comme défaillant.

Ainsi, il y a une forte probabilité de perdre la connectivité du réseau. Donc l'énergie est une contrainte clé dans les réseaux de capteurs.

Il est nécessaire d'avoir une stratégie efficace qui prend en considération l'énergie du réseau pour augmenter sa durée de vie en réduisant la perte d'énergie tout en étant réactive aux changements de l'environnement.

La consommation énergétique du module de surveillance dépend énormément du matériel employé et de la nature du phénomène observé. L'économie d'énergie obtenue par la mise en veille de certains nœuds pour l'observation est donc très variable. **[13]**

VIII.8 Coût de production :

Le cout de production d'un seul capteur est très important pour l'évaluation du cout global du réseau. Si ce dernier est supérieur à celui nécessaire pour le déploiement des capteurs classiques, l'utilisation de cette nouvelle technologie ne serait pas financièrement justifiée. **[16]**

VIII.9 Sécurité

L'objectif premier des nœuds d'un RCSF est de rassembler des donnes de surveillance et de les transmettre a un lieu de décision, cette opération doit se faire sans interférences malicieuses et avec un niveau de sécurité approprie.

Souvent déployés dans des environnements hostiles, les réseaux de capteurs sans fil peuvent être sujets à plusieurs types d'attaques. Afin d'assurer une fiabilité maximale du système, différents mécanismes de sécurité sont développés dans le but d'éliminer toute menace capable d'atteindre à la sécurité des informations échangées,

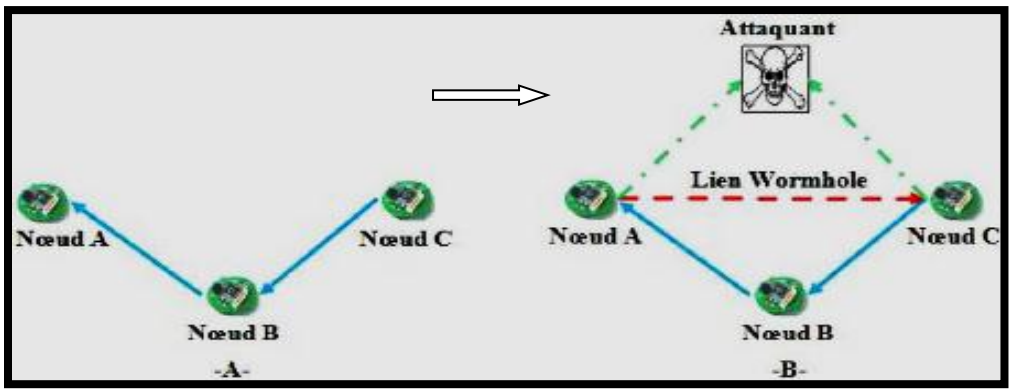


Figure I.19 : exemple d'une attaque sur un RCSF

Dans le chapitre suivant, nous présenterons la sécurité dans les réseaux de capteurs sans fil.

Conclusion

Les réseaux de capteurs sans fil sont une nouvelle technologie qui a surgi après les grands progrès technologiques concernant le développement des capteurs intellige.

De ce fait, le RCSF est un nouveau domaine de recherche s'est produit pour proposer des solutions économiquement favorables et facilement déployées à la surveillance et le traitement des données dans les milieux complexes et éloignés.

Nous avons présenté dans ce chapitre, des généralités sur les réseaux de capteurs sans fil.

La description que nous avons faite sur ces réseaux fournira au lecteur les bases nécessaires à la compréhension de la suite de document et le sensibilisera aux problématiques liées à nos travaux.

Et finalement nous avons déduire que les grands problèmes qui limitent les RCSF sont, le problème de la sécurité et de la tolérance aux pannes.

Afin de résoudre ces limites par une surveillance permanente d'un RCSF, nous consacrons le chapitre suivant pour détailler la notion de sécurité dans les réseaux de capteurs sans fil.


Chapitre 2

Introduction :

La sécurité est un domaine très important pour les RCSFs, particulièrement pour des applications sensibles du domaine militaire, médicale, et autres. La sécurité devrait intervenir pour certaines fonctions sensibles telles que l'expédition des paquets, le cheminement et la gestion d'un réseau, fonctions effectuées par certains ou tous les nœuds disponibles dans les RCSFs. En raison des différences de base entre réseaux fixes et des réseaux ad hoc généraux, la sécurité dans les RCSFs devrait être examinée avec beaucoup plus de minutie. Dans ce chapitre nous parlant de la sécurité dans ce type de réseau. Nous montrons quelles sont les vulnérabilités qui en découlent les RCSFs. Nous présentons ensuite une liste des attaques que l'on peut trouver dans ces réseaux particuliers et les solutions apportées par la communauté scientifique pour les sécuriser.

I. Les besoins de sécurité dans RCSF :

La sécurité constitue actuellement l'un des principaux obstacles à un large déploiement des réseaux ad hoc. Sécuriser un réseau ad hoc revient à instaurer les différents services de sécurité dans ce réseau, tout en prenant en compte ses différentes caractéristiques. [1]

La sécurité est une nécessite pour la majorité des applications qui utilisent les RCSFs, notamment si les nœuds capteurs sont déployés dans des endroits peu surs, tels que les champs de bataille, les lieux stratégiques (aéroports, bâtiments critiques, etc.). Ces nœuds capteurs qui opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie, peuvent être soumis à des actions perturbatrices et malveillantes susceptibles de compromettre l'essence même d'un RCSF. C'est pourquoi, il est primordial de pouvoir leur assurer un niveau de sécurité acceptable.

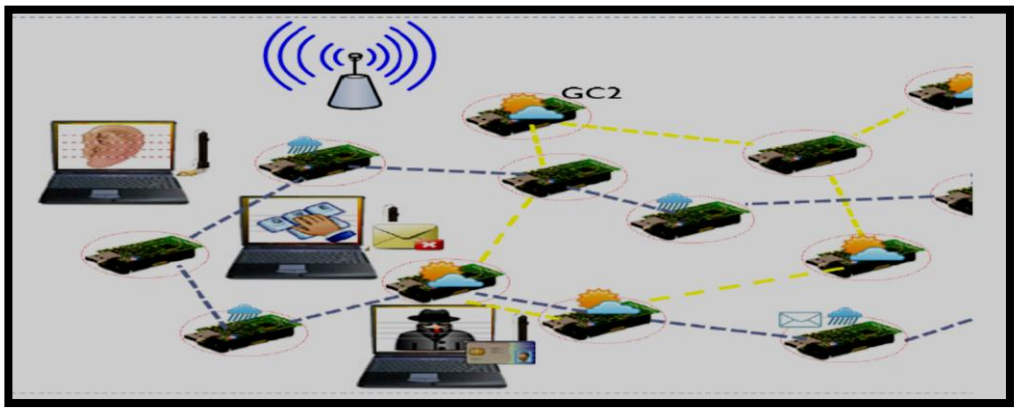


Figure II.1 : exemple sur les différentes attaques dans les RCSFs

II. Objectif et service de base de la sécurité :

La sécurité peut être définie comme la gestion du risque qui menace la confidentialité, l'intégrité, la fraicheur et la disponibilité des données.

II.1 La confidentialité des données :

La confidentialité des données est la question la plus importante dans la sécurité de réseau.

Elle consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées

L'approche standard pour sécuriser le transfert des données est de crypter les données avec une clef secrète connue par l'émetteur et le récepteur. [19]

II.2 L'intégrité :

Un nœud intrus (adversaire) peut modifier les données transférées. Par exemple, un nœud malveillant peut ajouter quelques fragments ou manœuvrer les données dans un paquet.

Ce nouveau paquet peut alors être envoyé au récepteur original. La perte ou les dommages de données peut même se produire sans présence d'un nœud malveillant dû à l'environnement dur de communication. Ainsi, l'intégrité des données s'assure qu'aucune donnée reçue n'a été changée en transit. [19]

II.3 L'authentification :

Consiste à vérifier l'identité authentique des nœuds. En effet, on ne peut assurer la confidentialité et l'intégrité des messages échangés si, dès le départ, on n'est pas sûr de communiquer avec le bon nœud. Si l'authentification est mal gérée, un attaquant peut se joindre au réseau et injecter des messages erronés. En raison de la nature du support sans fil et la nature des réseaux de capteurs (déployés dans des zones hostiles et sans surveillance), il est extrêmement difficile d'assurer l'authentification. [18]

II.4 La disponibilité :

La disponibilité permet de préciser si le réseau est libre pour la communication des messages et si le nœud a le droit d'utiliser ses ressources. Cette exigence garantit la disponibilité des services d'un RCSF, même si l'un des attaques internes ou externes est présent comme l'attaque par déni de service. [20]

II.5 La fraîcheur des données :

Elle concerne la fraicheur de données et la fraicheur des clés. Puisque tous les réseaux des capeurs fournissent quelques formes de mesures variables dans le temps, nous devons assurer que chaque message est frais. La fraicheur de données implique que les données sont récentes, et elle assure qu'aucun adversaire n'a rejoue les vieux messages. [1]

II.6 Le non répudiation :

La répudiation est signalée dans deux cas différents. Dans le premier cas, le nœud récepteur affirme que les données n'ont jamais été reçues, même si elles ont été correctement reçues. Par contre, dans

le deuxième cas c'est le nœud expéditeur qui affirme qu'il n'a jamais envoyé les données, même si le message a été correctement délivré au destinataire. Un système de sécurité doit interdire la répudiation afin d'améliorer la traçabilité des messages dans le réseau. [18]

II.7 Contrôle d'accès :

Un service très important consiste à empêcher un accès au réseau à tout élément étranger au système. Le contrôle d'accès donne aux participants légitimes un moyen de détecter les messages provenant de sources externes au réseau. [1]

II.8 La sécurité de localisation :

La localisation est un facteur très important pour la fiabilité de fonctionnement des RCSFs. En effet, un réseau de capteurs doit être capable de localiser automatiquement chaque capteur dans le réseau. Ainsi, un réseau de capteurs conçu pour localiser des événements aura besoin d'informations précises sur la localisation afin de repérer la position exacte de ces derniers. Un nœud malveillant peut essayer de compromettre les informations de localisation afin de déstabiliser le fonctionnement du réseau, ce qui rend la sécurité de localisation un objectif très important pour les systèmes de sécurité. [18]

III. Les menaces contre les RCSF :

Une menace étant définie comme l'arrivée potentielle d'événements qui peuvent causer des pertes. Les menaces qui peuvent affecter la sécurité dans les RCSF sont divisées en deux catégories : les mauvais comportements et les attaques.

III.1 Les mauvais comportements :

Les mauvais comportements qui peuvent affecter la sécurité dans les RCSF sont divisés en deux catégories :

III.1.1 Les nœuds égoïstes

On définit un nœud égoïste comme un acte non autorisé d'un nœud interne qui peut entraîner involontairement des dommages à d'autres nœuds. C'est-à-dire, ce nœud a d'autres objectifs que de lancer une attaque. Par exemple, un nœud refuse de transférer les paquets vers les autres nœuds pour préserver ses ressources : batterie ou bande passante.

Ils peuvent généralement être classés comme suite : [26]

III.1.1.1 L'auto-exclusion

Le nœud égoïste ne participe pas lorsque la procédure de découverte de la route est exécutée. Cela garantit que le nœud est exclu de la table de routage d'autres nœuds ; ce qui l'aide à ne pas réacheminer des paquets pour d'autres nœuds.

III.1.1.2 La non-forwarding :

Le nœud égoïste participe pleinement lorsque la procédure de découverte de la route est exécutée, mais refuse de transmettre les paquets pour d'autres nœuds à un moment ultérieur. Ce comportement égoïste d'un nœud est fonctionnellement indissociable d'une attaque comme le black hole ou le sink hole. [27]

III.2 Les attaques :

Une attaque est un ensemble de techniques informatiques, visant à causer des dommages à un réseau, en exploitant les failles de celui-ci.

Les attaques peuvent aggraver les problèmes de sécurité. En effet, les conséquences liées à ces attaques peuvent varier d'une simple écoute du trafic jusqu'à l'arrêt total du réseau selon les capacités des attaquants. Pour les combattre, il est nécessaire de connaître les classes et les types d'attaques afin de mettre en œuvre des solutions optimales. [27]

III.2.1 Classification des attaques :

Les attaques connaissent plusieurs classifications envisageables dont les plus utilisées sont groupées selon les catégories ci-dessous : [21]

III.2.1.1 Selon la nature :

A. Attaque passive :

Les attaques passives se limitent à l'écoute et l'analyse du trafic échangé. Ce type d'attaque est plus facile à réaliser (il suffit de posséder un récepteur adéquat) et il est difficile de le détecter puisque l'attaquant n'apporte aucune modification sur les informations échangées. L'intention de l'attaquant peut être la connaissance des informations confidentielles ou bien la connaissance des nœuds importants dans le réseau (chef de groupe "cluster head"). En analysant les informations de routage, l'attaquant va se préparer à mener ultérieurement une action précise.

B. Attaque active :

Les attaques actives, un attaquant tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service.

III.2.1.2 Selon l'origine :

A. Attaque externe :

Dans le cas de l'attaque externe, le nœud attaquant n'est pas autorisé à participer dans le réseau de capteurs.

B. Attaques internes :

L'attaque interne est considérée comme la plus dangereuse du point de vue sécurité.

Puisque l'attaquant qui capture un nœud, peut lire sa mémoire et avoir accès à son matériel cryptographique et par conséquent peut s'authentifier comme un nœud légitime et émettre des messages aléatoires erronés sans qu'il soit identifié comme intrus, puisqu'il utilise des clés valides. Les méthodes cryptographiques s'avèrent donc inefficace pour ce genre d'attaque.

III.2.2 Les types d'attaques :

Une variété d'attaques contre les RCSFs est rapportée dans la littérature. Pour faire face à ces attaques, diverses contre-mesures ont été proposées. Nous présentons dans la suite les principaux types d'attaques.

III.2.2.1 L'attaque passive:

A. Les attaques contre la vie privée

Comme les RCSFs sont capables de collecter automatiquement les données grâce à un bon et le déploiement stratégique de capteurs, confidentialité préservation des données sensibles est particulièrement un défi très difficile **[26]**

Un adversaire peut recueillir les données et d'en tirer les informations sensibles s'il sait comment agréger les données recueillies provenant de multiples capteur nœuds. C'est analogue au panda-chasseur problème, où le chasseur peut estimer exactement l'emplacement du panda par surveillance du trafic En outre, l'accès distant permet à un seul adversaire à surveiller plusieurs sites simultanément Les plus communes attaques Contre capteur vie privée sont les suivants : **[27]**

- **Surveiller et écouter : L'espionnage**

Du fait que les transmissions se font en diffusion par les ondes radio, aucun contrôle d'accès au réseau n'est possible, ce qui est d'autant plus vrai que le réseau peut être déployé dans un environnement ouvert accessible à tout le monde. Il est donc très facile d'intercepter des données échangées sur un réseau de capteurs et d'accéder à leur contenu si aucun service de confidentialité n'est prévu. **[21]**

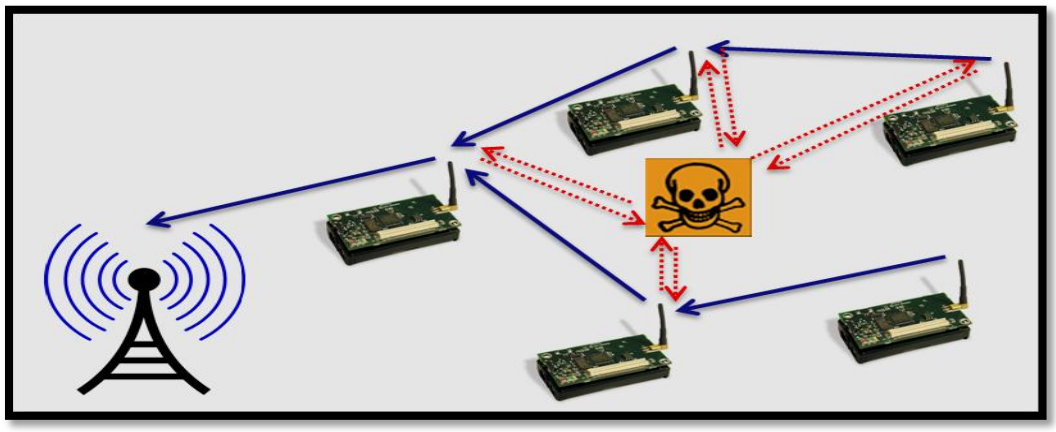


Figure II.2: L'espionnage dans les RCSFs

- **Analyse du trafic:**

Afin de rendre contribuer efficace l'attaque contre la vie privée, la surveillance et l'écoute devraient être combinée avec une analyse du trafic. Grâce à une analyse efficace du trafic, un adversaire peuvent identifier les rôles et les activités des différents nœuds. Par exemple, une augmentation soudaine des communications entre certains nœuds signifie que les nœuds ont certaines activités à suivre. Deng et tout ont démontré deux types d'attaques qui peuvent identifier la station de base dans un WSN par l'analyse du trafic. **[34]**

- **Les adversaires Camouflage:**

L'attaquant peut insérer un nœud ou compromettre les nœuds pour se camoufler dans le réseau pour attirer les paquets et les transmettre à l'attaquant **[27]**.

III.2.2.2 L'attaque active :

A. L'attaque trou noir

Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou trou noir dans le réseau. [**28**]

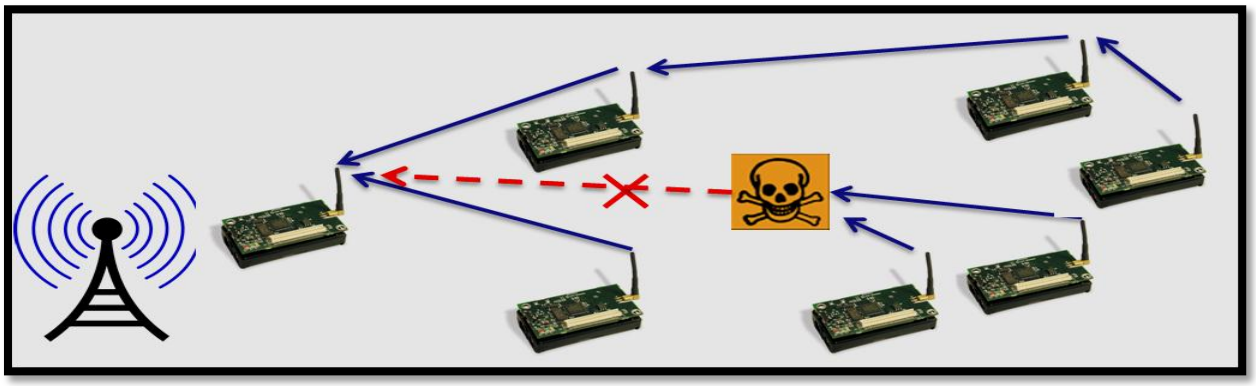


Figure II.3: L'attaque trou noir.

B. L'attaque Sink hole

L'effet d'un trou noir est limité par les nœuds qui sont connectés par l'attaquant. Par contre dans l'attaque Sink hole, l'attaquant tente d'attirer plus de voisins par la publicité des fausses informations de routage, souvent en plus courts sauts. Ce qui fait l'attaquant capable d'affecter un plus grand nombre de nœuds afin de contrôler la plupart des données circulant dans le réseau ou de ne rien transférer. [27]

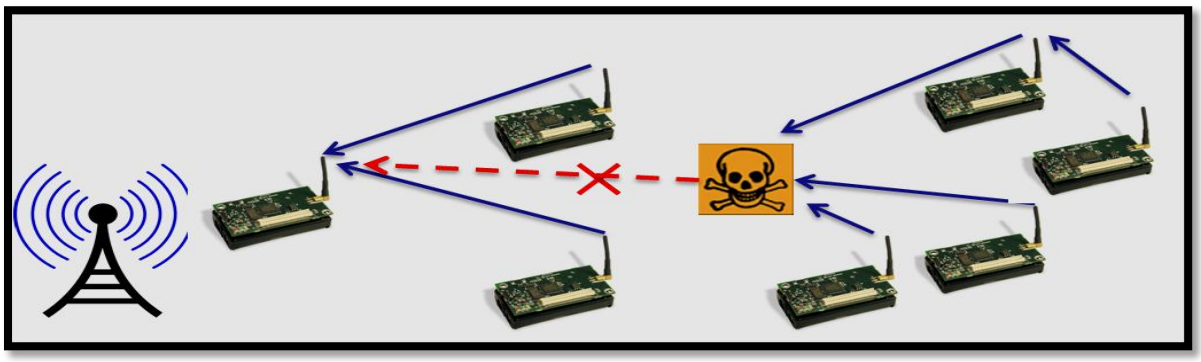


Figure II.4: l'attaque Sink hole

C. Transmission selective

Un nœud néglige son rôle de routeur et décide de ne pas transmettre les données de certains nœuds choisis selon certains critères ou d'une façon aléatoire. La raison peut être aussi bien

D'ordre énergétique, que liée a une attaque. [1]

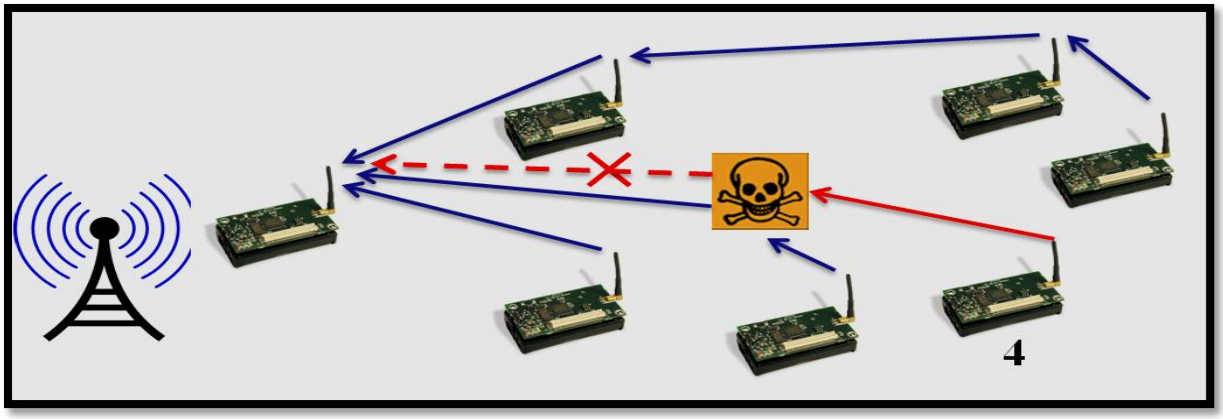


Figure II.5: transmission sélective

Dans la Figure : l'attaquant nœud d'un attaquant, transmet tous les paquets sauf ceux qu'elle reçoit de nœud 4, fondée sur l'adresse d'origine.

D. Nœud Outage

Si un nœud sert d'intermédiaire, un point d'agrégation ou un cluster Head, que se passe si le nœud arrête de fonctionner? Les protocoles utilisés par les RCSFs doivent être suffisamment robuste pour

atténuer les effets des pannes en fournissant des routes alternatives. [30]

E. Inondation par des paquets Hello (Hello Floods):

L'objectif de cette attaque est de consommer l'énergie des nœuds capteurs, notamment les plus éloignés, par un envoi continu, à un signal puissant des messages de découverte du voisinage de type HELLO. Les nœuds destinataires du message essayent de répondre au nœud malicieux même s'ils sont situés à des distances lointaines ne permettant pas de l'atteindre. A force détente de lui répondre, tous les nœuds concernés par ce message HELLO consomment l'intégralité de leur énergie. [5]

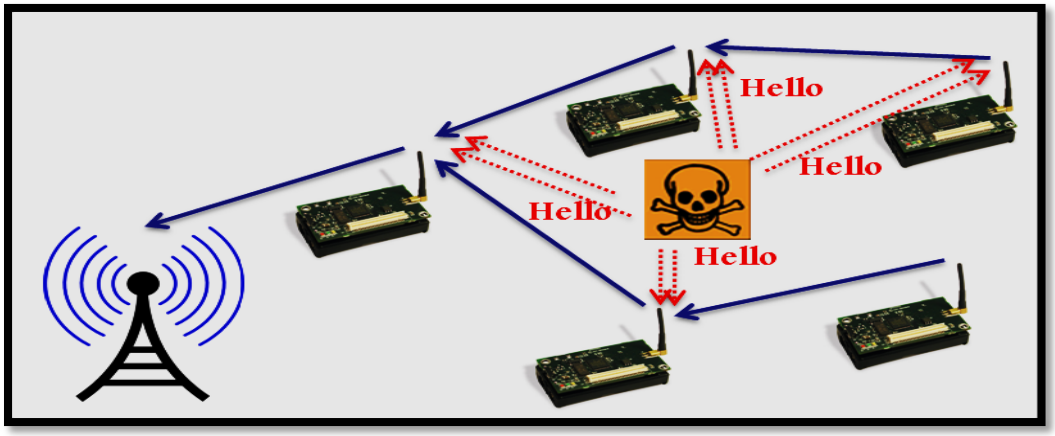


Figure II.6: Attaque hello floods.

F. Attaques contre les mécanismes d'agrégation de données :

L'agrégation de données est l'une des principales notions dans les RCSF. Elle permet aux nœuds intermédiaires de rassembler des données venant des nœuds sources au fur et à mesure de leur acheminement au nœud puits, et ensuite, à les agréger en une seule donnée pour la transmettre à l'utilisateur final. Ceci permet d'éliminer les redondances et de réduire le taux de transmissions dans le réseau, d'où, prolonger sa durée de vie.

La forme la plus simple que peut prendre une fonction d'agrégation est la suppression des messages dupliqués. Mais elle peut également être une fonction min ou max ou n'importe quelle fonction à plusieurs entrées.

Cependant, des attaques dangereuses peuvent provoquer un faux résultat d'agrégation. On peut en distinguer deux types :

-Le premier type permet aux nœuds capteurs malicieux d'injecter de fausses données,

-Le second, il peut être causé par les nœuds intermédiaires qui agrègent les données en modifiant le résultat de l'agrégation [27]

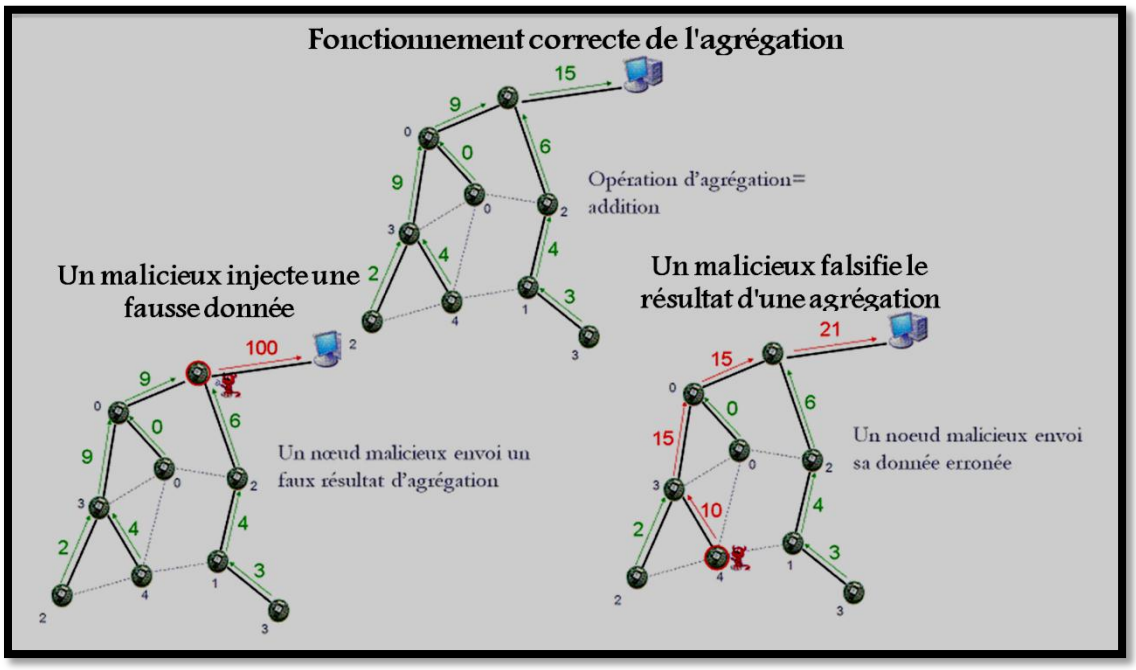


Figure II.7: Attaques contre l'agrégation de données.

Par exemple, dans la figure, la fonction d'agrégation est l'addition. Un nœud intermédiaire calcule la somme des nombres générés par des nœuds sources. Ce processus est répété jusqu'à ce que la somme finale arrive aux nœuds puits.

G. Privation du sommeil des nœuds:

Afin de ne pas gaspiller la ressource d'énergie du réseau, les nœuds qui fonctionnent inutilement vont se mettre en veille. Ce mécanisme va devenir une stratégie à part entière pour augmenter la durée de vie du réseau.

Cette attaque vise à forcer les nœuds à consommer leur énergie plus rapidement en privant un ou plusieurs nœuds victimes de leur sommeil (mise en veille). Les principales méthodes consistent à tromper le nœud en le maintenant éveillé, l'obligeant à écouter les communications et à retransmettre les paquets. [27]

H. Espionnage des connaissances:

Plusieurs algorithmes de routage dépendent des acquittements implicites ou explicites de la couche liaison. Un adversaire peut spoofer ces acquittements pour examiner les paquets adressés aux nœuds voisins. Le but de cette attaque est de faire croire à l'émetteur qu'un lien faible est fort ou qu'un nœud inactif est vivant. [31]

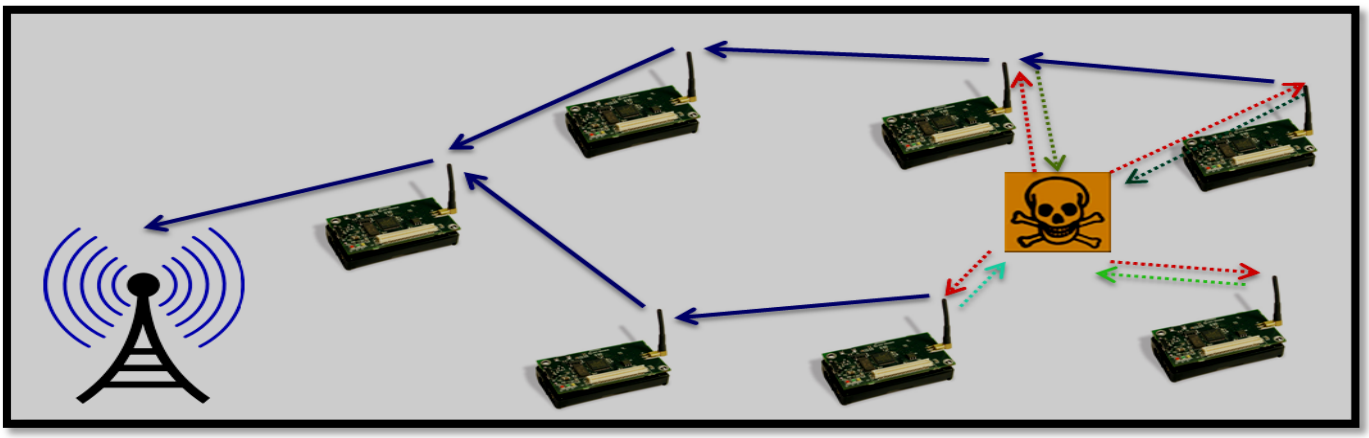


Figure II.8: Espionnage des connaissances:

I. L'empoisonnement de la table de routage

Certaines optimisations ont été développées afin d'augmenter la connaissance des chemins. Lorsqu'un nœud entend une information de routage, il met à jour sa table de routage locale en conséquence. Un nœud malicieux peut émettre un nombre important de fausses informations, remplissant ainsi les tables de routage des nœuds. Comme ces tables possèdent des tailles limitées, cela va engendrer un débordement, et les tables ne contiendront que de fausses routes. [32]

J. Faux Nœud :

Un faux nœud comporte l'addition d'un nœud par un adversaire et l'injection de malicieux des données ou l'adoption des véritables données. Insertion malicieux nœud est un des plus dangereuses attaques qui peuvent se produire : les données malicieux injectées dans le réseau pourraient s'étendre tous les nœuds, potentiellement détruire tout le réseau, ou pire encore, en attractant le réseau vers l'adversaire [27]

K. Nœud de réplication :

L'attaquant ajoute un nœud au réseau en copiant le nœud ID d'un nœud existant déjà. Un nœud répliqué dans cette approche peut gagner l'accès physique à la totalité du réseau et copier les clés de cryptage et répliquer les autres nœuds [31]

L. Nœud Défectuosité (Node Malfunction) :

Un nœud va générer des données inexactes que pourrait exposer l'intégrité du réseau des capteurs surtout si c'est un nœud cluster Head. [33]

M. Inondations :

C'est similaire l'attaque Hello-flood, sauf que l'application est fait à la couche transport plutôt qu'à la couche réseau. Ce type d'attaque mène à DOS soit par épuisement rapide du mémoire ou de la batterie. [27]

N. Brouillage (jamming) :

Une attaque bien connue sur la communication sans-fil, est celle qui consiste à perturber le canal radio en envoyant des informations inutiles sur la bande de fréquences utilisées. Ce brouillage peut être temporaire, intermittent ou permanent. [1]

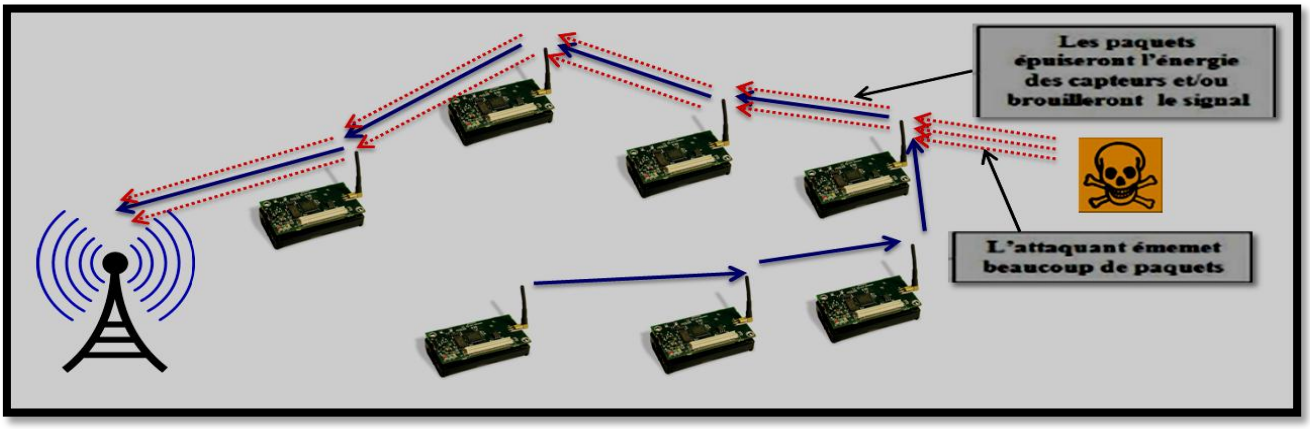


Figure II.9: attaque Brouillage

O. Le rejoue de messages:

Un nœud malicieux surveille les transmissions, modifie les paquets de données et les rejoue, ce qui occupe la bande passante inutilement et peut même affecter la justesse des informations concernant la topologie du réseau.

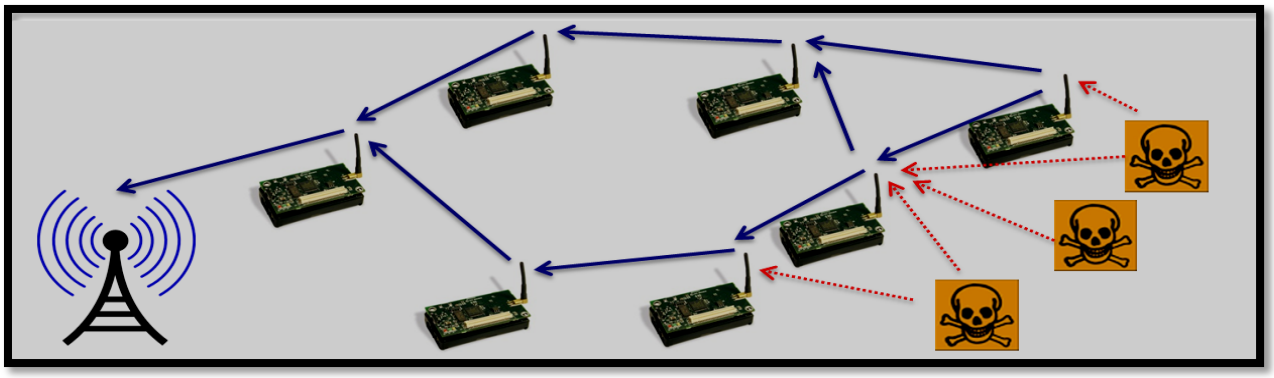


Figure II.10: Le rejoue de messages

P. L'attaque d'identités multiples :

Dans cette attaque, un nœud malveillant peut revendiquer différentes identités afin de participer à des algorithmes distribués tels que l'élection et de prendre de l'avantage sur les nœuds légitimes. Un nœud malveillant peut être capable de déterminer le résultat de n'importe quel vote en faisant voter toutes ses identités multiples pour une même entité. Les techniques d'authentification et de chiffrement peuvent empêcher un étranger de lancer une attaque Sybille sur le réseau de capteur. [21]

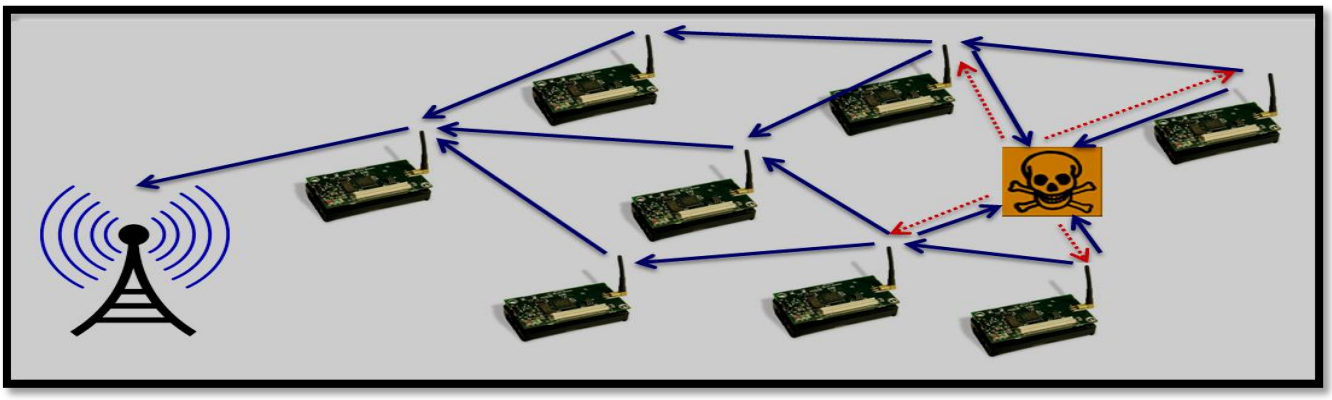


Figure II.11: L'attaque d'identités multiples.

Figure : Noud B envoie des données à C par A3, l'attaquant écoute la conversation L'attaquant A (3.2) recueille plusieurs identités A1, A2, A3.

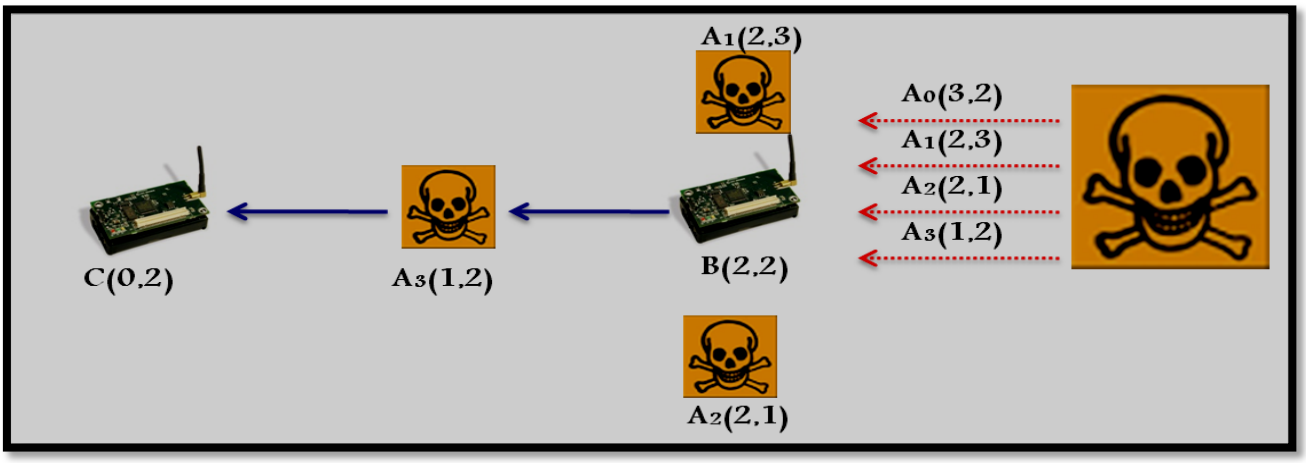


Figure II.12: L'attaque d'identités multiples.

Q. Attaque par ver/tunnel (Wormhole) :

Dans une attaque Wormhole, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant pour les réintroduire dans le réseau. L'encapsulation peut se faire de deux manières :

- **Multi-sauts:**

L'encapsulation multi-sauts permet de cacher les nœuds se trouvant entre les deux attaquants. Donc, les chemins passant par le nœud malicieux apparaissent plus courts. Cela facilite la création de sink holes avec des protocoles qui utilisent le nombre de sauts comme métrique de choix de chemins.

➢ **Communication directe :**

Les routes passant par les attaquants sont plus rapides, car ils sont à un saut. Donc, cette technique peut être employée contre les protocoles qui se basent sur la latence des routes ou ceux qui utilisent la première route découverte **[32]**

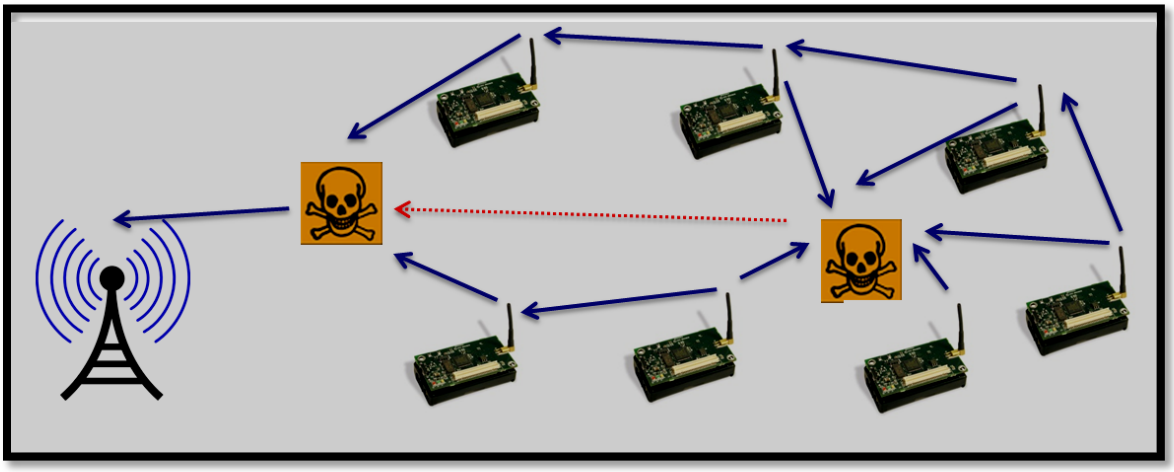


Figure II.13 : Attaque Wormhole.

R. Attaque physique d'un nœud :

C'est une attaque qui permet de reprogrammer, détruire ou violer un nœud légitime en accédant au logiciel ou aux matériels qu'il utilise. Une fois que l'adversaire a pris le contrôle total d'un nœud légitime il essaye d'extraire des informations sensibles telles que les clés secrètes partagées entre les nœuds (par exemple). **[29]**

S. Nœud Subversion :

La capture d'un nœud par un adversaire peut révéler ses informations notamment les clés de cryptage et compromettre ainsi le réseau **[33]**

T. La Corruption du message:

Attaques contre l'intégrité d'un message se produisent lorsqu'un attaquant insère lui-même entre la source et destination et modifie le contenu d'un message.

U. Manipulation:

Dans cette attaque, un attaquant simplement modifie les nœuds physiquement, et ensuite les interroge et les compromis.

V. Collision :

L'attaquant introduit une collision pendant la transmission d'un paquet. Même la corruption d'un octet peut conduire à retransmission de l'ensemble message. Il est très simple à mettre en œuvre et les réseaux peuvent affecter négativement. **[31]**

W.Epuisement:

Dans ce type d'attaque le nœud malveillant transmet un grand nombre de paquets RTS afin d'introduire des collisions multiples pour les transmissions des autres nœuds légitimes, et les force à retransmettre continuellement leurs paquets et d'épuiser en conséquence leur énergie. [28]

X. Injustice:

L'attaquant cherche à abuser une priorité coopérative de la couche MAC. Il ne peut entraîner un total DOS, mais elle pourrait diminuer le service du réseau [31]

Y. Désynchronisation :

Consiste à rompre la connexion existante entre deux nœuds en resynchronisant leur transmission. L'attaquant réalise cette attaque en envoyant des messages forgés à l'une des parties communicantes avec des fautes de type flags (séquence) et les l'oblige en conséquence à sortir de la synchronisation. [28]

IV. Mécanisme de sécurité :

Pour assurer les services de sécurité requis (disponibilité, intégrité, confidentialité, preuve..), on met en place des différents mécanismes de sécurité, on les développés dans le but d'éliminer toute menace capable d'atteindre à la sécurité des informations échangées.

IV.1 La cryptographie :

Le mot cryptographie est composé de deux mots grecs : « crypto » qui signifie caché et « graphie » qui signifie écrire, d'où la signification complète de la cryptographie est « l'écriture secrète ».

La cryptographie est définie comme la science qui convertit les informations en clair en informations cryptées c'est-à-dire codées. La plupart des mécanismes de sécurité des communications sont basés sur des outils cryptographiques utilisant des informations secrètes représentées par des nombres premiers, dites clés, combinées, en entrée d'une opération cryptographique, au message à coder pour produire le message crypté.

On distingue quatre types de clés utilisées dans les opérations cryptographiques :

- Clé individuelle.
- Clé globale.
- Clé partagée par paire de nœuds.

- Clé partagée par groupe de nœuds. (voir le chapitre suivant).

Plusieurs outils cryptographiques sont utilisés pour assurer la sécurité du routage, des entités du réseau et des liens.

Pour assurer un système cryptographique fiable, deux communicants doivent choisir soigneusement leur clé de chiffrement/déchiffrement et doivent appliquer les principes suivants, car un attaquant peut essayer un certain nombre de possibilités et par chance tomber rapidement sur la solution :

- La sécurité doit se reposer sur le secret de la clé et non pas sur la sécurité de l'algorithme.

- Le déchiffrement sans connaissance préalable de la clé doit être impossible en un temps raisonnable.

- Calculer la clé à partir du texte en clair et du texte chiffré doit être impossible en un temps raisonnable. **[5]**

IV.2 Les outils de cryptographies :

Les outils cryptographiques utilisant le principe de clé pour sécuriser les liens de communication sont nombreux, on cite :

IV.2.1 Le chiffrement :

Le chiffrement est une méthode permettant de renforcer la sécurité d'un message ou d'un fichier en brouillant son contenu de sorte que seules les personnes disposant de la clé de chiffrement appropriée pour les déchiffrer peuvent les lire.

IV.2.1.1 La cryptographie à clé symétrique

La cryptographie à clé symétrique est un mécanisme selon lequel la même clé est utilisée pour le chiffrement et le déchiffrement; elle est plus intuitive à cause de sa similarité avec ce que l'on s'attend à utiliser pour verrouiller et déverrouiller une porte : la même clé. Cette caractéristique requiert des mécanismes sophistiqués pour distribuer en toute sûreté la clé symétrique aux deux parties. **[37]**

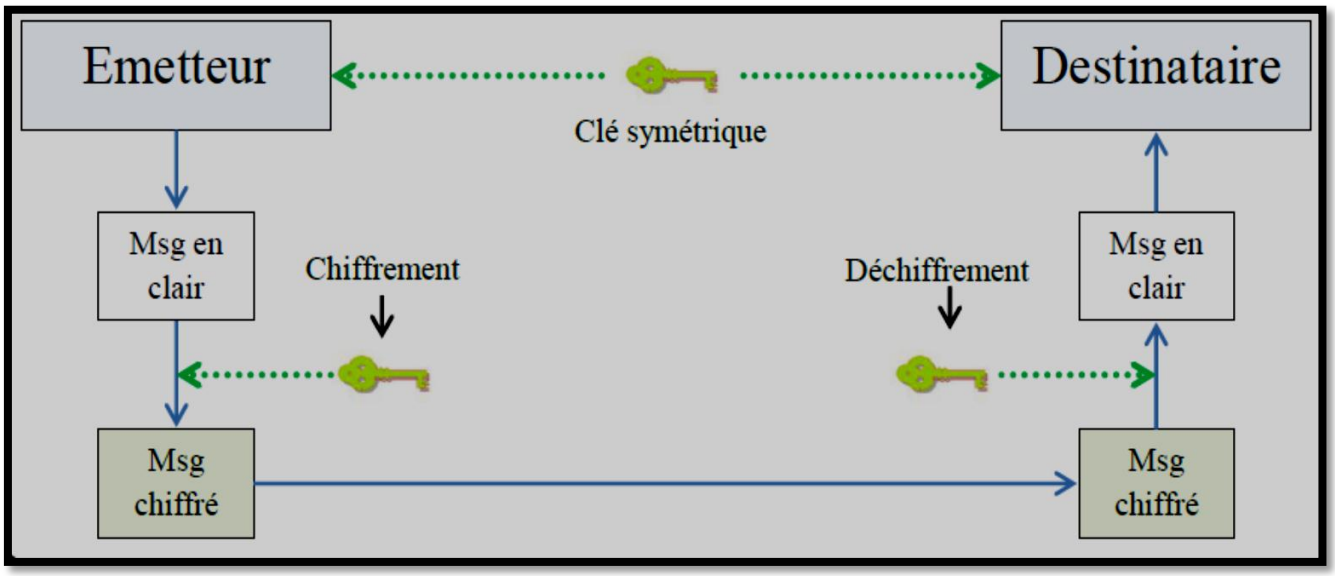


Figure II.14 : La cryptographie à clé symétrique

IV.2.1.2 La cryptographie à clé asymétrique :

Dans un crypto-système asymétrique (ou crypto système à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement.

Une donnée chiffrée par la clef publique ne peut être déchiffrée que par la clef privée.

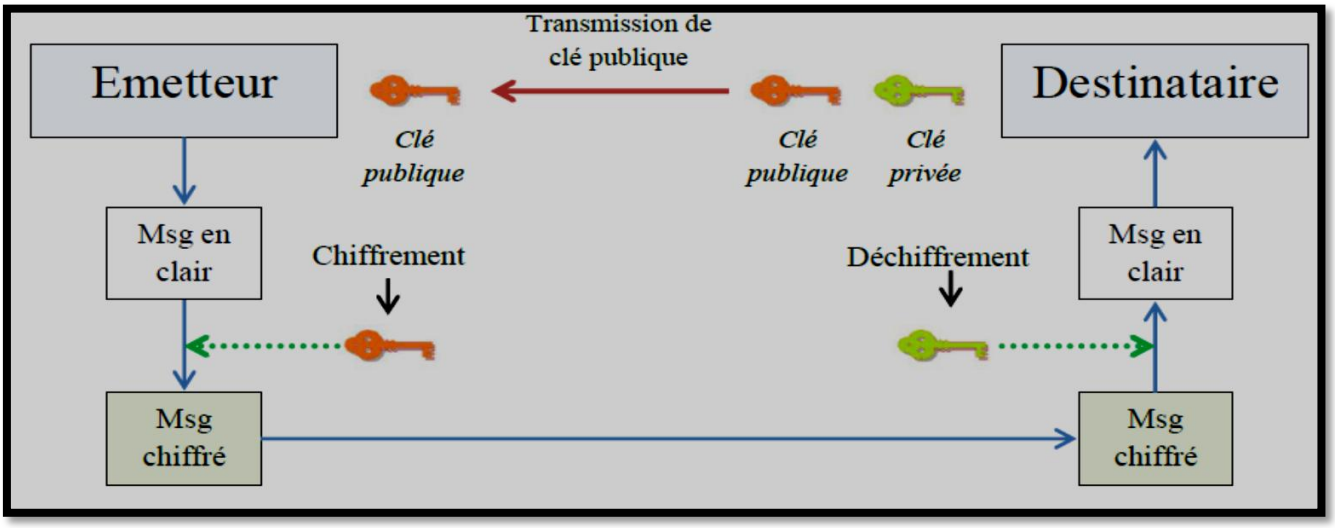


Figure II.15 : La cryptographie à clé symétrique

IV.2.2 Fonction de Hachage

Cette technique permet de produire un condensé de message (empreinte) qui est une représentation réduite et unique (qui s'apparente à une somme de contrôle sophistiquée) du message complet. Les algorithmes de hachage sont des algorithmes de chiffrement unidirectionnels (par exemples d'algorithme de hachage : SHA-1 et MD5), il est donc impossible de retrouver le message d'origine à partir du condensé.

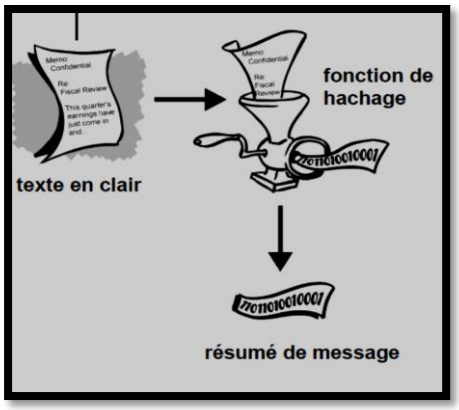


Figure II.16 : Fonctionnement d'une fonction de hachage

Les raisons principales pour lesquelles on produit un condensé de message sont :

- l'intégrité du message envoyé est préservée, toute altération du message sera aussitôt détectée.
- la signature numérique sera appliquée au condensé dont la taille est habituellement beaucoup plus petite que le message lui-même.
- les algorithmes de hachage sont bien plus rapides que n'importe quel algorithme de chiffrement (que ce soit à clé publique ou à clé symétrique).

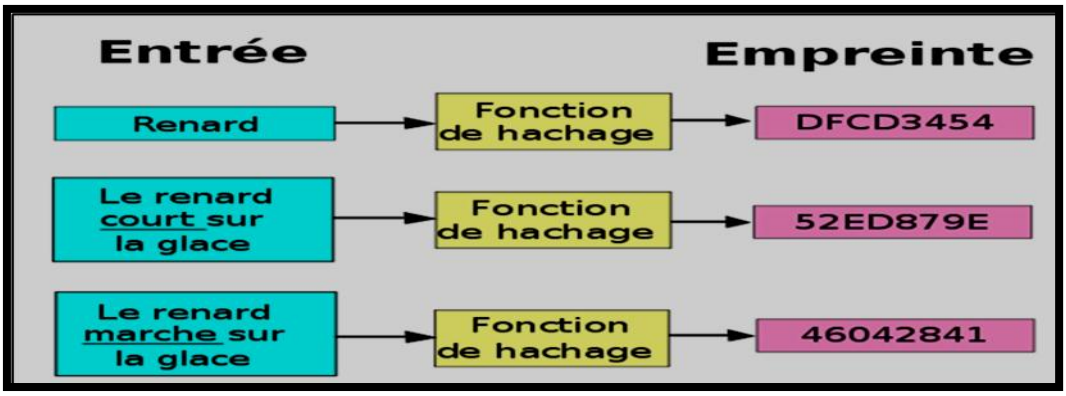


Figure II. 17: Exemple de fonction de hachage appliquée sur 3 entrées distinctes.

IV.2.3 La signature numérique :

La signature numérique est un mécanisme qui permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu. Elle assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. [36]

IV.2.4 Certificat numérique :

Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Le certificat numérique est un bloc de données contenant, dans un format spécifié, les données suivantes :

- la clé publique d'une paire de clés asymétriques,
- des informations identifiant le porteur de cette paire de clés
- (une personne, site ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
- l'identité de l'entité ou de la personne qui a délivré ce certificat (autorité de certification),
- La signature numérique des données ci-dessus par autorité de certification qui prend en charge la création et l'authentification de ce certificat. [35]

Le standard le plus utilisé pour la création des certificats numériques est le X.509.

V. Contraintes influençant à l'utilisation les solutions de sécurité dans un RCSF :

Les propriétés des réseaux de capteurs sont à double tranchant. Certes elles permettent une grande facilite de production et de déploiement, cependant, elles rendent le système global de communication fragile a un certain nombre de défaillances. La sécurisation des réseaux de capteurs reste un problème difficile pour les raisons suivantes :

V.1 Ressource limitée

Toutes les approches de sécurité exigent une certaine quantité de ressources pour leurs implémentations, y compris la mémoire, l'espace de stockage, la puissance de calcul et l'énergie. Comme ces ressources sont très limitées. Ceci restreint les types des algorithmes et des protocoles de sécurité qui peuvent être mis en couvre dans les RCSFs.

V.2 Limitation en énergie

L'influence qu'a la sécurité sur la durée de vie d'un capteur est a prendre en considération lors du rajout de ses services. Cet impact se résume dans la puissance supplémentaire consommée par les nœuds capteurs du au traitement exige par les services de sécurité, l'énergie pour transmettre les

données relatives a la sécurité et l'énergie nécessaire pour stocker les paramètres de sécurité d'une façon permanente (stockage des clés cryptographiques par exemple).

V.3 La communication non fiable

Certainement, la communication est un autre obstacle pour la sécurité des capteurs. La sécurité du réseau est fortement liée au protocole défini, qui lui dépend de la communication.

V.4 Le transfert non fiable

Les paquets peuvent être endommage en raison des erreurs de transmission ou supprime dans les nœuds fortement encombres. D'une manière primordiale, le protocole doit disposer d'une gestion d'erreur appropriée sinon il serait possible de perdre des paquets critiques de sécurité tels que les paquets contenant les clés cryptographiques **[25]**.

Les données sont transmises dans l'air, donc chaque capteur qui se trouve dans le rayon de couverture peut écouter les messages échangés. L'application d'un bruit sur le canal peut rendre les capteurs incapables de transmettre les messages vu que le media apparait comme occupé en permanence. En outre, la communication sans fil introduit d'autres vulnérabilités a la couche liaison en ouvrant la porte a des attaques de brouillage et de style déni de service par épuisement des batteries **[23]**.

V.5 Les collisions

Même si le canal est fiable, la communication ne peut pas toujours l'être. Ceci est du a la nature d'émission des paquets dans les réseaux de capteurs sans fil (broadcast). Si les paquets se rencontrent lors du transfert, les collisions se produisent et le transfert lui-même échouera. Dans un réseau de capteur d'une forte densité, ceci peut constituer un problème extrêmement important.

V.6 La latence

Le routage multi-saut, la congestion du réseau et le traitement effectué au sein Les nœuds peuvent mener à une plus grande latence dans le réseau. De ce fait la synchronisation entre les nœuds devient difficile à réaliser. Le problème de la synchronisation peut être très important pour la sécurité des nœuds ou le mécanisme de sécurité se base sur les rapports d'événement survenu et la distribution des clés cryptographiques **[25]**.

V.7 Communication multi-sauts

Dans la communication multi-sauts, il y a plus de probabilité d'attaques que dans une communication à un seul saut car les attaquants ont plus de chance d'atteindre leur but, a chaque transmission d'une donnée, d'un saut a un autre. En effet, lors de l'acheminement de données, les attaques visent la vulnérabilité de la sécurité et cela dans deux niveaux différents : l'attaque de la construction et la maintenance de la route, c'est-b-dire, dévier la route ou la donnée doit être

acheminée, et l'attaque de flux de données par l'injection, la modification ou la suppression des paquets.

En outre, la communication sans fil introduit d'autres vulnérabilités a la couche liaison qui permet l'établissement d'une infrastructure pour la communication saut-par-saut.

V.8 Communication sans fil

Les RCSF requièrent une communication sans fil qui est plus exposée aux risques de l'interception et de la récupération de données. Autrement dit, le réseau est confronté aux attaques passives

V.9 L'absence d'une topologie

La topologie d'un RCSF n'a pas de structure fixe, pour sa taille et pour sa forme. Elle exige une reconfiguration permanente des nœuds qui doivent s'adapter très vite aux changements imprévus comme l'ajout, l'absence (épuisement ou destruction) ou la poursuite d'un nœud qui ne peut pas être faite facilement dans un RCSF a grande échelle. Dans ce cas, un attaquant pourra s'infiltrer car les relations de sécurité (entre les nœuds) qui prévoient l'ajout de cet attaquant ne sont pas établies au préalable (par exemple les clés de cryptage). Donc, la difficulté est de concevoir des mécanismes de sécurité basés sur des opérations locales entre les nœuds voisins seulement et qui ne dépendent pas de la topologie globale du réseau **[22]**.

Conclusion

Les dernières avancées technologiques dans les réseaux de capteurs sans fil ont permis de généraliser l'utilisation de ce type de réseau.

Mais l'information est encore vulnérable à de nombreuses menaces, qui sont souvent spécifiques aux réseaux ad-hoc, voire exclusives aux réseaux de capteurs sans fil.

Les solutions apportées par la communauté scientifique pour contrer les menaces ne garantissent pas toujours une sécurité maximale et malheureusement parfois leur utilisation a consomme un coût énergétique incompatible avec des capteurs à énergie limitée, donc il nous faut encore chercher des solutions qui puissent concilier sécurité, durée de vie et rapidité d'exécution des capteurs. Ceci est discuté dans le chapitre suivant.


Chapitre 3

Introduction

Les propriétés des réseaux de capteurs sont à double tranchant. Certes ils permettent une grande facilité de production et de déploiement, mais rendent le système global de communication assez « fragile » à un certain nombre de défaillances et des attaques.

Afin d'assurer un déploiement à large échelle de cette technologie, il est nécessaire de pallier ces problèmes de sécurité d'une RCSF.

Dans ce chapitre nous avons présenté quelques algorithmes de chiffrements les plus utilisés, mais bien sûr il en existe d'autres.

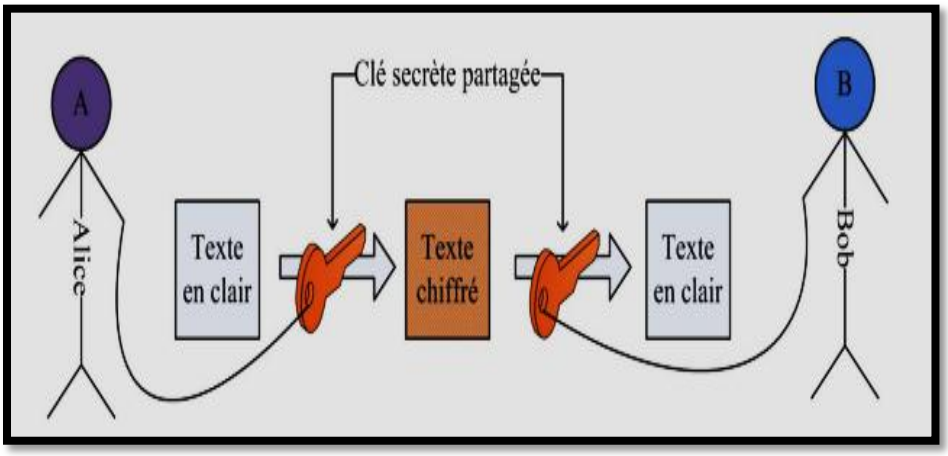
Nous concluons ce chapitre par une résumé sur les propositions qui garante la sécurité des communications dans les RCSF.

I. Les algorithmes de chiffrement :

Nous présentons dans cette partie les différents algorithmes cryptographiques utilisés de nos jours afin de sécuriser les communications des réseaux. Nous commençons par les algorithmes de cryptographie symétrique puis nous passons à l'algorithme de cryptographie asymétrique.

I.1 Le chiffrement symétrique :

Un algorithme de chiffrement symétrique transforme un message en clair avec une clé secrète. Le résultat est un message chiffré.
La fonction de chiffrement doit être inversible. **[34]**



FigureIII.1 : Principe de de chiffrement symétrique

Nous avons deux grandes catégories :

I.1.1 Chiffrement symétrique par bloc :

Bonnes performances, et sécurité bien étudiée, Elle chiffre des blocs de message de taille fixe (typiquement 64,128 ou 256 bit).

L'idée générale du chiffrement par blocs est :

- Remplacer les caractères par un code binaire
- Découper cette chaîne en blocs de longueur donnée
- Chiffrer un bloc en l'additionnant" bit par bit à une clef.
- Déplacer certains bits du bloc.
- Recommencer éventuellement un certain nombre de fois l'opération 3.
- Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré. [40]

Le chiffrement par bloc contient plusieurs algorithmes comme exemples : DES, AES, IDEA, RC6…

I.1.1.1 DES :

Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) est un algorithme de chiffrement par bloc, Le 15 mai 1973 le NBS (National Bureau of Standards, aujourd'hui appelé NIST - National Institute of Standards and Technology) a lancé un appel dans le Federal Register (l'équivalent aux Etats-Unix du Journal Officiel en France) pour la création d'un algorithme de chiffrement. Fin 1974, IBM propose « Lucifer », qui, grâce à la NSA (National Security Agency), est modifié le 23 novembre 1976 pour donner le DES.

Figure III.2: National Institute of Standards and Technology

Le DES a finalement été approuvé en 1978 par le NBS. Il résiste toujours très bien à la cryptanalyse et reste un algorithme très sûr mais elle devenu obsolète à cause de son âge. [24]

A. Particularités :

Le DES comporte plusieurs avantages qui en ont fait l'algorithme de chiffrement symétrique standard pendant longtemps, jusqu'il y a quelques années. En voici quelques-uns :

- il possède un haut niveau de sécurité,
- il est complètement spécifié et facile à comprendre,
- la sécurité est indépendante de l'algorithme lui-même,
- il est rendu disponible à tous, par le fait qu'il est public,
- il est adaptable à diverses applications (logicielles et matérielles),
- il est rapide et exportable,

- il repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement,
- Il est facile à implémenter.

B. Algorithme de chiffrement

Le D.E.S. est un crypto système agissant par blocs. Cela signifie que D.E.S. ne chiffre pas les données à la volée quand les caractères arrivent, mais il découpe virtuellement le texte clair en blocs de 64 bits qu'il code séparément, puis qu'il concatène. Un bloc de 64 bits du texte clair entre par un coté de l'algorithme et un bloc de 64 bits de texte chiffré sort de l'autre côté. L'algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions.

C'est un algorithme de chiffrement à clef secrète. La clef sert donc à la fois à chiffrer et à déchiffrer le message. Cette clef a ici une longueur de 64 bits, c'est-à-dire 8 caractères, mais dont seulement 56 bits sont utilisés. On peut donc éventuellement imaginer un programme testant l'intégrité de la clef en exploitant ces bits inutilisés comme bits de contrôle de parité.

L'entière sécurité de l'algorithme repose sur les clefs puisque l'algorithme est parfaitement connu de tous. La clef de 64 bits est utilisée pour générer 16 autres clefs de 48 bits chacune qu'on utilisera lors de chacune des 16 itérations du D.E.S... Ces clefs sont les mêmes quel que soit le bloc qu'on code dans un message.

Cet algorithme est relativement facile à réaliser matériellement et certaines puces chiffrent jusqu'à 1 Go de données par seconde. Pour les industriels, c'est un point important notamment face à des algorithmes asymétriques, plus lents, tels que l'algorithme R.S.A. **[33]**

Les grandes lignes de l'algorithme sont les suivantes :

- Fractionnement du texte en blocs de 64 bits (8 octets) ;
- Permutation initiale des blocs ;
- Découpage des blocs en deux parties : gauche et droite, nommées G et D ;
- Etapes de permutation et de substitution répétées 16 fois (appelées **rondes**) ;
- Recollement des parties gauche et droite puis permutation initiale inverse.

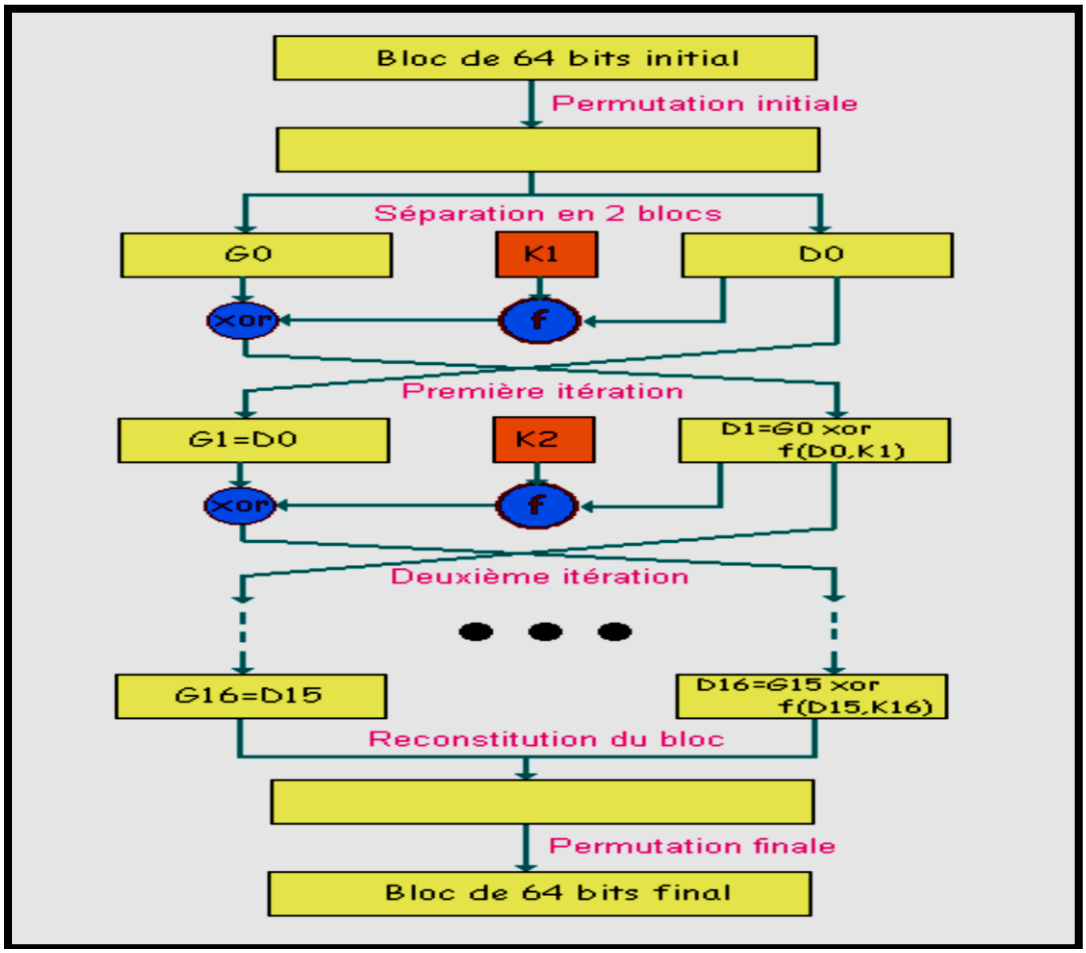


Figure III.3 : Algorithme principal du DES

C. Le triple DES :

Le Triple DES (aussi appelé 3DES) est un algorithme de chiffrement symétrique enchainant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes. L'algorithme va d'abord chiffrer avec une clé, déchiffrer avec la deuxième clé est enfin chiffrer encore avec la troisième clé.

Que l'on utilise cet algorithme avec 2 clés différentes (112 bits) ou 3 clés différentes (168 bits), la clé effective est de 112 bits.

Pour les même raisons, le double DES n'existe pas car la clé effective n'est que de 57 bits soit 1 bit de plus que le simple DES.

Cette utilisation de trois chiffrements DES a été développée par Walter Tuchman. **[39]**

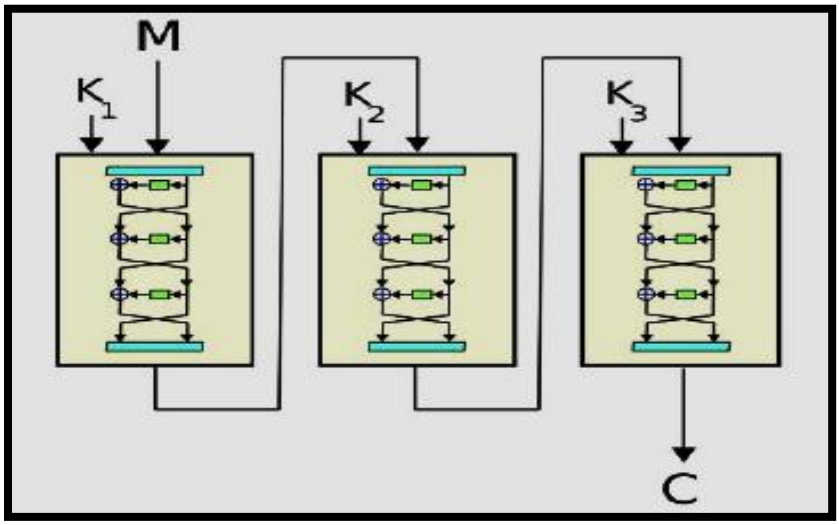


Figure III. 4 : le triple DES

I.1.1.2 AES :

Suite à la petite taille de clé du DES comparée aux possibilités croissantes de calcul des ordinateurs, le NIST lança le 12 septembre 1997 un appel à candidature pour trouver un remplaçant au DES. Cet algorithme, nommé AES (Advanced Encryption Standard), doit pouvoir chiffrer des blocs de 128 bits et être disponible en trois versions pour trois tailles de clé différentes (128, 192 et 256 bits). **[41]**

AES est un algorithme de chiffrement par bloc, il nécessite relativement peu de mémoire.
Il possède les propriétés suivantes :

- La résistance a toutes les attaques connues
- La rapidité du code sur une très grande variété de plateformes (logicielles et matérielles)
- La simplicité dans la conception
- Plusieurs longueurs de clef et de bloc sont possibles : 128, 192, ou 256 bits
- Le nombre de cycles (ou rondes) varie en fonction de la longueur des blocs et des clés (de 10 à 14)
- La structure générale ne comprend qu'une série de transformations, permutations
- Il est performant que le DES
- Il est facilement adaptable à des processeurs de 8 bits. **[1]**
- Le principe de fonctionnement de l'AES est décrit dans la figure (**III.5**):

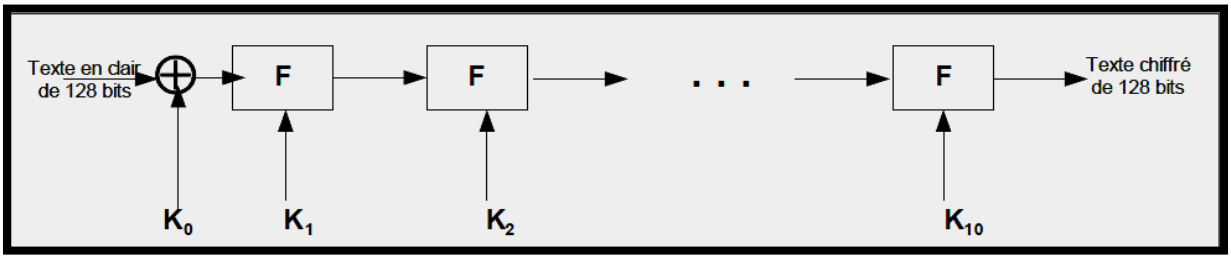


Figure III.5 : Itération de l'AES

Les messages sont chiffrés par blocs de 128 bits. En premier lieu, nous ajoutons bit à bit le message avec la clef secrète K0. Puis, comme pour tous les algorithmes de chiffrement par blocs, on itère une fonction F, paramétrée par des sous-chefs qui sont obtenues de la clef maître par un algorithme de cadencement de clefs.
Dans le cas d'AES, on itère 10 fois la fonction F.
La fonction F, itérée lors du chiffrement, prend en entrée des blocs de 128 bits répartis sur
16 octets. Tout d'abord, nous appliquons à chaque octet la même permutation S. Ensuite nous appliquons aux 16 octets une seconde permutation P. Au résultat obtenu, nous ajoutons alors bit à bit le sous-chef de 128 bits obtenue par l'algorithme de cadencement de clef. **[38]**

I.1.2 Chiffrement symétrique par flux

Un algorithme de chiffrement par flux (ou chiffrement par flot) est un algorithme agissant en continu sur les données. Il ne nécessite pas d'avoir toutes les données pour commencer à chiffrer, le chiffrement de flux agit sur chaque bit, l'un après l'autre.

Ce type de chiffrement est souvent utilisé pour les communications en temps réel telles que le WI-FI (RC4), puisqu'il a la particularité d'être beaucoup plus rapide que n'importe quel algorithme de chiffrement par bloc.

De plus, au niveau des données chiffrées en sortie, le chiffrement par flux ne donnera pas forcement le même résultat en sortie alors que pour un bloc donné un chiffrement par bloc aura toujours le même résultat.

Un algorithme de flux fonctionne avec ce que l'on appelle un générateur pseudo-aléatoire (key stream), c'est une séquence de bits précise utilisée en tant que clé. Le chiffrement se fait par la combinaison du key stream et du message, le plus souvent par une opération XOR

(OU exclusif). **[45]**

I.1.2.1 RC4

RC4 (Rivest Cipher 4) est un algorithme de chiffrement à flot conçu en 1987 par Ronald Rivest.

Il est longtemps resté secret avant d'être publié.

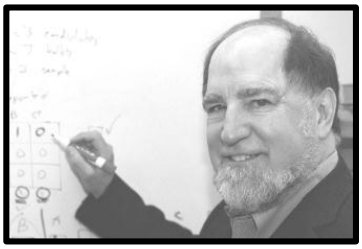


Figure III.6 : Ronald Rivest.

A. Particularités :

- RC4 peut utiliser des clés de taille variables jusqu'à 2048 bits.
- Cet algorithme très simple à comprendre et à implémenter.
- Le chiffrement RC4 est extrêmement rapide, sûrement le plus rapide des chiffrements utilisés à l'heure actuelle même. **[46]**

Algorithme	Longueur de la clé	Vitesse (en Mbps)
DES	56	9
3DES	168	3
RC4	Variable	45

Tableau. III.1 – Vitesses de quelques chiffrements symétriques. [40]

- Le RC4 a été largement utilisé dans des protocoles comme WEP (Wired Equivalent Protocol), WPA (Wi-Fi Protected Access) ou TLS, même s'il est resté pendant de nombreuses années secrètes **[47].**

B. Fonctionnement

Le fonctionnement de RC4 est le suivant :

- La clé K utilisée est d'une longueur variable. Elle peut avoir une taille de 8 à 2048 bits (comprise entre 1 et 256 octets).
- La clé est utilisée pour initialiser un vecteur S de 256 octets. Initialement, les cellules du vecteur S reçoivent des valeurs égales à leurs positions c'est-à-dire : S[0]= 0, S[1] = 1, …., S[255] = 255.
- On crée un vecteur temporaire T de longueur égale à S destiné à recevoir la clé K et utilisé pour produire la permutation initiale de S.

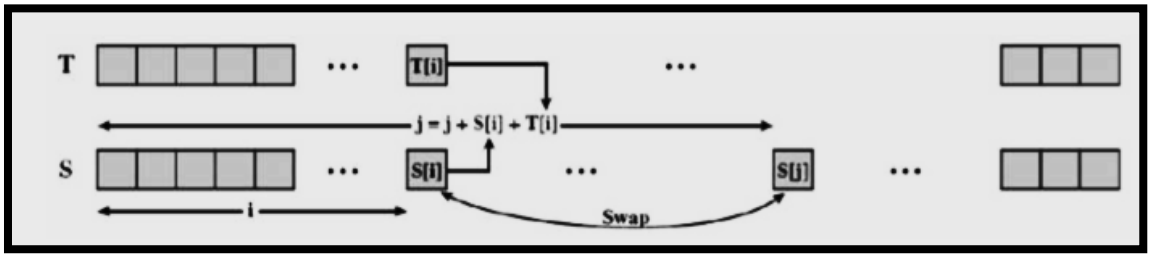


Figure III.7 : Initialisation de RC4

- Pour la génération des flux, la clé K n'est pas utilisée. Pour chaque S[i], on procède à un échange de contenu avec S[j]. Ensuite, on calcule un entier t = (S[i] + S[j]) mod 256 nécessaire pour déduire la clé K = S[t].

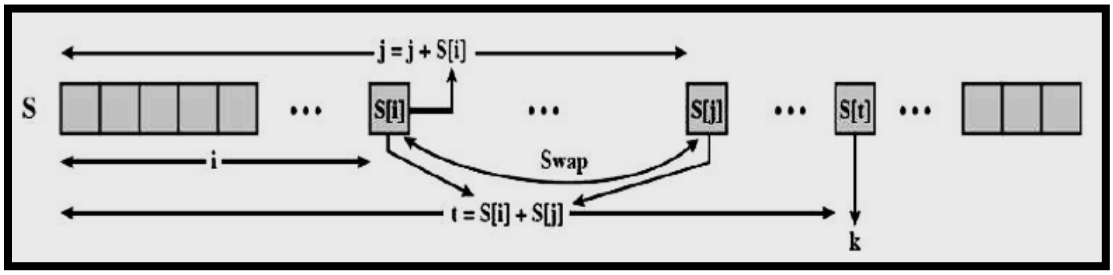


Figure III.8 : Génération du flux RC4

- La valeur de la clé K est utilisée pour les opérations de chiffrement et de déchiffrement. Le chiffrement est obtenu en réalisant une opération XOR entre un octet de la clé K et du message en clair. Le déchiffrement est obtenu en réalisant un XOR entre un octet de la même clé K et du texte chiffré. **[5]**

C. Algorithme

- 1er étépe : KSA

L'algorithme de Key Schedule initialise Aléatoirement la fonction S.

```
K := [ clef ]
L := longueur(K)
pour i de 0 à N
    S[i] := i
finpour
j := 0
pour i de 0 à 255
  j := j = j + S[j] + K[i]   mod 8
  échanger(S[i], S[j])
finpour
```

Figure III.9 :algorithme d'Initialisation de RC4

- 2émé étape :PRGA

Génére des octets pseudo-aléatoire, et les ajoute aux caractéres du message.

```
i := 0
j := 0
tant_que générer une sortie:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    échanger(S[i], S[j])
    octet_chiffrement = S[(S[i] + S[j]) mod 256]
    result_chiffré = octet_chiffrement XOR octet_message
fintant_que
```

Figure III.10 :Génération du flux RC4

D. Exemple de fonctinnemnt

- 1er étape

Les deux operation de la boucle sont

j := (j + S[j] + K[i] mod L) mod 256 échanger(S[i], S[j])

On prend N = 8 et K = [4,6,2,4,6,3,3,7] et donc L = 8

Step(i)	0	1	2	3	4	5	6	7	$j = j + S[j] + K[i] \mod 8$	Echange
Init.	0	1	2	3	4	5	6	7	0	
0		1	2	3		5	6	7	$0+0+4 \mod 8 = 4$	$S[0] \leftrightarrow S[4]$
1	4			3	0	5	6	7	$4+0+6 \mod 8 = 2$	$S[1] \leftrightarrow S[2]$
2	4	2		3	0		6	7	$2+1+2 \mod 8 = 5$	$S[2] \leftrightarrow S[5]$
3		2	5		0	1	6	7	$5+1+4 \mod 8 = 1$	$S[3] \leftrightarrow S[1]$
4		2	5	4		1	6	7	$1+2+6 \mod 8 = 1$	$S[4] \leftrightarrow S[1]$
5	0	2	5	4	3			7	$1+2+3 \mod 8 = 6$	$S[5] \leftrightarrow S[6]$
6	0	2		4	3	6		7	$6+1+3 \mod 8 = 2$	$S[6] \leftrightarrow S[2]$
7	0	2	5	4	3	6			$2+5+7 \mod 8 = 6$	$S[7] \leftrightarrow S[6]$

Tab III.2 :solution de L'exemple

- $2^{ème}$ étaper

On considéré le message M = [100,101,...]. nous appliquons l'algorithme PRGA.[49]

1. *Initialisation* $i = 0, j = 0$

k	0	1	2	3	4	5	6	7
$S[k]$	0	2	5	4	3	6	7	1

2. $i = 1, j = 0 + S[i] = 0 + 2$, on échange $S[1] \leftrightarrow S[2]$

k	0	1	2	3	4	5	6	7
$S[k]$	0			4	3	6	7	1

On chiffre le premier bloc de M. On a

$octet\_chiffrement = S[(S[i] + S[j]) mod 256] = S[5 + 2] = S[7] = 1$

et donc $C_1 = [100] \oplus [001] = 101$.

3. $i = 2, j = 2 + S[2] = 2 + 5 = 7$, on échange $S[2] \leftrightarrow S[7]$

k	0	1	2	3	4	5	6	7
$S[k]$	0	5		4	3	6	7	

On chiffre le deuxième bloc de M. On a

$octet\_chiffrement = S[(1 + 2) \mod 256] = S[3] = 4$ et donc

$C_2 = [101] \oplus [100] = 001$

Figure III.11 : suit de solution de L'exemple

I.2 Le chiffrement asymétrique :

La cryptographie asymétrique ou « à clé publique » se base sur l'utilisation d'une paire de clés de chiffrement. Les clés asymétriques sont générées par paire. La clé publique est extraite et publiée à travers des annuaires, par exemple, tandis que la clé privée est gardée secrète chez l'utilisateur. Un message chiffré par la clé publique est déchiffré par la clé privée, et inversement.

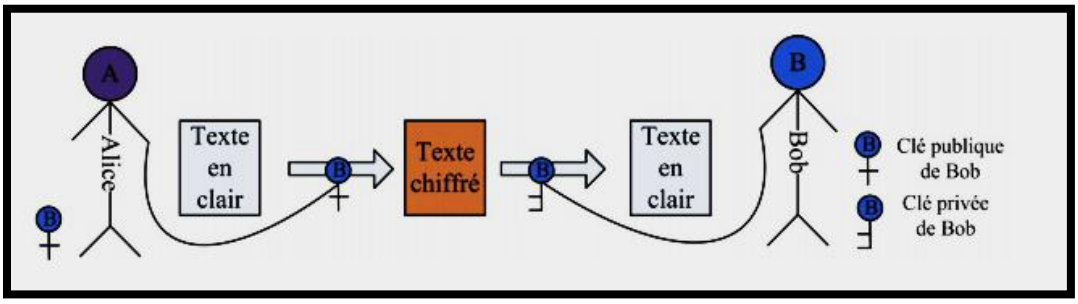


Figure III.12 : Chiffrement asymétrique.

I.2.1 RSA

R.S.A signifié Rivest-Shamir-Adleman (nommé par les initiales de ses trois inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman) est un algorithme de cryptographie asymétrique, il a été décrit en 1977.

Figure III.13 : les trois inventeurs de RSA

Le brevet de cet algorithme appartenait jusqu'au 6 Septembre 2000 à la société américaine RSA Data Security, qui fait maintenant partie de Security Dynamics et aux Public Key Partners, (PKP à Sunnyvale, Californie, états-Unis). Tout le principe de RSA repose sur le fait qu'il est très difficile et donc très long de décomposer un très grand nombre en deux grands facteurs premiers, sauf cas particuliers. **[46]**

- Le système RSA ne nécessite pas de transfert de clés entre l'expéditeur et le destinataire.
- Le système RSA est basé sur les fonctions à sens uniques, c'est-à-dire il est simple d'appliquer la fonction, mais extrêmement difficile de la trouvée à partir de son image seulement.

II. Gestion de clefs dans les réseaux par clef symétrique :

La gestion de clés fournit des mécanismes efficaces, sécurisés et stables de distribution de clés utilisés dans les opérations cryptographiques. Par conséquence, la gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Sous les contraintes des RCSF, la conception d'un système de gestion de clés est un grand défi. Sélectionner une solution cryptographique appropriée pour les RCSF est un autre défi.

La figure suivante résume les contraintes découlant des propriétés des RCSF, à prendre en compte dans la conception d'une solution de gestion de clés pour les RCSF.

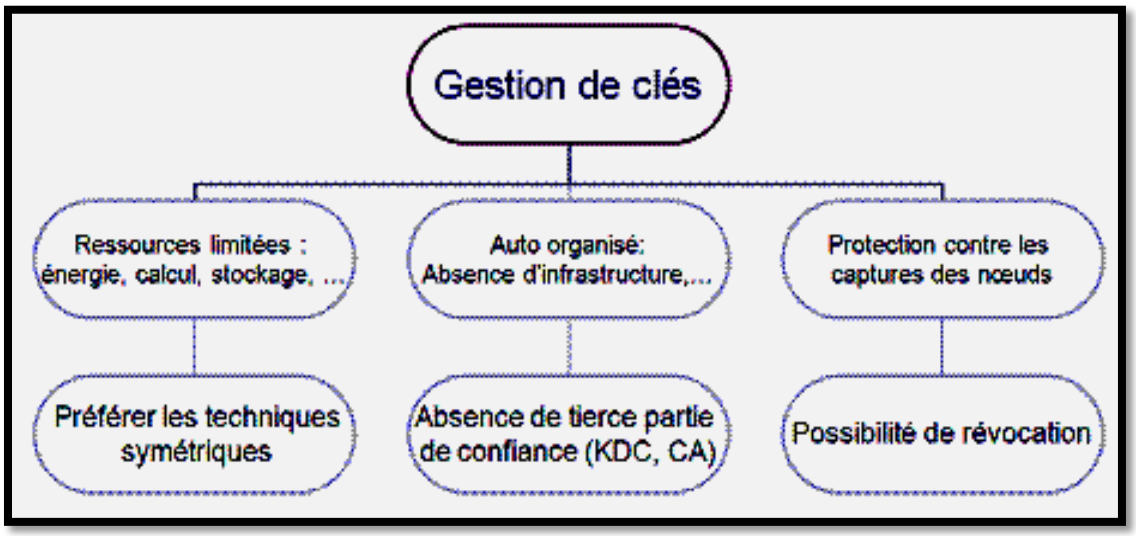


Figure III.14 : Contraintes de conception de solutions de gestion de clés

Bien que la cryptographie à clé publique comporte des avantages certains par rapport à la cryptographie à clé symétrique et malgré les recherches qui visent à les appliquer aux RCSF, la cryptographie à clé symétrique possède ses propres qualités qui la rend toujours la plus préférée pour les RCSF. Pour cette raison la plupart des schémas de gestion de clés proposés pour les RCSF sont basés sur la cryptographie symétrique. Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui facilite l'établissement des clés entre les nœuds. La solution commune est d'utiliser une méthode de pré-distribution, dans laquelle les clés sont chargées dans les nœuds capteurs avant le déploiement.

Nous avons choisi quelque solutions qu'ils sont garanti des certains niveaux de sécurité :

II.1 Clé individuelle :

Chaque nœud possède une clé personnelle partagée uniquement avec la station de base.

Après chaque envoi, le nœud émetteur chiffre son message avec sa clé personnelle et restera anonyme sur le réseau jusqu'à atteindre la station de base. Cette solution présente des avantages de sécurité pour sa simplicité mais demeure inappropriée pour les architectures où on effectue des traitements sur les données (exemple : agrégation de données).

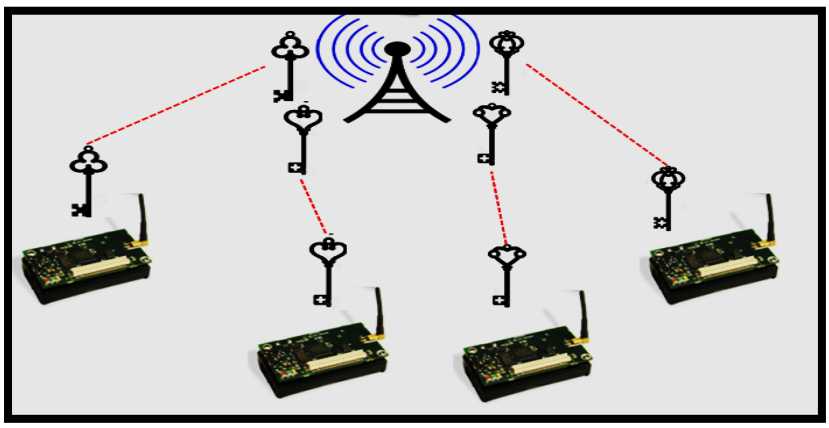


Figure III.15 : la sécurité dans RCSF par un Clé individuelle

II.2 Clé globale :

Une seule et même clé est partagée par tous les nœuds du réseau. Un message est chiffré et déchiffré par la même clé (principe de clé symétrique). Cette solution est très économe en énergie mais moins sure et moins sécurisante. Toutefois, si un attaquant récupère la clé, il pourra déchiffrer tous les messages circulant sur le réseau.

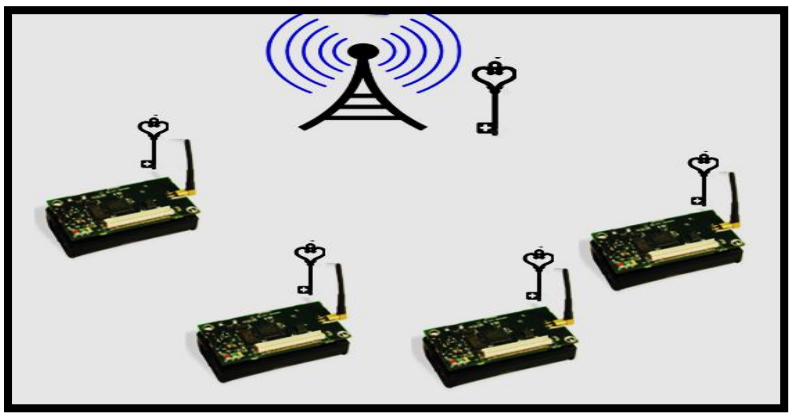


Figure III. 16 : la sécurité dans RCSF par un Clé globale

II.3 Clé partagée par paire de nœuds :

C'est une solution plus sûre mais plus couteuse en énergie. Le principe est que chaque nœud du réseau partage une clé avec son voisin, ainsi si un nœud possède n nœuds voisins, il doit stocker n clés. Après chaque envoi, le nœud source chiffre son message avec la clé de son voisin et après chaque réception, le nœud destinataire déchiffre le message avec sa clé et le chiffre à nouveau avec la clé de son voisin, et ce,

jusqu'à atteindre la station de base. Une quantité énorme d'énergie sera dissipée dans les opérations de chiffrement et de déchiffrement pour chaque envoi.

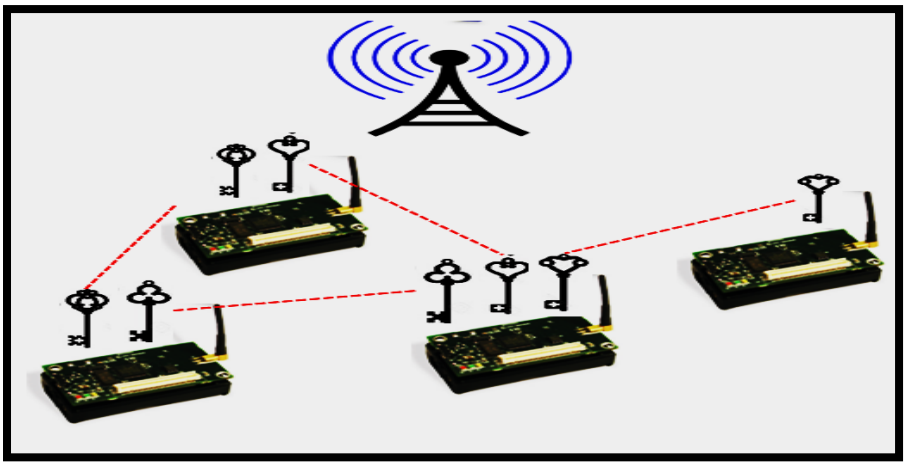


Figure III.17 : la sécurité dans RCSF par un Clé partagée par paire de nœuds

II.4 Clé partagée par groupe de nœuds :

Les clés sont établies sur deux niveaux :

Une clé partagée par les nœuds du même cluster et une clé partagée par les nœuds chefs de zones.

- D'abord Le chiffrement se fait avec une clé partagé entre les membres du même cluster
- Chaque chef de cluster déchiffre les messages par ce même clés partagés et ré-chiffré avec la clé partagé entre les nœuds chefs de zone.

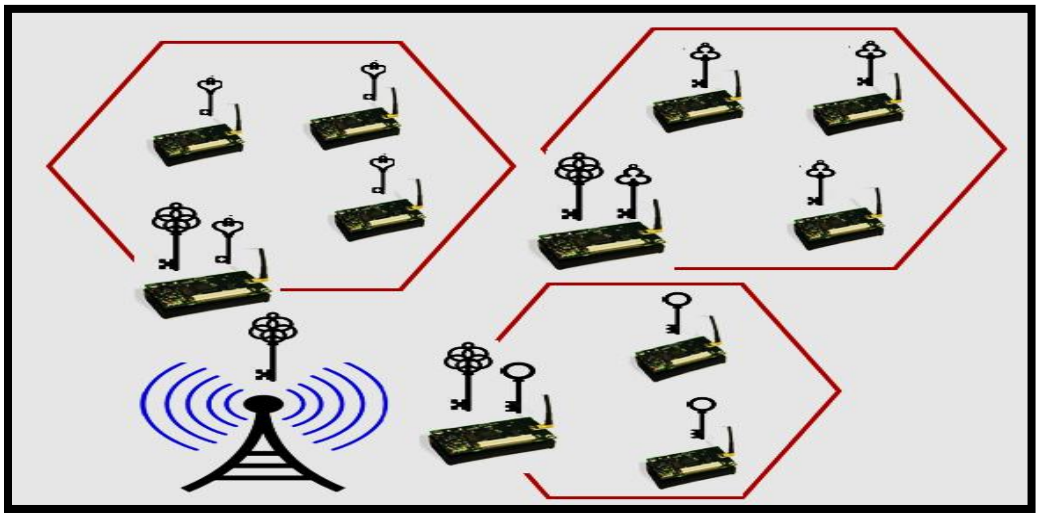


Figure III.18 : la sécurité dans RCSF par un Clé partagée par groupe de nœuds

III Gestion de clef par clef asymétrique micro PKI :

Les derniers avancés dans les technologies de capteurs sans fil ont permet une augmentation dans la puissance de calcul qu'a permet l'utilisation de la cryptographie a clef publique. Micro-PKI (Micro Public Key Infrastructure), est une version simplifiée des PKI conventionnelles, dans laquelle seule la station de base possède une clé publique et une autre privée.

La clé publique est utilisée par les nœuds du réseau pour authentifier la station de base, et la clé privée est utilisée par la station de base pour déchiffrer les données envoyées par les nœuds.

Avant le déploiement, la clé publique de la station de base est stockée dans tous les nœuds. Dans cette méthode, il y'a deux types d'authentification (HandShake).

Le premier type d'authentification se fait entre un nœud du réseau et la station de base. Le nœud génère une clé symétrique de session et la chiffre avec la clé publique de la station de base. La clé chiffrée est transmise à la station de base sans être déchiffrée en chemin puisque les nœuds ne connaissent pas la clé privée de la station de base. À la réception, la station de base déchiffre la clé de session et la stocke dans une table.

Le deuxième type d'authentification se déroule entre n'importe quel couple de nœuds du réseau en passant par la station de base. Cette dernière joue le rôle de l'authentificateur entre eux. L'un des deux nœuds envoie une requête à la station de base contenant l'identifiant de l'autre nœud. À la réception, la station de base génère une clé aléatoire et la chiffre avec la clé de session correspondante au nœud émetteur de la requête.

Pour les nouveaux nœuds désirant rejoindre le réseau, il suffit de stocker dans ces nœuds la clé publique de la station de base avant le déploiement. **[12]**

Conclusion

Nous avons présenté dans ce chapitre un état de l'art qui détaille les synthèses bibliographiques des algorithmes de cryptographie et des mécanismes qui peuvent sécuriser les réseaux. L'adaptation de ces derniers aux RCSF représente de grands challenges.

Dans le chapitre suivant, on présente les outils logiciels et matériels ainsi que la démarche à suivre pour réaliser une application dans le but de mesure la température et l'échangé sécurisé par les capteurs.


Chapitre 4

Introduction

Depuis quelques décennies, le besoin d'observer et de contrôler les environnements est devenu essentiel pour de nombreuses applications. Ceci nécessite une nouvelle technologie qui prend en considération la sensibilité de l'environnement et qui fournit des informations pertinentes sur le milieu balayé. Cette technologie est capable de détecter différents types d'informations, comme la température, l'humidité, la lumière, les vibrations sismiques, et la présence ou la nature d'organismes biologiques.

Ce chapitre propose une mise en œuvre d'un réseau de capteur sans fil, capable de surveiller la température dans un environnement domestique tel que les maisons, et la sécurisation des transferts des données entre les capteurs et la station de base en utilisant un système de gestion de clé basé sur la cryptographie symétrique.

I. Cadre general du travail :

L'idée majeure de notre travail est d'implémenter un réseau de capteurs sans fil capable de mesurer la température ambiante dans un environnement domestique et envoyer ces mesures vers la station de base. Le système de surveillance de la température sera compléter par un mécanisme de gestion de clé afin de distribuer les clés cryptographique aux capteurs. Ce mécanisme de sécurité sera basé sur la cryptographie symétrique. L'utilisation de ce type de cryptographie vient du fait que les capteurs et vis-à-vis leur capacité de stockage et de calcul ne peuvent pas utiliser d'autre technique de cryptographie tel que la cryptographie asymétrique.

II.Matérielle utilisé :

Afin de mettre en œuvre ce réseau on a utilisé un ensemble de capteurs de type telesb, l'architecture générale de ces capteurs sera comme suite.

II.1 L'architecture d'un capteur :

Un nœud capteur contient quatre unités de base :

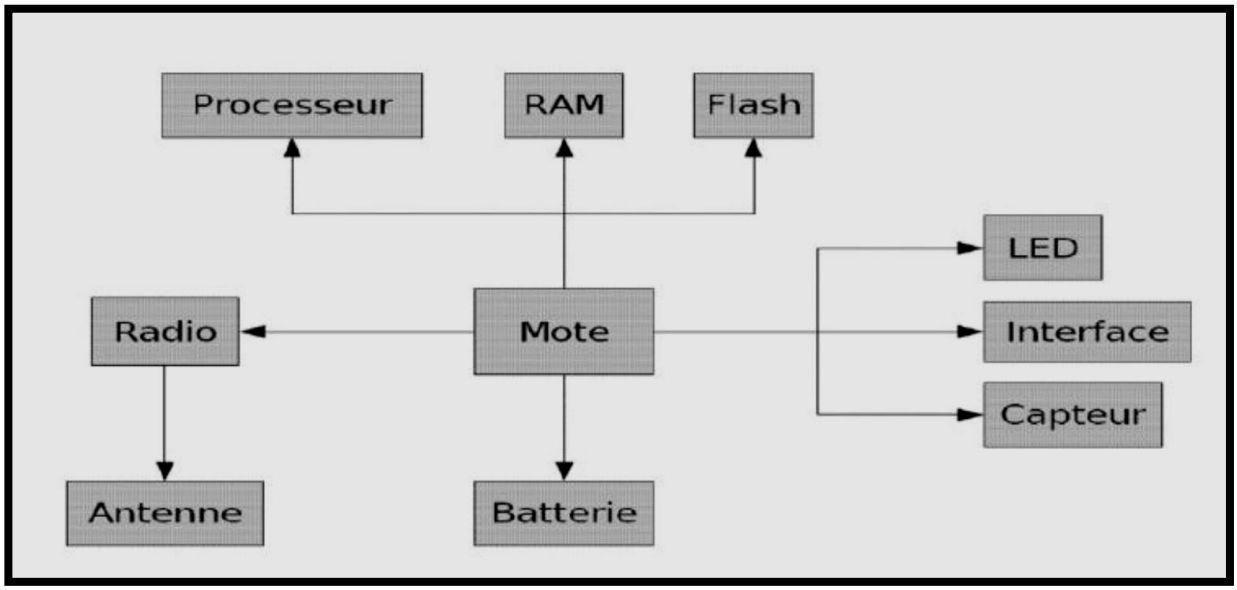


Figure IV.1 : Architecture d'un capteur sans fils

On peut voir sur la figure les différents composants qui constituent un capteur. Pour être plus précis chaque groupe des composants possède son propre rôle :

II.1.1 Unité de traitement

Mote, processeur, RAM et Flash : On appelle généralement Mote la carte physique utilisant le système d'exploitation pour fonctionner. Celle-ci a pour cœur le bloc constitué du processeur et des mémoires RAM et Flash. Cet ensemble est à la base du calcul binaire et du stockage, temporaire pour les données et définitif pour le système d'exploitation. Cette unité est chargée d'exécuter les protocoles de communications qui permettent de faire collaborer le nœud avec les autres nœuds du réseau. Elle peut aussi analyser les données captées pour alléger la tâche du nœud puits.

II.1.2 Unité de transmission

Radio et antenne : les équipements étudiés sont donc généralement équipés d'une radio ainsi que d'une antenne. Cette unité est responsable d'effectuer toutes les émissions et réceptions des données sur un medium sans fil. Elle peut être de type optique (comme dans les nœuds Smart Dust), ou de type radiofréquence ou acoustique. Les communications de type optique sont robustes vis-à-vis des interférences électriques. Néanmoins, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes. Par conséquent, elles ne peuvent pas établir de liaisons à travers des obstacles.

II.1.3 Unités de captage

LED, interface, capteur : On retrouve donc des équipements de différents types de détecteur et d'autre entrée. Le capteur est généralement composé de deux sous-unités : le récepteur (reconnaissant l'analyste) et le transducteur (convertissant le signal du récepteur en signal électrique). Le capteur est responsable de fournir des signaux analogiques, basés sur le phénomène

observé, au convertisseur Analogique/Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement.

II.1.4 Unités de control d'énergie

Batterie : Un micro-capteur est muni d'une ressource énergétique (généralement une batterie de type AAA) pour alimenter tous ses composants. Cependant, en conséquence de sa taille réduite, la ressource énergétique dont il dispose est limitée et généralement irremplaçable. Cette unité peut aussi gérer des systèmes de rechargement d'énergie à partir de l'environnement observé telles que les cellules solaires, afin d'étendre la durée de vie totale du réseau. **[4]**

II.2 Capteur utilisée

Nous utilisons un capteur sans fil de type TelosB et se prénomme MTM-CM5000-MSP.de « MAXFOR TECHNOLOGY ING ». Il est composé d'un microcontrôleur MSP430 :

- d'un émetteur-récepteur,
- d'un capteur de température et d'humidité,
- d'un capteur de luminosité pour le domaine du visible, d'un autre pour l'infrarouge,
- d'un « bouton utilisateur »,
- d'un bouton reset,
- de trois LEDs,
- d'un port USB...

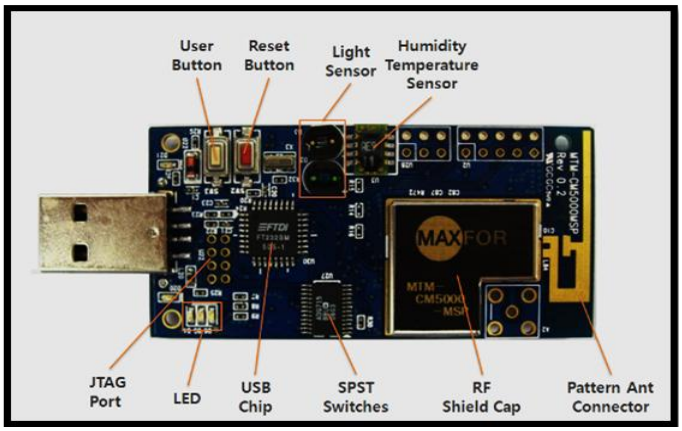


Figure IV. 2: Description de capteur Mtm-cm5000-msp

En résumé, ce mote est bien équipé.Le capteur de température détecte des températures allant de

-40°C à 123°C, avec une précision de l'ordre de 0,4°C. Pour fonctionner, un mote a besoin de deux piles de 1,5V, sa durée de vie est donc limitée par le voltage des piles. En outre, il possède 10kB de mémoire vive et seulement 48kB de mémoire flash, ce qui est relativement peu. Dans le réseau de capteurs sans-fil que nous souhaitons déployer, chaque nœud communique avec ses voisins en Wi-Fi sur la bande de fréquence 2,4GHz. **[48]**

III. logiciel utilisé :

L'environnement utilisé pour implémenter notre application sera représenté dans ce qui suit. Nous avons utilisé « TinyOS » comme système d'exploitation et le «nesC» comme langaged'implémentation.

III.1 Virtuelle machine

VirtualBoxest un logiciel de virtualisation de systèmes d'exploitation. En utilisant lesressources matérielles de l'ordinateur (système hôte), VirtualBox permet la création d'un ou deplusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation(systèmes invités).

Les systèmes invités fonctionnent en même temps que le système hôte, mais seul cedernier a accès directement au véritable matériel de l'ordinateur. Les systèmesinvités exploitent du matériel générique, simulé par un « faux ordinateur » (machine virtuelle)créé par VirtualBox.

La réalisation de la plateforme de notre expérimentation nécessite le choix d'un systèmed'exploitation car il existe plusieurs versions de TinyOS, la version qui nous intéresse est le **TinyOS-2.x**parce qu'il est le plus développé en termes d'applications par rapport auxanciennes versions. **[43]**

III.2 TinyOS

Figure IV. 3 : Logo de TinyOS.

TinyOS est un système d'exploitation Open Source pour les réseaux des capteurs, conçu par l'université américaine de BERKELEY. Le caractère open source permet à ce système d'être régulièrement enrichie par une multitude d'utilisateurs. Sa conception a été entièrement réalisée en NesC, langage orienté composant syntaxiquement proche du C. Il respecte une architecture basée sur une association de composants, réduisant ainsi la taille du code nécessaire à sa mise en place. Cela s'inscrit dans le respect des contraintes de mémoires qu'observent les capteurs, pourvus de ressources très limités dues à leur miniaturisation. Pour autant, la bibliothèque des composants de TinyOS est particulièrement complète, puisqu'on y retrouve des protocoles réseaux, des pilotes de capteurs, et des outils d'acquisition de données. Un programme s'exécutant sur TinyOS est constitué d'une sélection de composants systèmes et de composants développés spécifiquement pour l'application à laquelle il sera destiné (mesure de température, du taux d'humidité…).

TinyOS s'appuie sur un fonctionnement évènementiel, c'est à dire qu'il ne devient actif qu'à l'apparition de certains évènements, par exemple l'arrivée d'un message radio. Le reste du temps, le

capteur se trouve en état de veille, garantissant une durée de vie maximale connaissant les faibles ressources énergétiques des capteurs. Ce type de fonctionnement permet une meilleure adaptation à la nature aléatoire de la communication sans fil entre capteurs. **[4]**

III.3 Langage de programmation NesC :

NesC est comme le langage de programmation C basé sur des composants. NesC est développé grâce à la contrainte de systèmesembarqués.

L'implémentation avec le langage NesC est simple, et permet aussi de minimiser la taille du code vu le critère de la capacité limitée de lamémoire.**[20]**

Dans la pratique, NesC permet de déclarer 2 types de fichiers : les modules et lesconfigurations.

IV. Installation logicielle

Pour mettre en œuvre les programmes dérivésprécédemment on a besoin d'un certain nombre de logiciels pour programmer et implémenter l'application. La majorité de ces logiciels sont des logiciels libres tels que Virtual Box Linux.

- Pour commencer, nous devons installer le VirtualBoxpour exécuter Linux à sous de Windows et cela pour pouvoir utiliser l'outil de développement de TinyOS.
- Dans ce programme, nous allons créer une machine virtuelle.
- Nous avons choisir le type de système d'exploitation qui sera installé dans la machine virtuelle, qu'est l'environnement Linux (Ubuntu).

V. Installation matérielle :

Une fois l'installation logicielle terminée, il a fallu installer le matériel :

- une station de base reliée à l'ordinateur via un câble USB.
- différents capteurs telosB (Sender/Receiver).
- chaque capteur mesure la température.

Figure IV.4 : Le matérielle utilisé.

VI. Le déploiement du système :

Cette application est utilisée pour surveiller et mesurer la température dans tous les endroits du bâtiment (les chambres, la cuisine et la serre...). Le système est composé d'un ensemble des capteurs de type teloseB. Ces capteurs doivent être déposés dans des endroits bien protégés contre le sabotage ou d'utilisation malveillante.

Ces capteurs sans reliées les uns aux autres à l'aide d'une liaison sans fil vers une station de base, cette dernière permet de visualiser les alertes en cas de feux, trop de chaleur fourni par les chauffages, et d'augmentation ou diminution de la température dans les serres (Trop élevée ou trop froide, peut ralentir le développement des plantes cultivées à l'intérieur).

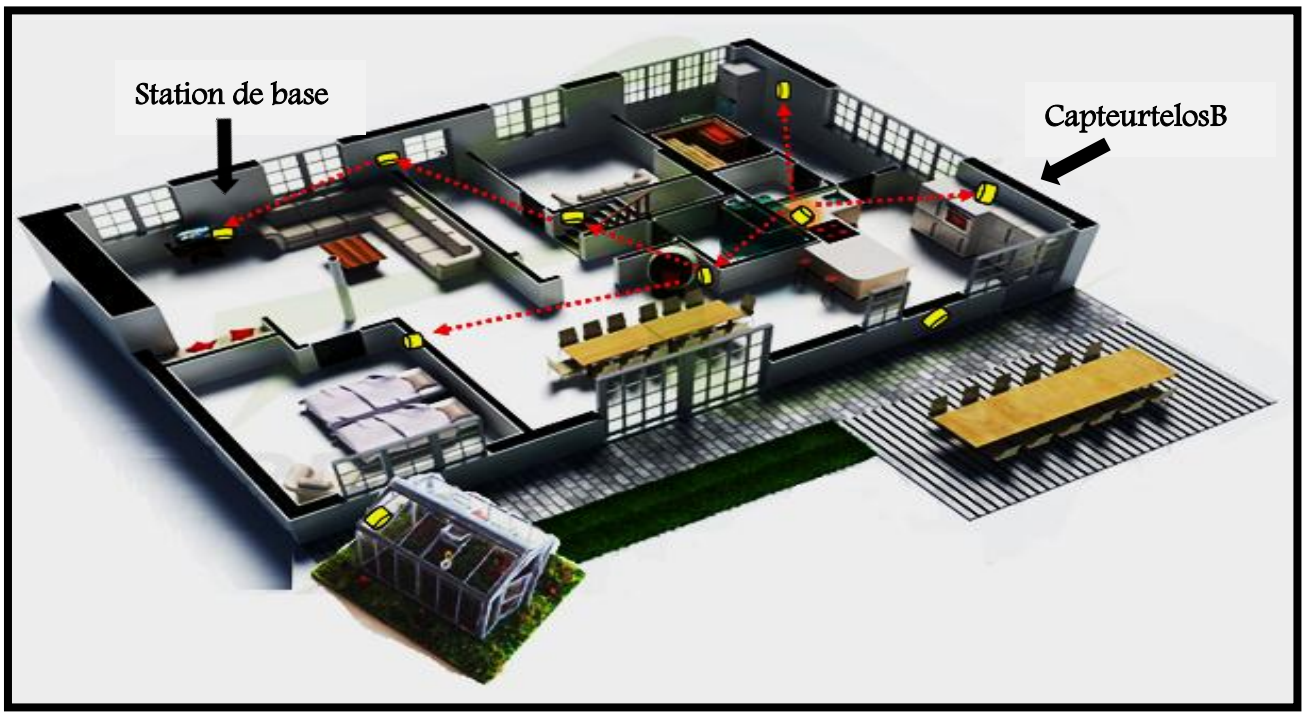


Figure IV.5 : Exemple d'utilisation un RCSF dans une maison.

VI.1 Les principales fonctionnalités de l'application :

Pour contrôler la température par les capteurs, l'application doitcomposerdes fonctionnalités suivantes :

VI.1.1 Captage de la température :

Chaque capteur telosB mesure périodiquement la température ambiante, et vérifie si elle dépasse certain seul, si oui il envoie une alerte vers la station de base, cet alerte sera acheminer par les autres capteurs en utilisant des liaisons sans fil de proche en proche jusqu'à ce qu'il arrive à la station de base.

Si $T>T_{seul}$, alors envoi alerte (T) ;

Sinon rien ;

VI.1.2 Envois des alertes :

Comme mentionné dans la section précédente, chaque capteur mesure périodiquement la température ambiante dans les chambres, hall ou les serres et teste si cette mesure dépasse un certain seuil fixé par le propriétaire de la maison, dans ce cas le capteur envoi une alerte vers la station de base en utilisant le protocole de routage sou jacent, cette alerte contient la valeur de la température ainsi que les coordonnées GPS de l'endroit où le prélèvement de la température a eu lieu, la structure des alertes est la suivante :

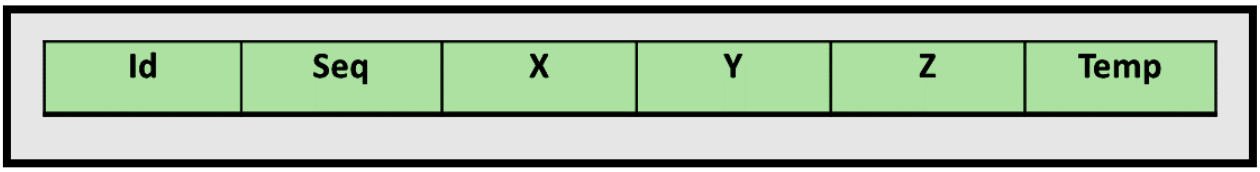


Figure IV. 6 : Structure de paquet.

- **Id** : définit l'identificateur de chaque capteur.
- **Seq** : définit le numéro de séquence utilisé par les capteurs afin d'éviter qu'un message alerte soit traiter deux fois.
- **(x,y,z)** :la position de capteur.
- **Temp** : la température mesurée par le capteur.

VI.1.3 Le routage « Flooding»

Pour simplifier l'implémentation du système et vue sa taille qui ne dépassera pas la taille d'une maison, on a proposé d'utiliser le flooding comme méthode de routage. Le floodingou diffusiondirect est une manière d'acheminer les messages, vers tous les capteurs du réseau d'une manière aveugle sans aucun traitement spécial.

Les applications de cette opération sont nombreuses, telles que la découverte des routes, la découverte des services, le lancement d'alertes au sein du réseau, la synchronisation ou encore la dissémination d'informations ou d'ordres pour un réseau des capteurs. La diffusion est donc un processus dont l'efficacité est primordiale pour le bon fonctionnement du réseau.

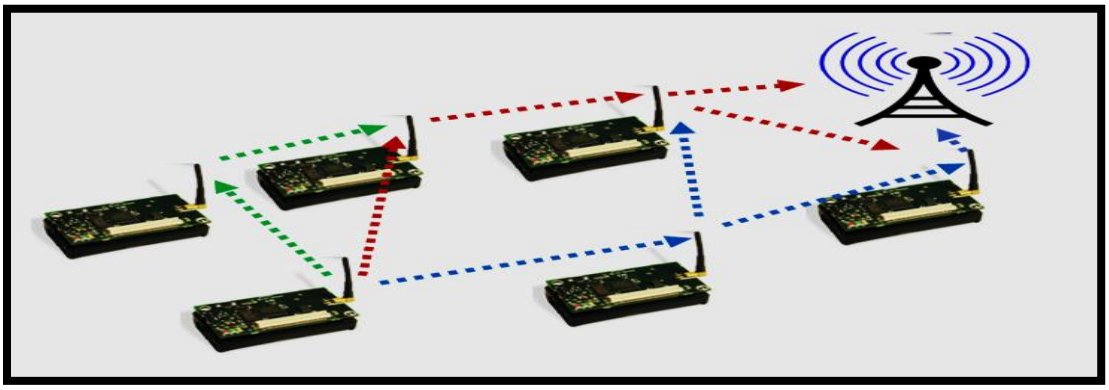


Figure IV.7 : La diffusion d'un paquet.

La diffusion aveugle (ou blindflooding en anglais). Son principe est que chaque hôte recevant pour la première fois le message à diffuser réémet celui-ci à destination de ses voisins. Si le réseau est connexe (il existe un chemin entre la source et n'importe quel autre hôte) et que l'on suppose l'absence de collisions, alors ce processus aboutit à une couverture complète du réseau. Malheureusement, cet algorithme très simple n'est pas efficace car il requiert la participation de tous les hôtes, alors que cela n'est pas toujours nécessaire. En conséquence, il conduit à une grande quantité des messages redondants et d'énergie gaspillée. Pour minimiser l'effet de la redondance on utilise un numéro de séquence pour chaque nouveau paquet acheminer, ce numéro est vérifié par les nœuds intermédiaires afin pour éviter le traitement multiple de même paquet.

Si Seq>SeqA, alors renvoi(T) ;

Si non rien ;

VI.1.4 la station de base :

La station de base se présente sous forme d'un capteur relié à un ordinateur permet de visualiser les mesures et les alertes envoyés par les capteurs, en utilisant une interface graphique dans notre cas simple avec un minimum des commandes car le système n'effectue pas des taches complexes.

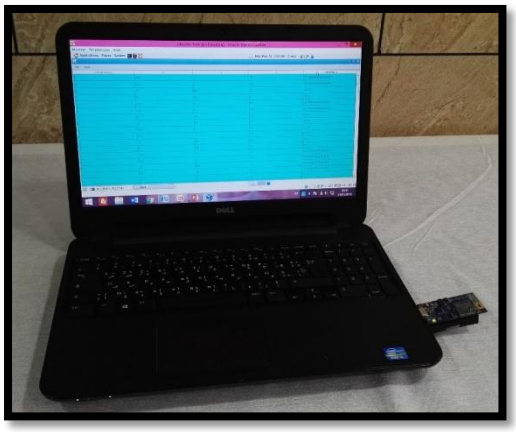


Figure IV.8 : station de base relai a une ordinateur

VII. sécurisation du système de contrôle de latempérature :

Le déploiement des réseaux de capteurs sans assurer la sécurité est une grande erreurparce qu'ils sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques.

Quiconque possédant le récepteur adéquat peut potentiellement écouter ou perturber les messages échangés, et exécuter des attaques comme l'écoutes sur le réseau et l'analyse du trafic ou même la modification du paquet, usurpation d'identité, saturation du réseau et déni de service

Les nœuds eux-mêmes sont des points de vulnérabilité du réseau car une attaque peut compromettre un composant laissé sans surveillance, dans notre cas cette attaque n'est pas envisager car les capteurs sont déployer à l'intérieur de la maison loin de tout sabotage ou vole.

Dans la section suivante on va présenter un mécanisme de gestion de clef permettant de distribuer d'assurer la sécurité de notre réseau utilisant la cryptographie symétrique et l'algorithme RC4.

VII.1 Descriptiongénérale du mécanisme de gestion de clé :

Notre proposition sera basée sur l'utilisation de la cryptographie symétrique, Bien que la cryptographie à clé asymétrique comporte des avantages certains par rapport à la cryptographie à clé symétrique et malgré les recherches qui visent à les appliquer aux RCSF, la cryptographie à clé symétrique possède ses propres qualités qui la rend toujours la plus préférée pour les RCSFs (la consommation d'énergie due au calcul des algorithmes, et le stockage des clés connues pour être plus petites que les clés asymétriques). Pour cette raison la plupart des schémas de gestion de clé proposés pour les RCSF sont basés sur la cryptographie symétrique.

Dans notre proposition de gestion de clefs on a utilisé deux clés cryptographiques une globalement partagées par les capteurs afin d'assure le routage et l'autre individuelle pour chaque capteur partagées avec la station de base :

VII.1.1 Le chiffrement par une clé globale

Tous les capteurs utilisent une clé globale (Une seule et même clé est partagée par tous les nœuds du réseau) soit pour le chiffrement soit pour le déchiffrement.

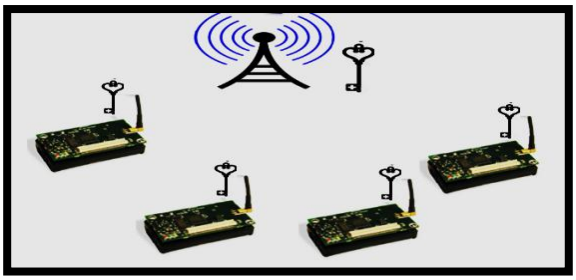


Figure IV. 9 : La sécurité dans RCSF par un Clé globale

VII.1.2 Chiffrement par une clé individuelle

Chaque nœud possède une clé personnelle partagée uniquement avec la station de base. Cette clef sert à sécuriser les paquets dans la période de diffusion car les capteurs intermédiaires doivent lire des données comme le numéro de séquence afin d'éviter la rediffusion à l'infini de ces messages.

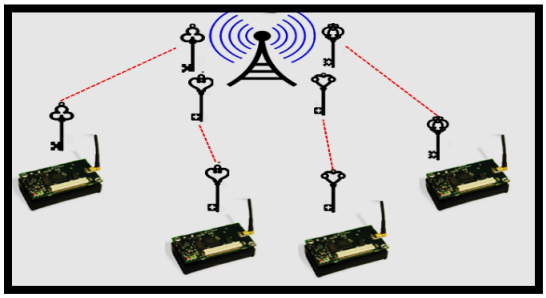


Figure IV. 10: La sécurité dans RCSF par un Clé individuelle

VII.2 Démarrage de système :

Avant le déploiement des capteurs dans leurs positions une configuration doit être effectué pour assurer la sécurité cette configuration consiste à fixer les clés globale et individuelle pour chaque capteur. La clef individuelle est une clef secret entre la station de base et le capteur cette dernière est générer aléatoire et stockée au niveau de la station de base dans la table des clefs et la deuxième clé c'est la clef globale elle est la même pour tous les capteurs. Apres cette étape les capteurs sont déposés aléatoirement dans des endroits sure.

Les clefs utilisées sont des clés de taille de 128 bit car les capteurs ne peuvent pas supporter des clefs pus longue.

Remarque :pour ajouter un nouveau nœud a notre réseau tous simplement nous suivons ces même démarche de déploiement.

VII.3 Utilisation des clés

Avant d'envoyer un paquet, il doit être crypté en utilisant les deux clefs définies précédemment :

- **Utilisation de la clef globale** : cette clef est partagée entre tous les capteurs du réseau et sert à crypter l'identificateur et le numéro de séquencequisont utilisés dans le routage donc ils doivent être connus par tous les nœuds de réseau. Pour cela nousavonsutilisé la clé partagéepourchiffrer ces premier 32bit de paquet Voilà la structure de paquet après le premier cryptage

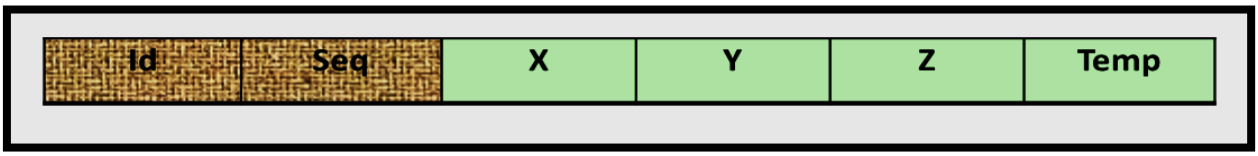


Figure IV. 11 : Structure de paquet après le 1er chiffrement.

- **Clef individuelle :** cette clef est utilisé pour chiffré le reste du paquet à savoir les coordonnées GPS et la valeur de la température, ces informations ne doivent connus que par la station de base et le capteur concernée donc on utilisé la clef pré-partagée entre ces deux correspondant, la station de base arrive à déchiffrer ces champs à l'aide d'une table contenant les clefs partagés avec chaque capteur

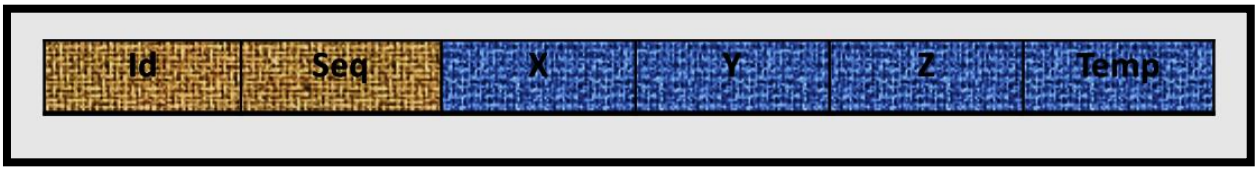


Figure IV.12: Structure de paquet après le 1er chiffrement.

- **Traitement des paquets par les nœuds intermédiaires :** après avoir effectué les deux opérations sur le paquet ce dernier est envoyé vers la station de base

- Les nœuds intermédiaires déchiffrent par la clé globale l'identificateur et le numéro de séquence pour vérifier si ce paquet est déjà traité ou non si ce paquet est reçu pour la première fois les nœuds intermédiaires le ré-envoi vers les nœuds voisins jusqu'à ce qu'il arrive à la station de base.
- Après la réception du paquet par la station de base, elle utilise la clé globale pour déchiffrer l'identificateur et le numéro de séquence.En utilisant l'identificateur du capteur elle détermine la clé individuelle partagée avec ce capteur en utilisant la table des clefs, car dans cette table chaque identificateur du capteur est associé àune clef de 128 bits.
- La clef est utilisé ensuite pour déchiffré le reste de paquet (la position et la température) et afficher ces paramètre sur l'écran..

N° d'identificateur	Clé individuelle
Id_1	$Clé_1$
Id_2	$Clé_2$
⋮	⋮
Id_n	$Clé_n$

Tableau IV.1 : table association entre l'identificateur et la clé individuelle

VII.4 L'algorithme utilisé

Nous avons utiliséun algorithme de chiffrement à flot qui est le RC4.

- nous générons un tableau pseudo-aléatoire à partir de clé globale.
- Cette suite des bits utilisés pour chiffrer le message via un XOR.

Nous avons fait cette opération 2 fois une seule par la clé globale qui nous avons nommé RC4et l'autre par la clé individuelle nommé RC14.

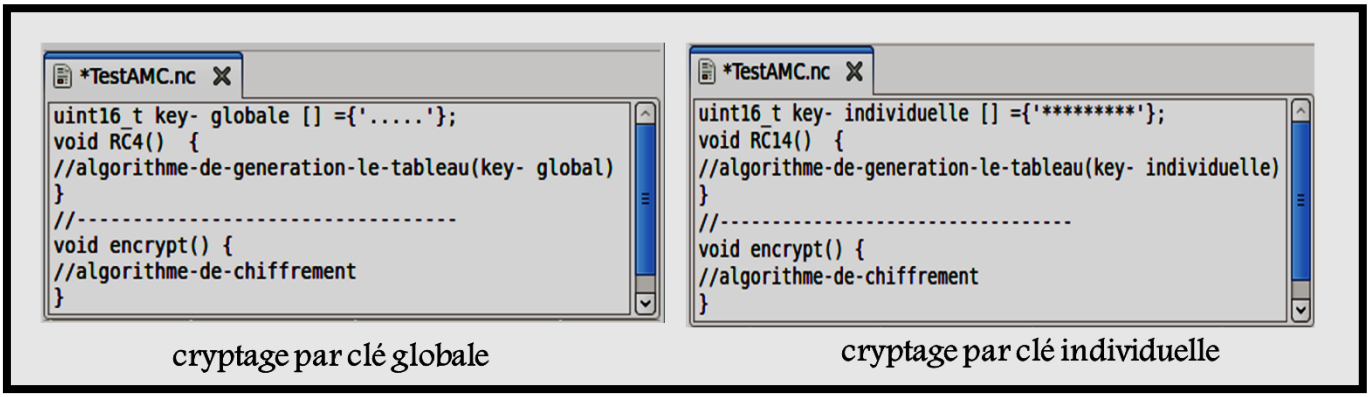


Figure IV.13 : Structure de programme de cryptage par algorithme RC4

VIII. L'implémentation de notre application :

Tout d'abord, Nous avant commençai par installé notre matérielle et logicielle.Suite à cela, on va installer le programme dans les capteurs et pour faire cette étape, il faut d'abord le compiler pour obtenir une image binaire sous TinyOS.

Les commandes pour compiler et installer le programme sont :

- Cd /desktop /temperature
- Maketelosb
- Make telosb reinstall bsl, /dev/ttyUSB0

Les trois lignes de commandes montrent respectivement, la méthode d'accès au répertoire (température) qui contient l'application, la compilation de cette application et l'installation de cette dernière dans le capteur.

Après l'installation de programme dans les capteurs, ces derniers peuvent collecter la température et la communiquer aux autres capteurs.

➢ Ensuite nous avons déployé nos capteurs dans des différents endroits d'une maison.

Figure IV.14 : le déploiement des capteurs dans unemaison

Remarque : Au cours de notre travail, on a pris le seuil de température égale à 20°C juste pour visualiser les résultats.

Mais ce seuil dépend de l'application et l'endroit de déploiement des capteurs, par exemple :

- si nousvoulonsjustecontrôlé la température d'une chambre, il doit être compris entre 18 et 25°C (La plupart des scientifiques estiment que la température (18-25) est généralement optimale pour la santé humaine).
- pour que les capteurs déclenchent une alerte de feu d'une forêt$T_{seuil} \geq 70°$.
- Pour maîtriser la température dans une serreil doit être compris entre 12 et 36°C…

➢ Après la réalisation de notre travail, nousavonsinstalléunestationde base qui permet le traitement et l'analyse des données collectées et la vérification des alertes

VIII.1 Visualisation des résultats :

Les Leds des capteurs clignotent chaque huit secondes par la couleur verte. Cela nous permet de savoir qu'un capteur détecte la chaleur et annonce unealerte(après un dépassement de certain seuil de température).

La figure suivante illustre la diffusion des messages d'alerte :

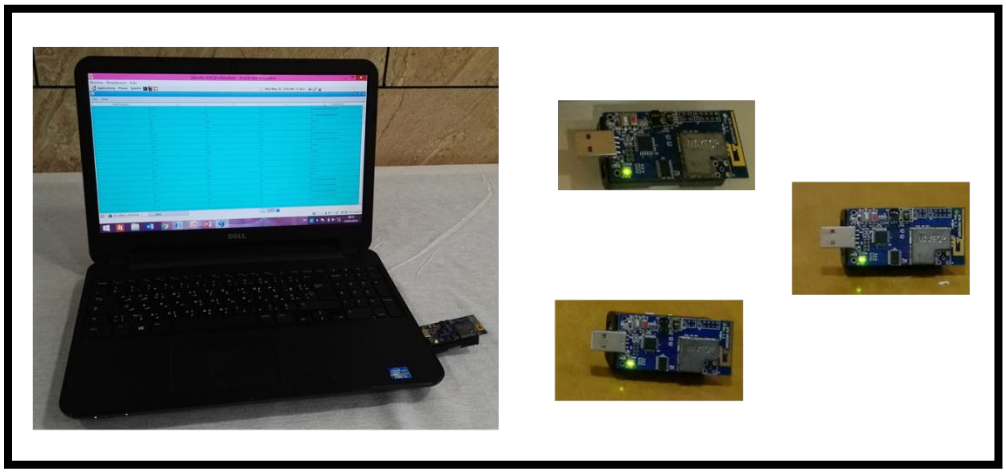


Figure IV.15 : Diffusion d'alerte entre les nœuds de restau

Les résultats récoltés par la station de base sont e hexadécimal, Le résultat obtenu est illustré dans la figure :

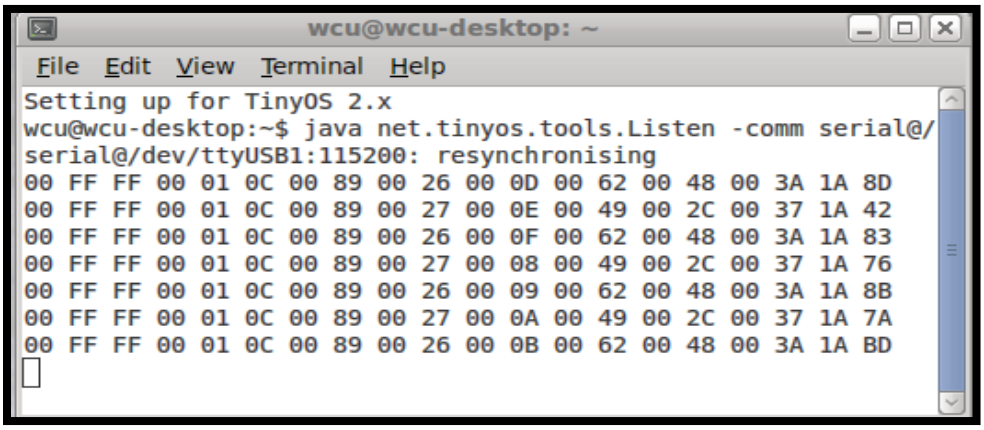


Figure IV.16 : détection d'alerte dans la station de base

D'après cette figure nousdéduisons que le rôle de la station de base consiste à afficher l'alerte sous forme des valeurs en hexadécimale en respectant l'ordre de la structure de programme : N° de l'identificateur, numéro de séquence, coordonnées (X, Y, Z) et le paramètre de température

Nous avons créé une interface sur l'environnement java sous la forme d'une fenêtre qui contient la valeur de température détectée par les capteurs en décimale ainsi que les identificateurs et les

coordonnées (X, Y, Z)de ces derniers. Cela est illustré dans la figure suivante :

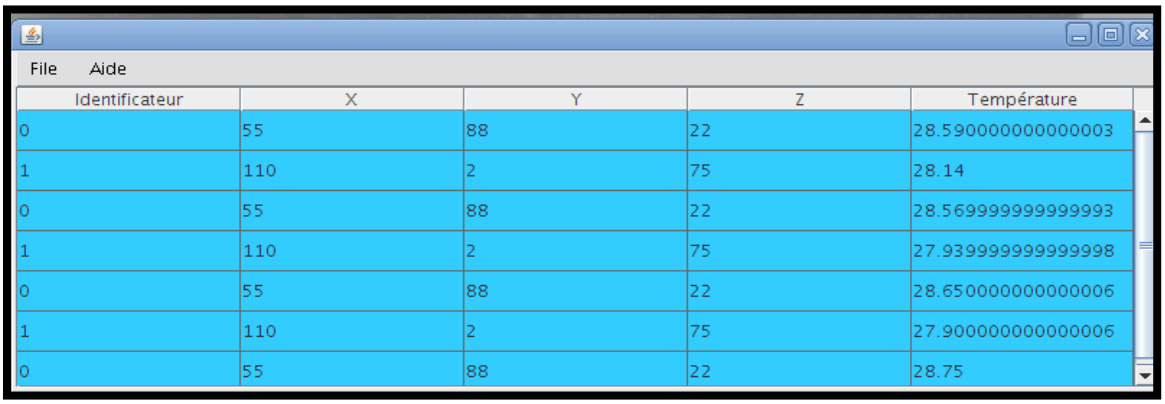


Figure IV.17 :Affichage d'alerte

IX. Analyse de sécurité pour cesystème :

Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace.Dans cette section on va citer comment notre mécanisme de sécurité permet de garantir les services de sécurité et faire face aux attaques habituelles.

IX.1 Les services de sécurité garantie :

- **La confidentialité :**Ce critère permet de garantir que les données échangées entre capteurs ne sont pas lisible par d'autres nœuds externes au réseau. Comme mentionné précédemment ce service est garanti à l'aide de la cryptographie symétrique car seuls les capteurs légitimes ont les clefs valides.
- **L'authentification :** Ce service assure que seuls les capteurs légitimeset station de base légitime peuvent participer aux tâches du réseau de capteurs. Ce service est partiellement garanti à l'aide des clefs pré-partagées car seuls les nœuds et la station de base légitime peuvent s'authentifié à l'aide de ces clefs partagées.
- **L'intégrité :**Ce service est garanti à l'aide de la cryptographie car puisque les messages sont illisibles un intrus ne peut pas modifier le paquet parce qu'il ne reconnait pas les clés et l'algorithme utilisé dans le cryptage.
- **Contrôle d'accès :** Ce service est garanti car seul un capteur partageant la même clef avec la station de base peut faire partie du réseau.

IX.2 Les services de sécurité qui ne sont pas garantie :

- **Le non répudiation :** Un expéditeur pouvoir, par la suite, nier d'avoir envoyé un message.
- **La fraîcheur des clefs:** Notre programme ne contient pas un algorithme pour faire une mise ajour périodique desclés.

- **La sécurité de localisation** : Nous n'avons pas mis un service de La localisation (notre réseau de capteurs n'est pas capable de localiser automatiquement chaque capteur dans le réseau).

X. Les attaques arrêtées par le système

Nos procédures ou techniques permettant de résoudre des vulnérabilités ou de contrer des attaques spécifiques.

Attaques
Usurpation d'identité
Ecoute de trafic
Modification du trafic

Tableau IV.2 : Les attaques arrêtées par le système

Conclusion

Dans ce chapitre on a déployé un réseau de capteurs sans fil pour la surveillance et le control de la température dans un environnement domestique tel que les maisons et les jardins. Vu la possibilité d'écoute passive sur le réseau on a essayé d'implémenter un mécanisme sécurité permettant d'assurer la confidentialité de notre réseau, ce mécanisme basé sur la cryptographie symétrique qui se voit une bonne alternative de cryptographie vu sa faible consommation d'énergie et rapidité de cryptage. Comme vu dans les dernières sections du chapitre ce mécanisme de sécurité permet d'assurer un grand nombre de services de sécurité tels que la confidentialité, authentification et le control d'accès, mais aussi il peut arrêter plusieurs attaques telles que l'coute passive et active.

Conclusion générale

Les réseaux de capteurs sans fil sont une nouvelle technologie qui a surgi après les grands progrès technologiques concernant le développement des capteurs intelligents, des processeurs puissants et des protocoles de communication sans fil. Ce type de réseau composé de centaines ou de milliers d'éléments, a pour but la collecte de données de l'environnement, leur traitement et leur dissémination vers le monde extérieur.

L'utilisation des réseaux de capteurs sans fil (RCSF) dans des applications critiques nécessite un certain degré de sécurité afin de les protéger contre des menaces qui profitent de la vulnérabilité des nœuds pour attaquer ces réseaux.

La sécurité des RCSFs présente des défis liés aux contraintes énergétiques des nœuds et leurs capacités physiques.

De ce fait ce mémoire avait pour objectif d'apporter des solutions aux problèmes liés à la sécurité dans les réseaux de capteurs, en proposant un protocole de gestion de clefs dans un réseau de capteurs sans fil basé sur la cryptographie symétrique, la solution proposée utilise l'algorithmes RC4 reconnu par sa vitesse et sa facilité d'utilisation pour chiffrer les données échangées entre la station de base et les nœuds capteurs

La solution proposée a été utilisée au dessue d'un système de contrôle de la température afin de prouver sa faisabilité.

Nous avons étudié quelques solution qui permettent d'offrir le service de sécurité de base pour n'importe quel système basé sur la communication.et nous montrons les limites de certaines solutions et bien sûr nous avons proposé des solutions plus adaptées à l'environnement des réseaux de capteurs.

GLOSSAIRE

A	
AES :	Advanced Encryption Standard
B	
bps :	Bit par second
D	
D.E.S	Data Encryption Standard
DOS	Disk Operating System
G	
GPS	Global Positioning System
Go	Giga octet
I	
ID	Identification
IDEA	International Diving Educators Association
IBM	International Business Machines
K	
Ko	Kilo octet
KSA	Key Schedule initialize Aleatory
L	
LED:	Light-Emitting Diode
M	
MANET	Mobile Ad hoc NETwork
MAC	Media Access Control
MD5	Message Digest 5
Micro-PKI	Micro Public Key Infrastructure
N	
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NSA	National Security Agency
O	
OSI	Open Systems Interconnection
OS	Operating System
P	
PKP	Public Key Partners
R	
RAM	Random Access Memory
RCSF	Réseaux de Capteurs Sans-Fil

GLOSSAIRE

RC4	Rivest Cipher 4
R.S.A	Rivest–Shamir–Adleman
RTS	Request To Send
S	
SHA–1	Secure Hash Algorithm–1
T	
TLS	Transport Layer Security
U	
WEP	Wired Equivalent Protocol
UWSN	Underwater Sensors Networks
W	
WSN	Wireless Sensor Network
WI–FI	Wireless Fidelity
WPA	Wi–Fi Protected Access

- [1]Messai Mohamed Lamine, « Sécurité dans les Réseaux de Capteurs Sans-Fil », Université de Bejaia, 2008.
- [2] I. F. Akyildiz, W. Su, Y. Sankara Subramaniam, et E. l. Cayirci. « A survey on sensor Networks ». IEEE Communications Magazine, August 2002.
- [3] Equipe de Get 2005 Capt'Ad-hoc. «Sensor networks: State of the art». Technical Report, Telecom Paris, Mars 2006.
- [4] FARES Abdelfatah, Rapport en Master Informatique, « Développement d'une bibliothèque de capteurs », 2008.
- [5] Ramdani Mohamed, Mémoire de magister Spécialité : Informatique Répartie et Mobile, « Problèmes de sécurité dans les réseaux de capteurs avec prise en charge de l'énergie », Université De Saad Dahlab De Blida, Novembre 2013.
- [6] Yacine Challal « Réseaux de Capteurs Sans Fils » Article : Systèmes Intelligents pour le Transport, 2008.
- [7] Maarouf Samia Ouadah Souhila, Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique « Implémentation et évaluation des schémas de routage sur une plateforme réelle de réseaux de capteurs sans fil », 2014.
- [8] Mo Li et Yunhao Li, «Underground structure monitoring with wireless sensor net-works», (2007).
- [9]Ian F Akyildiz, Tommaso Melodia, et Kaushik R Chowdhury, «A survey on wireless multimedia sensor networks », Article Academy: Computer networks, 2007.
- [10] Hadjila Mourad, Thèse pour l'obtention du diplôme de Doctorat « PROTOCOLES DE ROUTAGE ECONOMES EN ENERGIE POUR LES RESEAUX DE CAPATEURS SANS FIL », 2014.
- [11] Sihem Souiki, « Les réseaux de capteurs sans fil sous-marins : Applications et Défis », Laboratoire STIC Université de Tlemcen, Algérie.
- [12] E. Munivelet G. M. Ajit, « Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks », conférence international sur la communication sans fil et capteur informatique, 2010.
- [13] Sofiane Moad, « Optimisation de la consommation d'énergie dans les réseaux de capteurs sans fil » Université : IFSIC-Rennes 1, 2008.

- [14]Kabou Salaheddine, « Etat de l'art sur les réseaux de capteurs sans fil», Université de Béchar, Juin 2010.
- [15] Yaser Yousef, « Routage pour la gestion de l'énergie dans les réseaux de capteurs sans », 2010.
- [16] R.kacimi, «Techniques de conservation d'énergie pour les réseaux de capteurssans », 2009.
- [17] David Martins, Hervé Guyennet, « Etat de l'art Sécurité dans les réseaux de capteurs sans fil », 2008.
- [18] Boubiche Djallel Eddine, «Une approche Inter-Couches (cross-layer) pour la Sécurité dans les R.C.S.F», Université de Batna.
- [19] Samir Athmani, «Protocole de sécurité pour les réseaux de capteur sans fil », Université de Batna, 2010.
- [20] Naourez Hadjtaieb, «Sécurité des réseaux de capteurs sans fil par le protocole TNT : Amélioration et application », Université de Sfax, 2013.
- [21] LABRAOUI Nabila, «La Sécurité Dans Les Réseaux Sans Fil Ad HOC», Université de Tlemcen, 2012.
- [22] Lyes Khelladi, Nadjib Badache, «Security in mobile wireless sensor networks: a roadmap», article: Encyclopedia of wireless and mobile communication, Université d'Alger, 2007.
- [23] Berrachedi Amel, Diarbakirli Amina, Mémoire ingénieur d'état, «Sécurisation du protocole de routage hiérarchique-LEACH-dans les réseaux de capteurs sans fil », Ecole nationale Supérieure d'Informatique (E.S.I), Oued-Smar, Alger, 2009.
- [24] W. Stallings, « Cryptography and Network Security Principles and Practices», quatrième Edition, 2005.
- [25] Ohn Paul Walters, Zhengqiang Liang, Weisong Laurent-Maknavicius, «Sécurité dans les réseaux de capteurs sans fils : Conception et implémentation », Université de Telecom Et Management Sud Paris, 2008.
- [26] Avinash Srinivasan, Joshua Teitelbaum, Huigang Liang, Jie Wuand Mihaela Cardei, «Reputation and Trust-based Systems for Ad-Hoc and Sensor Networks», Department of Computer Science and Engineering, Université de Florida Atlantic, 2003.
- [27] Bounegta Nadia, AiciNacira, «Approche Décentralisé pour la sécurité d'un sécurité Réseau de Capteurs Sans Fil (RCSF)», Université de Béchar, 2010.

- [28] Kaci Bader, « Détection d'intrusion dans les réseaux de capteurs sans fils», 2010.
- [29]Sedjelmaci Sid Ahmed Hichem, «Mise en oeuvre de mecanismes de securite bases sur les ids pour les reseaux de capteurs sans fil», Université de Tlemcen, 2012.
- [30] Matthew Pirretti, Sencun Zhu, Narayanan, Patrick McDaniel, and Mahmut Kandemir. The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. Université de Pennsylvania State University Park U.S.A.
- [31] Anthony D.Wood, John A.Stankovic, «Denial of Service in Sensor Networks»October 2002.
- [32] Xavier Perséguers, Projet de Master « La sécurité dans les réseaux de capteurs sans fil » Ecole Polytechnique Fédérale de LAUSANNE, 2005.
- [33] M.Hacini Souleyman Boumedyen, M.Inal Mohamed Taha, « implémentation d'algorithmes de Cryptographie», 2014.
- [34] Pierre-Alain Fouque, Cours « Algorithmes de chiffrement symétrique par bloc (DES et AES) ».
- [35] B.Kadri cours de Master 2 en RMST, « Infrastructure à clé publique (PKI) » université Abou Bekr Belkaid Tlemcen faculté de technologie.
- [36] Benoît DEPAIL, les cours de troisième année de la filière Informatique et Réseau « Exposé de système et nouvelles technologies réseaux », l'école Ingénieurs 2000 de l'UMLV.
- [37] Étude technique réalisée par Groupe CGI, « Cryptographie à clé publique et signature numérique Principes de fonctionnement ».
- [38] Omar Cheikhrouhou, «Sécurité des réseaux ad hoc », Université de Sfax, 4 juillet 2005,
- [39] B.Kadri, cours de Master 2 en RMST « Initiation à la cryptographie» université Abou Bekr Belkaid Tlemcen faculté de technologie.
- [40] Renaud Dumont, « Cryptographie et Sécurité informatique», Université de Belgique, 2010.
- [41] Christophe Giraud, « Attaques de crypto systèmes embarques et contre-mesures associées », Université de Paris, 2007.
- [42] Mathieu BADET, Willy BONNEAU, «Réseaux de capteurs», 2006.
- [43] BOURAI AMAR, BENTABET Abdel Hamid, « détection des feux».

- [44]Boumediene Siham, Maharrar Nadia, « Optimisation de la diffusion dans les Réseaux de capteurs », Université de Tlemcen, juin 2013.
- [45] Alexandre Marguerite, « Chiffrement symétrique », 2014, http://www.devensys.com/blog/chiffrement-symetrique
- [46] Rolland Balzon Philippe, « Principaux algorithmes de cryptage », 2002.
- [47] Alexandre Berzati, Thèse de Doctorat de l'Université de Versailles Saint-Quentin-en-Yvelines, Spécialité informatique« Analyse cryptographique des altérations d'algorithmes », 2010.
- [48] Anthony Deroche, Thierry Duhal, «Mise en œuvre d'un réseau expérimental de capteurs sans fil et application domotique», 2014
- [49] « Chiffrement par flot », 2012. http://perso.univperp.fr/christophe.negre/Enseignements/Cryptographie/Master1/slide-stream-cipher1.pdf

Résumé

Depuis quelques décennies, le besoin d'observer et de contrôler des phénomènes physiques tels que la température, la pression ou encore la luminosité est essentiel pour de nombreuses applications scientifiques et industrielles. Pour cela, les réseaux de capteurs sans fil sont des progrès technologiques réalisés pour surveiller une zone géographique et de remonter une alarme en cas de détection d'un événement redouté. Le fait que les RCSF traitent des données très souvent sensibles, opérant dans des environnements hostiles et inattendus, la notion de sécurité est considérée comme indispensable. Cependant, à cause de la limitation des ressources et la faible capacité de calcul d'un nœud capteur, le développement d'un mécanisme garantissant une sécurité pose de vrais défis de conception.

Dans ce mémoire, nous avons développé une application de surveillance de température dans l'environnement à base d'un réseau de capteurs sans fil. Et nous avons essayé de proposer un mécanisme de sécurité dédié à ce réseau.

Mots clé : Réseaux de capteurs sans fil, sécurité, système de gestion de clef, RC4, RSA, NesC, tinyos, protocoles de sécurité des RCSF.

ملخص

في العقود الأخيرة، الحاجة إلى رصد ومراقبة الظواهر الفيزيائية مثل درجة الحرارة أو الضغط وحتى الرطوبة امرا بالغا في الاهمية للعديد من التطبيقات العلمية والصناعية. لأجل ذلك تكنلوجيا شبكات الاستشعار اللاسلكية في تطور مستمر لتحقيق مراقبة شاملة لمناطق والإنذار عند الكشف عن حدث معين.

في كثير من الأحيان تكون شبكات الاستشعار اللاسلكية موزعة في مناطق معزولة وخطيرة وتقوم بمعالجة معلومات حساسة. لذلك يعد مفهوم أمن هذه الشبكات ضروريا لكن وضع آلية تضمن الأمن يعد تحديا حقيقيا وذلك بسبب محدودية الموارد وضعف قدرة حوسبة العقدة استشعارية.

في هذه الأطروحة، قمنا بتطوير تطبيق لمراقبة درجة الحرارة البيئة بواسطة شبكة استشعار لاسلكية. وحاولنا أن نوفر آلية أمنية مخصصة لهذه الشبكة.

كلمات مفتاحية: شبكات أجهزة الاستشعار اللاسلكية، والأمن، RC4، RSA، NESC، TinyOS, البروتوكولات الأمنية شبكات أجهزة الاستشعار اللاسلكية.

Abstract

In recent decades, the need to monitor and control physical phenomena such as temperature, pressure or the brightness is essential for many scientific and industrial applications. For this, wireless sensor networks are the best tool to monitor a geographical area and reassembling an alarm upon detection of a dreaded event. The fact that the WSN dealing with often sensitive data, operating in hostile and unexpected environments makes the aspect of security primordial before any WSN deployment. However, due to the limit of resources and low computing capacity of sensors, the development of a security mechanism guaranteeing all security services poses real design challenges.

In this work, we developed a temperature monitoring application using WSN, in which we have tried to implement a security mechanism based on symmetric cryptography to guaranty security and stop most known attacks.

Key words: Networks of wireless sensors, security, key management system, RC4, RSA, NESC, TinyOS, WSN security protocols.