Table des matières

Liste des figures

Liste des abréviations

MEMS	Minuscules Systèmes Micro-Electromécaniques
RCSFs	Réseaux de Capteurs Sans Fil
MANets	Mobile Ad hoc Networks
DARPA	Defense Advanced Research Project Agency
STAR	Système Télé-Assistance Réparti
TLF	Time Link Failure
TWC	Time Without Change
SPIN	Sensor Protocols for Information via Negotiation
DD	Direct Difusion
GPS	Global Positioning System
GAF	Geographic Adaptive Fidelity
GEAR	Geographic and Energy Aware Routing
RCMSF	Réseaux de Capteurs Multimédia Sans Fil
IDS	Systèmes de Détection d'Intrusion
DoS	Deni de Service
FDI	Fault Detection and Isolation
FTC	Fault Tolerant Control
RNG	Relative Neighborhood Graph
GG	Gabriel Graph
DT	Delaunay Triangulation
RLE	Run Length Encoding
LZW	Lempel-Ziv-Welch
TDC	Transformation Discrète en Cosinus
FoV	Field of View
WISN	Wireless Image Sensors Network
CSMA	Carrier Sense Multiple Access
MPR	MultipathRouting

Introduction générale

Contexte du travail

Ce travail entre dans le contexte d'une thèse de Doctorat en informatique. Cette thèse est réalisée au sein du laboratoire de recherche en informatique industrielle et réseau (LRIIR) de l'université d'Oran dans le cadre de sa coopération avec le laboratoire d'informatique de l'université de Pau, France (LIUPPA projet de coopération Tassili).

Aperçu sur le travail

Les progrès rapides des systèmes micro-électro-mécaniques (MEMS) ont rendu possible l'existence de minuscules nœuds de capteurs dotés de capacités de détection, de communication et de traitement. Lors du déploiement dans une zone, ces nœuds sont capables de former un réseau sans fil à multi-sauts. La disponibilité du matériel à faible coût a permis le développement de réseaux de capteurs multimédia sans fil (RCMSFs). Le réseau de capteur image sans fil (RCISF) est une catégorie de réseaux de capteurs multimédia sans fil où les nœuds de capteurs sont équipés d'un appareil photo numérique (caméra) qui est capable de fournir des images à basse résolution.

La consommation d'´energie est un problème fondamental lorsque les capteurs sont déployés dans des zones inaccessibles ou encore déployés sur de grands espaces, c'est-à dire lorsqu'il est difficile voire impossible de remplacer les batteries des nœuds quand elles arrivent à épuisement. De ce fait, la durée de vie limitée des nœuds va avoir un impact sur la durée de vie du réseau tout entier.

Lorsque le déploiement est aléatoire, il peut y avoir une grande redondance entre les nœuds et une approche couramment utilisée est de définir un sous-ensemble de nœuds qui seront actifs pendant que d'autres seront inactifs. Le résultat est un ordonnancement de l'activité des nœuds qui maintient la couverture et la connectivité de la zone à surveiller. Des travaux récents ont étendu la problématique de la surveillance en intégrant des données de type multimédias et ce, grâce au développement technologique dans le domaine des capteurs et Wasmotes.

Congduc Pham et al. du LIUPPA, France Laboratoire présente une approche pour ordonnancer de manière adaptative l'activité des nœuds vidéo en mode capture image, en fonction de la couverture, des considérations énergétiques et des objectifs de l'application.

Disposer de plusieurs niveaux d'activité est aussi nécessaire car les applications de surveillance comme la détection d'intrusion doivent pouvoir être opérationnelles sur le long terme puisque personne ne sait quand une intrusion se produira.

Problématique de la thèse

Lors de la détection d'intrusion, des alertes sont envoyées. L'envoie de ces alertes se fait sous forme de diffusion générale pour tous les nœuds du réseau.

Ceci créée une inondation du réseau par des messages d'alertes avec possibilité d'implosion. Ce phénomène est très néfaste pour le réseau de capteurs image sans fil car il épuise rapidement l'énergie du réseau or que ce dernier est destiné à assurer des objectifs très critiques de la surveillance.

Contributions

Dans le but de contribuer sur le contrôle coopératif des réseaux de capteurs sans fil pour les applications critiques de surveillance, notre objectif dans cette thèse est d'étendre l'application de surveillance à base de réseau de capteurs d'image sans fil du laboratoire LIUPPA, avec une contribution pour la gestion de la diffusion d'alerte en se basant sur le principe de la redondance. L'idée principale de notre algorithme est de réduire les inondations du message d'alerte, afin de préserver la consommation d'énergie.

Organisation du manuscrit

Le premier chapitre est consacré à un état de l'art sur les réseaux de capteurs sans fil. Il présente les caractéristiques physiques de ce type de réseau ; leurs applications ; les spécificités du routage dans ce type de réseau ; la contrainte énergétique ; la sécurité contre des attaques; et les solutions envisageables dans ce cadre. La dernière section de ce chapitre est dédiée au réseau de capteur image sans fil et leurs introductions dans le domaine de la surveillance.

Le deuxième chapitre présente l'importance de la détection d'intrusion pour assurer une bonne surveillance. Ce chapitre étale les différentes terminologies dans le domaine de la surveillance du réseau lui même; les différents type de système de détection d'intrusion (IDS), les techniques de la cryptographie, et les enjeux de la sécurité dans les réseaux de capteurs sans fil y sont présentés.

Le troisième chapitre est consacré à exposer les différentes techniques de la redondance exploité dans le domaine des réseaux de capteurs sans fil. Un état de l'art est donné pour explorer les différents travaux réalisés dans ce domaine. Une section de chapitre est consacrée à l'exploitation de la redondance dans le domaine de réseaux de capteurs image sans fil. Elle étale les techniques de prétraitement, filtrage et compression sur les images.

Le quatrième chapitre présente nos contributions dans le domaine de la gestion de la diffusion d'alertes suite aux détections d'intrusion dans le domaine de la surveillance par réseau de capteurs image sans fil. Nos algorithmes proposés ont un impact sur l'optimisation d'envoie de paquet d'alerte en exploitant la propriété champs de vue du capteur image (Field of View : FoV) combinée à la redondance des nœuds capteurs. Cette technique a un impact significatif sur la gestion de l'énergie sur ce type de réseau de capteur. Ceci est montré par les différentes expérimentations réalisées à l'aide du simulateur Omnet++/Castalia.

Une conclusion générale est donnée pour synthétiser nos travaux, et proposer des perspectives de recherche.

Chapitre 1 : Etat de l'art sur les réseaux de capteurs sans fil.

1.1 Introduction

Les récentes avancées technologiques dans le domaine des communications sans fil ont permis le développement à faible coût de minuscules systèmes micro-électromécaniques (MEMS), appelés capteurs, capables de détecter, mesurer et rapporter des données physiques liées à leur environnement. Ces capteurs sont caractérisés par de faibles ressources (énergie, capacité de calcul, mémoire, etc.) et de faible consommation énergétique. Ils ont trois fonctions principales : la capture de données reliées à leur environnement physique (température, pression, vibration, lumière, mouvement, etc.) ; le traitement des données collectées, et la transmission de ces données à un centre de traitement nommé « sink ». Selon leur structure électronique, ils peuvent détecter des signaux mécaniques, acoustiques, électriques, photoniques, électromagnétiques, vibratoires, etc. Les réseaux de capteurs sans fil (RCSFs) sont des réseaux sans infrastructure, généralement destinés à être déployés en grand nombre, pour couvrir des surfaces plus ou moins larges. Leurs applications potentielles diversifiées, dans les domaines militaire, industriel et domestique, sont la source de l'intérêt qu'ils suscitent, aussi bien dans la communauté scientifique qu'industrielle.

Par conséquent, les possibilités en termes d'application sont très vastes. Elles s'étendent du domaine médical au domaine militaire, en passant par celui du bâtiment et du contrôle industriel. Néanmoins, il est impossible à l'heure actuelle de concevoir un réseau de capteurs générique qui soit capable de répondre à toutes les exigences de toutes les applications de manière efficace. En effet, les contraintes de conception (alimentation électrique, niveau de précision, coût unitaire par nœud, dimensions d'un noeud ...) sont la plupart du temps fonction de l'application visée. Pour cette raison, les solutions envisagées pour répondre aux exigences de l'application sont conditionnées par ces contraintes. Elles peuvent donc être plus ou moins efficaces selon l'application.

En d'autres termes, l'application ou le type d'application reste donc l'élément le plus influent pour la conception des protocoles du réseau. L'objet de ce premier chapitre est de réaliser un état de l'art général sur les réseaux de capteurs sans fil.

1.2. Evolution des RCSFs

Les nouveaux systèmes d'acquisition basés sur des réseaux de capteurs sans fil sont le fruit du développement conjoint des technologies sans fil de ces dernières années et de la miniaturisation des architectures électroniques. Avant cette évolution, l'acheminement des informations relevées par un capteur était réalisé via un support de transmission filaire, encombrant et coûteux, et son installation devait justifier de perspectives de profits économiques importants. A présent, chaque capteur également appelé nœud est doté d'un circuit radio lui permettant de transmettre et de recevoir des informations via un médium sans fil.

Un réseau est un ensemble de terminaux interconnectés par un moyen de communication. Selon leur méthode de constitution et d'administration on distingue les réseaux statiques, les réseaux ad hoc et les MANets (Mobile Ad hoc Networks) [1].

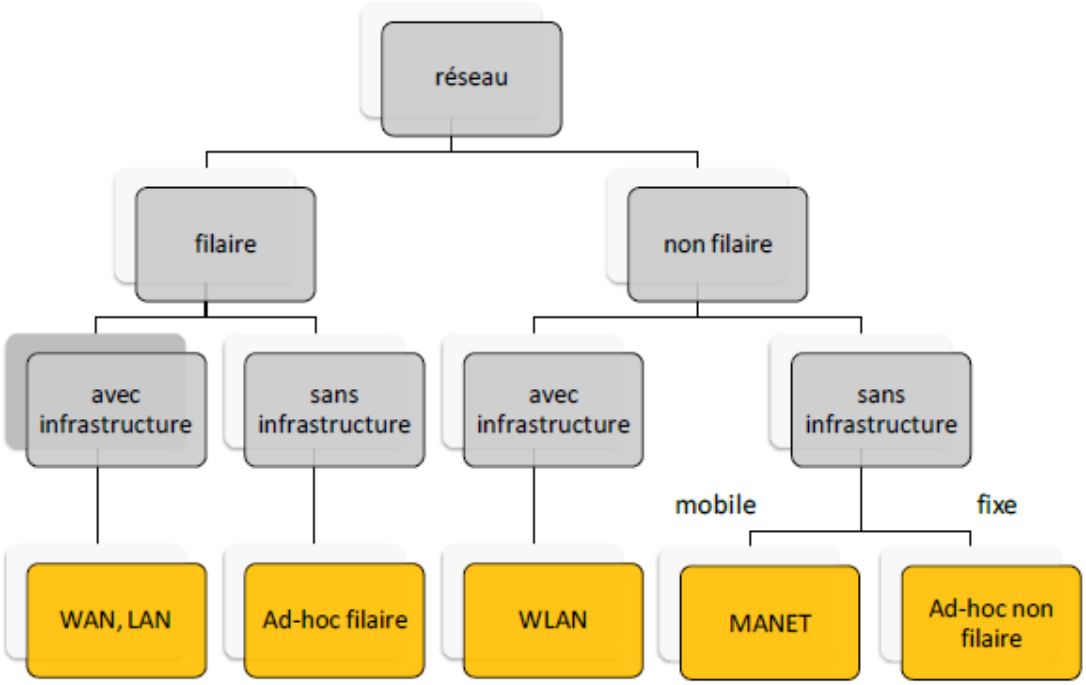

Figure 1.1 Classification des réseaux

Les réseaux statiques sont des réseaux qui ont vocation à être utilisés par des groupes humains dont la composition est connue à l'avance et évolue relativement peu rapidement, comme par exemple les collaborateurs d'une entreprise ou les membres d'un laboratoire de recherche. Ces réseaux, le plus souvent filaires, sont mis en œuvre grâce à du matériel permettant de créer une infrastructure, comme des commutateurs, des routeurs ou dans certains cas des points d'accès sans fil.

Les réseaux ad hoc sont des réseaux souvent temporaires constitués le plus souvent lors d'un rassemblement, par exemple une conférence. Ils utilisent la plupart du temps une infrastructure proche de celle fournie par un réseau statique et à laquelle les terminaux accèdent via des points d'accès sans fil. Ils peuvent aussi se former, et c'est en cela qu'ils se différencient, sans aucune infrastructure, en utilisant uniquement des connexions reliant les terminaux entre eux.

Les MANets sont le type de réseau le plus instable. Ils ne comportent pas d'infrastructure et les terminaux peuvent apparaître ou disparaître à tout moment suivant leurs capacités à communiquer ou leurs intérêts applicatifs ; ces changements peuvent donc être choisis ou subis. Par exemple, un réseau MANet peut-être constitué par les personnes à l'intérieur d'un commerce à un instant donné. Les terminaux utilisés sont très hétérogènes : ordinateurs portables, assistants personnels, téléphones ou même capteurs [2].

Les réseaux mobiles ad-hoc peuvent être caractérisés par:

- Une topologie dynamique due principalement à la mobilité des nœuds, aux changements dans l'environnement radio,
- Une bande passante limitée qui influe considérablement sur le volume des informations échangées,

- Un taux d'erreur élevé du à l'utilisation d'un environnement radio.
- Éventuellement des contraintes énergétiques fortes dues aux alimentations embarquées dans les matériels, souvent petites.

1.3. Architectures de RCSF

Un nœud capteur est composé de plusieurs éléments ou modules correspondant chacun à une tâche particulière d'acquisition, de traitement, ou de transmission de données. Il comprend également une source d'énergie.

- *Unité d'acquisition des données* : le principe de fonctionnement des détecteurs est souvent le même ; il s'agit de répondre à une variation des conditions d'environnement par une variation de certaines caractéristiques électriques (par exemple pour une thermistance, une variation de température entraîne une variation de la résistance). Les variations de tension sont ensuite converties par un convertisseur Analogique-Numérique afin de pouvoir être traitées par l'unité de traitement. On trouve aussi des structures plus complexes pour détecter d'autres phénomènes, les MEMS (pour Microelectromechanical system), qui sont utilisés pour une grande variété de phénomènes physiques (accélération, concentration chimique...).

Figure 1.2 Unité d'acquisition des données d'un capteur

- *Unité de traitement des données* : les microcontrôleurs utilisés dans le cadre de réseaux de capteurs sont à faible consommation d'énergie. Leurs fréquences sont assez faibles, moins de 10 MHz pour une consommation de l'ordre de 1 mW. Une autre caractéristique est la taille de leur mémoire qui est de l'ordre de 10 Ko de RAM pour les données et de 10 Ko de ROM pour les programmes. Cette mémoire consomme la majeure partie de l'énergie allouée au microcontrôleur, c'est pourquoi on lui adjoint souvent de la mémoire flash moins coûteuse en énergie. Outre le traitement des données, le microcontrôleur commande également toutes les autres unités notamment le système de transmission.

Figure 1.3 Unité de traitement des données d'un capteur

- *Unité de transmission de données* : les composants utilisés pour réaliser la transmission sont des composants classiques. Ainsi on retrouve les mêmes problèmes que dans tous les réseaux sans-fil : la quantité d'énergie nécessaire à la transmission augmente avec la distance. Pour les réseaux sans-fil classiques (LAN, GSM) la consommation d'énergie est de l'ordre de plusieurs centaines de milliwatts, et on se repose sur une infrastructure alors que pour les réseaux de capteurs, le système de transmission consomme environ 20 mW et possède une portée de quelques dizaines de mètres. Pour augmenter ces distances tout en préservant l'énergie, le réseau utilise un routage multi-sauts.

Figure 1.4 Unité de transmission des données d'un capteur

- *Source d'énergie* : pour des réseaux de capteurs sans fil autonomes, l'alimentation est une composante cruciale. Il y a essentiellement deux aspects : premièrement, stocker l'énergie et la fournir sous la forme requise ; deuxièmement, tenter de reconstituer l'énergie consommée par un réapprovisionnement grâce à une source externe au nœud-capteur telles les cellules solaires. Le stockage de l'énergie se fait traditionnellement en utilisant ses piles, à titre indicatif, ce sera souvent une pile AA normale d'environ 2.2-2.5 Ah fonctionnant à 1.5 V.

Figure 1.5 Un nœud capteur complet

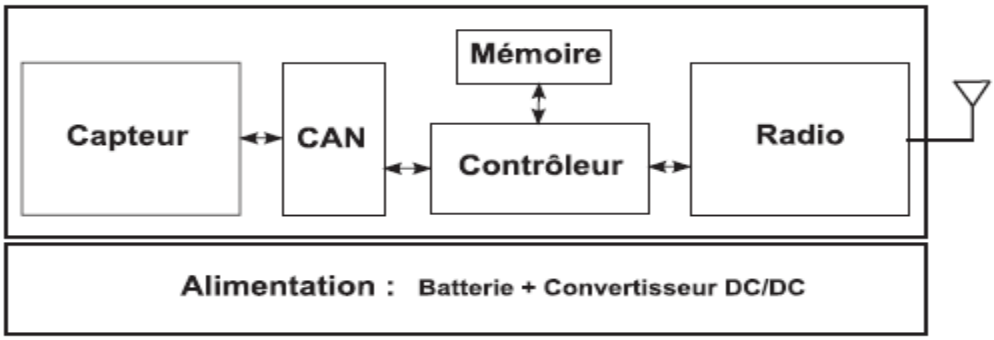

Figure 1.6 Schéma d'un nœud capteur

Un réseau de capteurs est généralement constitué de nombreux nœuds répartis dans une zone (sensor field). Ces nœuds sont reliés à une ou plusieurs passerelles (Sink) qui permettent l'interconnexion avec d'autres réseaux (Internet, satellite . . .) et la récupération des données [3].

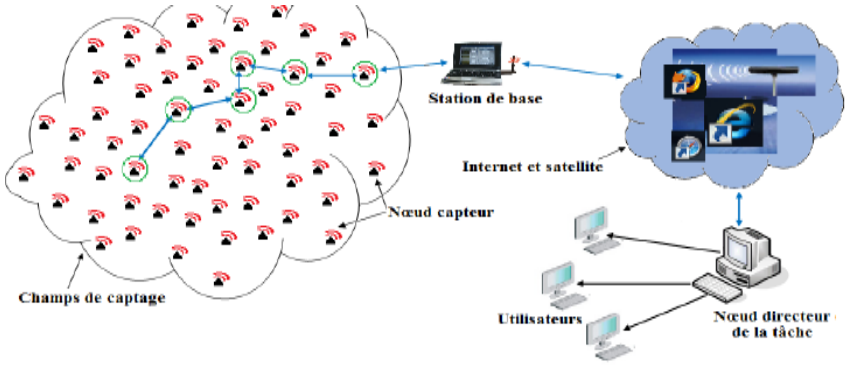

Figure 1.7 Réseau de capteurs sans fil

En raison de leur forte densité dans la zone à observer, il faut que les nœuds-capteurs soient capables d'adapter leur fonctionnement afin de maintenir la topologie souhaitée.
On distingue généralement trois phases dans la mise en place et l'évolution d'un réseau:

- Déploiement : Les nœuds sont soit répartis de manière prédéfinie soit de manière aléatoire (lancés en masse depuis un avion). Il faut alors que ceux-ci s'organisent de manière autonome.
- Post-Déploiement - Exploitation : Durant la phase d'exploitation, la topologie du réseau peut être soumise à des changements dus à des modifications de la position des nœuds ou bien à des pannes.
- Redéploiement : L'ajout de nouveaux capteurs dans un réseau existant implique aussi une remise à jour de la topologie.

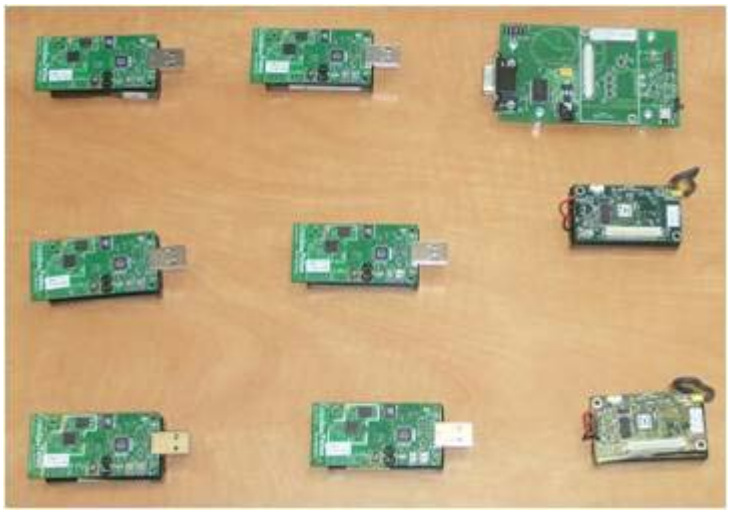

Figure 1.8 Modèles de nœuds capteur vue réelle

La pile de protocoles utilisée par le puits (Sink) ainsi que par tous les nœuds-capteurs est donnée dans la figure 1.5. Cette pile de protocoles combine routage et gestion d'énergie et intègre les données avec les protocoles réseau.

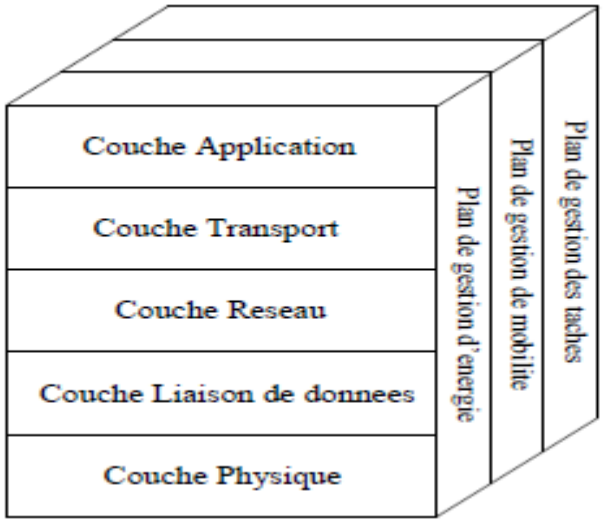

Figure 1.9 La pile protocolaire

Elle communique de manière efficace (en terme d'énergie) à travers le support sans fil et favorise les efforts de coopération entre les nœuds-capteurs. La pile de protocoles comprend une couche application, une couche transport, une couche réseau, une couche liaison de données, une couche physique, un plan de gestion d'énergie, un plan de gestion de mobilité et un plan de gestion des tâches. Selon les tâches de détection, différents types de logiciels d'application peuvent être construits et utilisés dans la couche application.

La couche transport contribue au maintien du flux de données si l'application du réseau

de capteurs l'exige. La couche réseau s'occupe de l'acheminement des données fournies par la couche transport. Comme l'environnement est sujet au bruit et que les nœuds capteurs peuvent être mobiles, le protocole MAC doit tenir compte de la consommation d'énergie et doit être en mesure de réduire les collisions entre les nœuds voisins lors d'une diffusion par exemple. La couche physique répond aux besoins d'une modulation simple mais robuste, et de techniques de transmission et de réception [4].

Figure 1.10 Déploiement du réseau de capteur sans fil

En outre, les plans de gestion d'énergie, de mobilité et des tâches surveillent et gèrent la consommation d'énergie, les mouvements, et la répartition des tâches entre les nœuds capteurs. Ces plans aident les nœuds-capteurs à coordonner les tâches de détection et à réduire l'ensemble de la consommation d'énergie.

1.4. Applications des RCSFs

Les applications militaires:
Il faut reconnaître que les applications militaires ont souvent été au centre de nombreux développements technologiques. En effet, pour de nombreuses technologies comme ARPANET devenue INTERNET, les réseaux ad hoc et aujourd'hui les réseaux de capteurs, le domaine militaire a été le point de départ. Les réseaux de capteurs ont été initiés en 1993 dans le cadre du projet WINS de la DARPA (Defense Advanced Research Project Agency). Dans le domaine militaire, cette technologie peut impulser de nouvelles stratégies de communication ou encore servir à détecter des dispositifs nucléaires et les dépister, à surveiller les activités d'ennemies, ou à analyser un endroit stratégique et difficile d'accès avant un déploiement de troupes.

Figure 1.11 Capteurs dans les applications militaires

Les applications médicales:

Le domaine médical constitue un intérêt de plus en plus grandissant pour les nouvelles technologies. On utilise de plus en plus de matériels hautement technologiques en médecine. L'apport de ces techniques permet non seulement de garder le patient à son domicile mais aussi de lui éviter le traumatisme de l'hospitalisation. Il faut ajouter qu'à l'aide de capteurs, les comportements anormaux des personnes dépendantes tels que des chutes, des chocs ou des cris peuvent être détectés, ce qui facilitera les interventions immédiates. Dans le même sens, le projet STAR (Système Télé-Assistance Réparti) [5] de l'équipe LIMOS de Clermont-Ferrand en collaboration avec le service de cardiologie du CHU de la même ville propose une plateforme de télésurveillance novatrice permettant de suivre en continu et à distance les personnes ayant des troubles du rythme cardiaque.

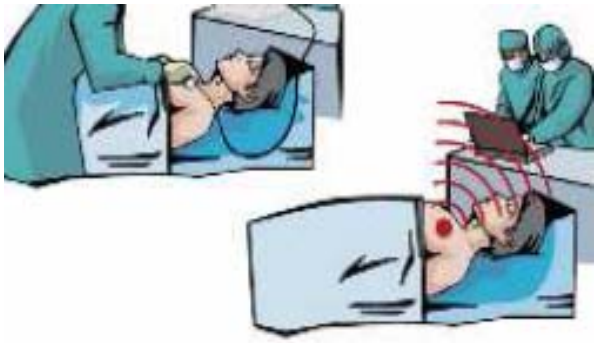

Figure 1.12 Capteurs dans le domaine médical

Les applications liées à la sécurité des infrastructures:

Après l'effondrement du pont de Minneapolis dans le Minnesota (USA) en Août 2007, de nombreux budgets ont été déployés pour la recherche sur la surveillance de ponts à l'aide de capteurs. En effet, après cet effondrement une grande polémique s'est développée autour de sa cause. De ce fait, à l'aide de capteurs, il sera possible de prévoir, voire anticiper la détérioration des ponts dans un univers où le paysage urbain connaît déjà une utilisation avancée des "systèmes de transport intelligents" [6]. Par exemple, le projet de transport intelligent *GuidestarTMS* à Minneapolis a permis une réduction du nombre d'accidents. Les chercheurs s'intéressent également à la surveillance des bâtiments à l'aide de capteurs.

Figure 1.13 Capteurs dans les infrastructures

La domotique:

Nous imaginons très bien les maisons du futur où une véritable interaction avec des capteurs embarqués permettra de contrôler localement ou à distance des appareils domestiques. Ces smart home, c'est à dire ces maisons intelligentes, vont faciliter les activités domestiques quotidienne telles que l'automatisation de l'activation/l'extinction de la lumière qui existe déjà dans certains garages ou encore la mise en marche automatique de la télévision, la climatisation ou le chauffage lorsqu'il y a présence dans le salon [7].

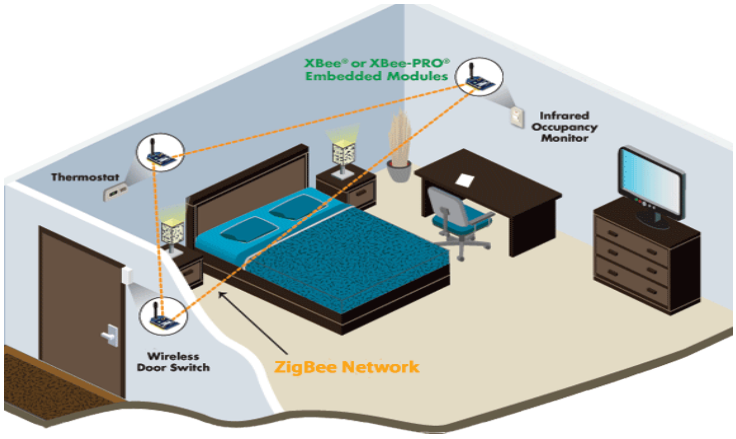

Figure 1.14 Capteurs dans la domotique

Les applications environnementales:

Au cœur des débats, l'environnement constitue un axe important pour le devenir des Hommes. L'observer, le comprendre, le connaître a toujours été un but fondamental pour les Hommes et pour la Science. De ce fait, utiliser le progrès technique pour conduire ces différentes actions constitue un atout sans précédent. C'est pour cette raison que les réseaux de capteurs constituent un nouvel outil pour les applications environnementales.

Figure 1.15 Capteurs pour l'environnement, sécurité routière

La mise en place d'un réseau de capteurs permettra non seulement d'observer notre environnement mais aussi d'anticiper sur d'éventuelles catastrophes naturelles, ce qui constitue une évolution dans un monde qui se voit alerter par la situation de son environnement. La taille des capteurs et leurs autonomie leurs donnent la capacité d'être déployés en grand nombre et dans tout environnement, comme ceux qui sont considérés

comme sensibles et hostiles pour l'homme [8].

Figure 1.16 Capteurs pour l'environnement, feux de forêts

D'autre part, cette technologie dans le cadre d'une étude environnementale fait appel à plusieurs compétences, ce qui permettra de réunir plusieurs unités de recherches provenant de domaines différents.

1.5. Couverture dans les RCSFs

Le processus de découverte de voisinage est généralement réalisé par un protocole hello. Ce dernier permet de construire et de maintenir des tables de voisinage grâce à un échange périodique de messages contenant nécessairement l'identifiant du nœud émetteur et éventuellement sa position. Ce protocole dépend de plusieurs paramètres, par exemple la fréquence d'émission des paquets, la puissance de transmission, etc. Certains protocoles, par exemple les couches MAC pour les réseaux de capteurs, peuvent utiliser des mécanismes un peu plus complexes comme l'ordonnancement des activités et l'introduction de périodes de sommeil. L'idée est de mettre en veille périodiquement les nœuds afin d'économiser leur énergie. Ces mécanismes introduisent plusieurs nouveaux paramètres, comme la durée des périodes d'activité et de sommeil, qui peuvent avoir un impact considérable sur les performances et l'efficacité des protocoles hello.

En effet, ces paramètres peuvent avoir une influence non négligeable sur la durée du processus de découverte de voisinage, c'est à dire le temps nécessaire avant que chaque nœud ne découvre tous les autres nœuds présents dans son voisinage.

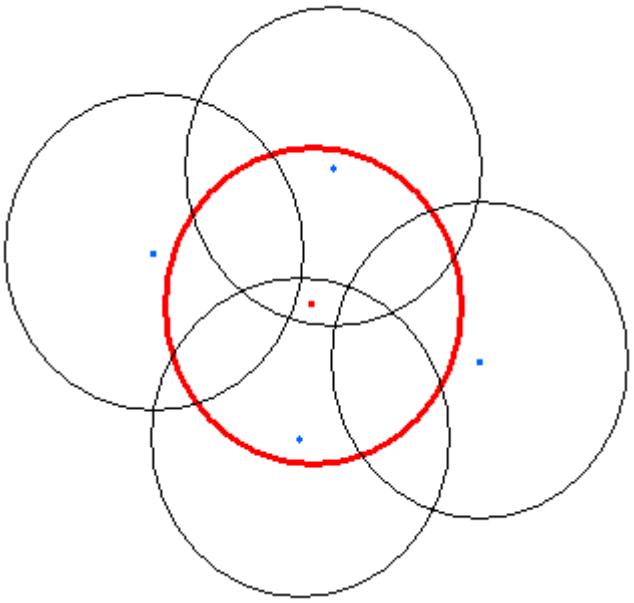

Figure 1.17 Couverture dans un réseau de capteur sans fil

La consommation d'énergie peut également constituer une contrainte forte lors de la conception d'un protocole hello, notamment pour les réseaux de capteurs et les dispositifs utilisés pour enregistrer les contacts entre les personnes. De plus, la couche physique peut également avoir un impact important sur le processus de découverte de voisinage, particulièrement sur la probabilité de découverte des nœuds. En effet, dans les environnements réels, les liens radios sont peu fiables où les interférences ainsi que les phénomènes liés à la propagation peuvent avoir un impact considérable sur les performances des protocoles hello. Toutes ces problématiques doivent donc être considérées lors de la conception d'un protocole de découverte de voisinage. En effet, un dimensionnement mal adapté de ce protocole pourrait influer négativement sur les performances des protocoles de haut niveau.

Une famille de protocoles hello [9] est proposée par la communauté scientifique utilisant des transmissions aléatoires afin de découvrir les voisins à portée de communication dans un réseau ad hoc. Les nœuds sont supposés synchronisés et stationnaires, et peuvent être dans l'un des trois états suivants : écoute (L : Listen), transmission (T : Transmission) et hibernation (S : Sleep). Lors du déploiement, le protocole BL (Birthday Listening) est utilisé où les nœuds alternent entre les états S et L. L'intérêt de ce protocole est de minimiser la consommation d'énergie lors de la phase initiale du déploiement des nœuds.

Une fois que les nœuds sont déployés, le protocole BLT (Birthday Listen and Transmit) est utilisé où les nœuds alternent entre les trois états possibles suivant une certaine probabilité p. Une étude théorique est alors réalisée afin de calculer la probabilité p optimale permettant de maximiser le nombre de liens découverts tout en minimisant la consommation d'énergie.

D'autres propositions sont faites dans ce cadre par la communauté scientifique introduisant un modèle général afin d'étudier et évaluer plusieurs types de protocoles

hello dans le contexte des réseaux ad hoc sans fil. Les nœuds sont supposés synchronisés et le temps est divisé en slots. Chaque nœud peut être dans l'un des deux états suivants : écoute ou transmission. Trois protocoles hello sont considérés : 1) le protocole RP (Random Protocol) où les nœuds émettent un paquet hello avec une probabilité p et écoutent le médium avec la probabilité inverse, 2) le protocole LP (Listen after talking Protocol) où dès qu'un nœud émet un paquet, il écoute le médium durant le slot suivant, et enfin 3) le protocole SP (Sleep Protocol) où le nœud qui reçoit un message hello, choisit un temps aléatoire, ou back off, et émet au slot suivant [10].

Grâce à des simulations, les chercheurs ne cessent de comparer ces différents protocoles et montrent l'efficacité de l'approche SP lorsque le nombre de nœuds dans le réseau est inconnu. Dans le cas contraire, l'approche LP s'avère plus performante. Cependant, le grand inconvénient de ceci est la non-prise en compte de la consommation énergétique.

Ces protocoles sont étendus aux réseaux ad hoc multifréquences, où chaque noeud peut soit émettre ou écouter sur l'une des fréquences disponibles dans le système. Des protocoles hello aléatoires et statiques sont étudiés analytiquement avec différentes stratégies d'allocation des fréquences : dynamique et statique.

D'autres chercheurs proposent un protocole MAC intégrant la découverte de voisinage en exploitant la notion d'antennes directionnelles. Ce type d'antenne permet d'augmenter la capacité du réseau en optimisant la réutilisation spatiale du médium. Chaque nœud peut être dans l'un des trois états suivants : 1) recherche de nouveaux voisins à portée de communication, 2) interrogation des nœuds voisins connus, et enfin 3) transfert de données. Ainsi, chaque nœud interroge périodiquement la liste de ses voisins afin d'adapter l'orientation de l'antenne en fonction de la nouvelle position des nœuds. Ceci permet de garantir la présence d'un lien de communication avec chacun des nœuds du voisinage.

Cette proposition est validée par simulation et grâce à une étude théorique qui montre l'efficacité de ce protocole MAC en terme de capacité. Cependant, l'inconvénient de cette étude est la nécessité de l'utilisation d'un type d'antenne bien spécifique [11].

Plus récemment, certaines études ont considéré le problème de l'optimisation des paramètres des protocoles de découverte de voisinage. Elles proposent un protocole *hello* adaptatif où chaque nœud évalue deux paramètres : le temps de coupure du lien, ou *time link failure* (TLF), et le temps sans changement, ou *time without change* (TWC). Ces deux paramètres sont évalués en surveillant les liens du voisinage, et permettent d'adapter la fréquence d'émission des messages hello en fonction de l'état du réseau : si le temps TLF est inférieur à un certain seuil, le protocole augmente la fréquence d'émission des paquets hello, alors que si le réseau est statique, et par conséquent le temps TWC est supérieur à un certain seuil, le protocole diminue la fréquence d'émission. Le calcul d'une fréquence optimale est difficile à réaliser puisque les valeurs des seuils peuvent évoluer au cours du temps.

1.6. Routage dans les RCSFs

Le routage consiste à trouver un chemin pour envoyer le message de la source à la destination. Dans le cadre des réseaux de capteurs, le routage doit être efficace en

énergie. Pour cela, il faut bien sûr être capable de trouver une route qui ne coûte pas trop d'énergie, une route pas trop longue. Mais il faut aussi être capable de trouver ou de maintenir les routes sans dépenser trop d'énergie. Les protocoles dans lesquels on maintient à jour des tables de routage à l'aide d'envois périodiques de paquets "hello" ont un coût constant non négligeable. Ce coût constant est particulièrement pénalisant puisque l'on a des trafics très sporadiques : maintenir une table de routage, pour avoir des routes très efficaces, n'est pas intéressant si l'on n'utilise que très rarement ces routes.

Les protocoles de routage spécifiques aux réseaux de capteurs doivent tenir compte du type de communications induit par l'application. Outre le fait que la quantité de données échangées est très faible par rapport aux applications de types réseaux ad hoc, notons que le trafic est particulièrement prévisible puisqu'il va des nœuds vers le puits ou du puits vers les nœuds.

Beaucoup de solutions de routage ont été proposées; néanmoins, elles peuvent être regroupées selon plusieurs classifications, selon plusieurs critères a savoir, la topologie du réseau, les opérations supportées et la destination des paquets transmis. La topologie du réseau adopté, subdivise les solutions du routage en trois (03) catégories principales: Protocoles à topologie plate, protocoles hiérarchiques, protocoles géographique (location-based) [12].

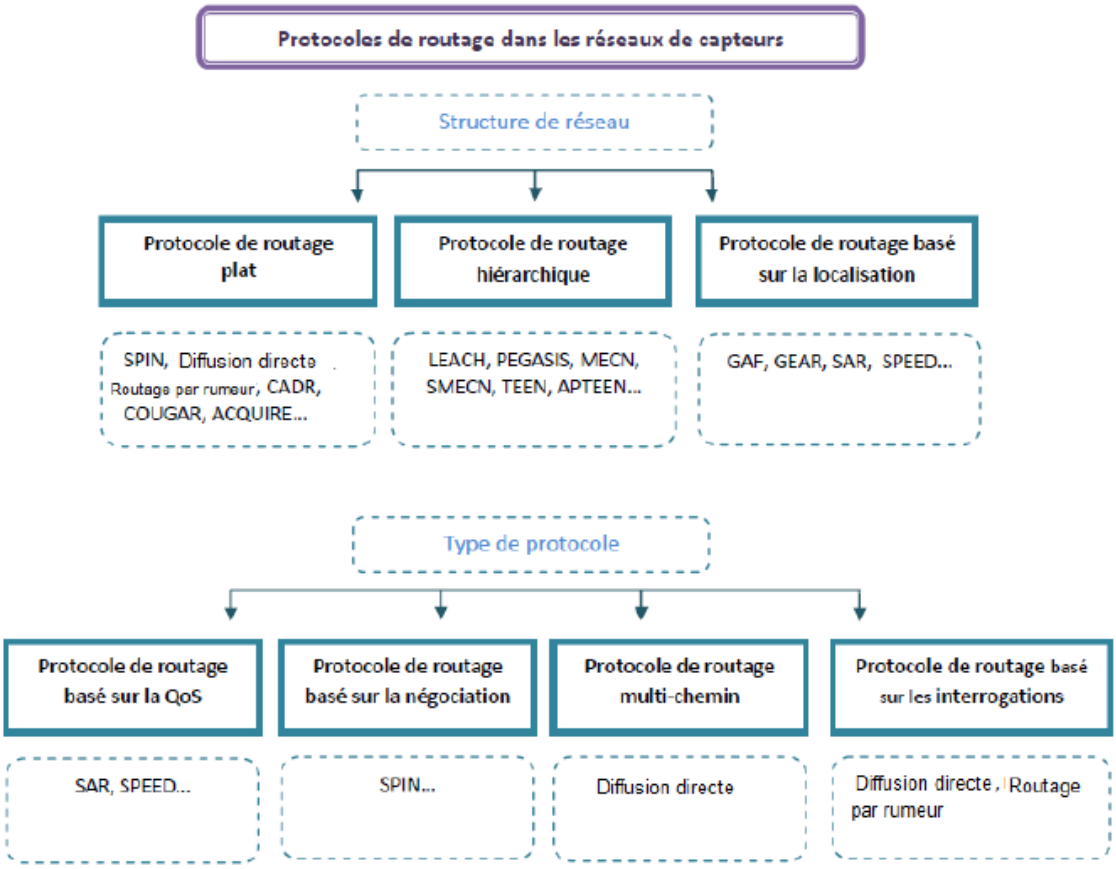

Figure 1.18 Classification des protocoles dans les RCSFs

En plus, si les opérations supportées sont prisent en charge, les solutions peuvent être classées en: basée multi-chemins (multipath-based), basée requêtes (query-based), basée négociation (negociation-based), basée sur les qualités du service (Qos-based) et basée sur la cohérence du traitement des données (coherent-based): Un traitement non cohérentde données signifie que chaque nœud agrège ses données avant la transmission, par contre, un traitement cohérent signifie que les données sont transmises vers des nœuds spécifique dits (Aggregator) pour les opérations d'agrégation. Les protocoles de routage peuvent aussi être classés comme suit :

Les protocoles à topologie plate:
Ce type de protocoles est le premier a être utiliser pour le routage sur les RCSFs; son principe est simple, c'est le puits qui envoi des requêtes vers des zones spécifiques du réseau et attend l'arrivée des réponses des nœuds vises. Deux exemples phares de cette classe de protocoles sont **SPIN** (Sensor Protocols for Information via Negotiation) et **DD** (Direct Difusion)[13].

Les protocoles géographiques:
Dans ce type de protocoles la position du nœud prime sur son adresse; pour cela, il est supposé que chaque nœud du réseau connaisse sa position et les positions de ses voisins. Le positionnement du noeud peut être obtenu en utilisant un système de géo-positionnement tel que le GPS (Global Positioning System) ou bien via des algorithmes de positionnement relatif. Le principe général consiste à obliger les nœuds, qui ne sont pas sur le chemin du routage choisi, a entrer en mode sommeil pour conserver l'énergie. Chaque nœud source de données connait la position du destinataire de ses données de cette façon une estimation de la consommation de l'énergie est réalisée au préalable pour designer le chemin le plus rentable énergétiquement. Deux solutions phares de ce type de routage, a savoir: GAF (Geographic Adaptive Fidelity) et GEAR(Geographic and Energy Aware Routing), EAGRP (An energy-aware WSN geographic routing protocol), et TBF (Trajectory-based forwarding).

Les protocoles considérant la qualité de services (QoS):
Dans cette catégorie, le protocole essaye de trouver un compromis entre la consommation de l'énergie et un ou plusieurs qualités de services lors de la livraison de données; ces qualités de services peuvent être, le délai, la bande passante, …etc. un exemple de ce type de routage est le protocole SPEED[14]. (Real Time Routing Protocol for Sensor Network) c'est un protocole géographique conçu pour les communications en temps réel sur les RCSFs. SPEED améliore le protocole géographique GEAR (Geographic and Energy Aware Routing) en prenant en compte le délai de livraison de données.

1.7. Problématique de l'énergie dans un RCSF

Les capteurs sans fils sont des éléments indépendants les uns des autres, comme leur nom l'indique. Par conséquent, ils doivent également disposer d'une alimentation autonome. Leur durée de vie est limitée par la durée de vie de leur batterie. Cette contrainte forte a une influence majeure sur l'ensemble des techniques, mises en place pour le déploiement de tels réseaux. Un effet majeur de cette limitation énergétique est la limitation maximale des transmissions par voie hertzienne, très coûteuses. Il est donc

primordial d'effectuer tant que possible le traitement de l'information localement au niveau du nœud.

L'enjeu est donc d'étendre la durée de vie du système et sa robustesse, en cas de chute de certains nœuds seulement. Les problématiques sont donc très éloignées de celles des réseaux classiques, telle la maximisation du débit. Dans les réseaux de capteur sans fils, il faut assurer une consommation répartie de l'énergie au sein du réseau. Cet énergie et consommé par les diverses fonctionnalités de réseaux qui sont donc par ordre décroissant de consommation d'énergie Radio (Communication) Protocoles (MAC, routage) CPU (calcul, agrégation) Acquisition. L'enjeu d'énergie est un capital dans les réseaux de capteur, pour augmenter l'autonomie de capteur il faut agir sur plusieurs paramètres : Sur quels paramètres est-il possible d'agir ?

L'interdépendance des paramètres est un casse-tête pour réaliser une optimisation. Si on augmente le taux de transmission alors la probabilité de collision diminue, le taux d'erreur augmente, et la consommation augmente. Si on augmente la puissance de la correction d'erreur alors le taux d'erreur diminue, la probabilité de collision augmente et la consommation augmente. Si on augmente la puissance d'émission alors le taux d'erreur diminue, la probabilité de collision augmente et la consommation augmente [15].

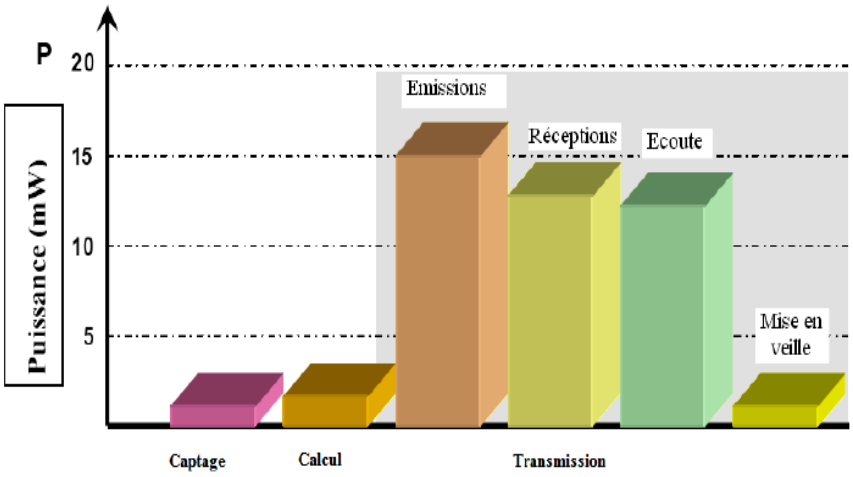

Figure 1. 19 Consommation de l'énergie du capteur

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. Evidemment, pour augmenter de manière significative la durée de vie d'un capteur sans fil, il faut s'intéresser en priorité aux composants les plus gourmands en énergie.

- L''energie consommée au moment de la mesure varie suivant la nature du capteur.

- Le coût en réception est fixe mais le coût en émission dépend de la puissance d'´emission du signal radio, de débit binaire, de la taille des données à transmettre
- L'unité de traitement des données consomme généralement moins d'´energie que l'unité de communication.

Les techniques suivantes proposent des solutions efficaces à la problématique de l'energie, on cite: EAR (Energy-aware routing), EAD (Energy-aware data-centric routing), MECN (Minimum energy communication network), EAGRP (An energyaware WSN geographic routing protocol), LEACH (Low-energy adaptive clustering hierarchy), PEGASIS (Power-efficient gathering in sensor information systems), HEED (Hybrid energy-efficient distributed clustering), MLER (Maximum lifetime energy routing), EAQSR (Energy-aware QoS routing protocol), EBAB (Energy balanced ant based routing protocol) , EEABR (Energy efficient ant based routing) .

Techniques de conservations de l'énergie :

La consommation d'´energie est un problème fondamental lorsque les capteurs sont déployés dans des zones inaccessibles ou encore déployés sur de grands espaces, c'est-à dire lorsqu'il est difficile voire impossible de remplacer les batteries des nœuds quand elles arrivent à épuisement. De ce fait, la durée de vie limitée des nœuds va avoir un impact sur la durée de vie du réseau tout entier [10].

L'unité de communication est le plus souvent constituée d'un émetteur/récepteur radio qui fournit au capteur la capacité de communiquer avec les autres au sein d'un réseau. Elle est généralement la partie la plus gourmande en énergie. Le coût en réception est fixe mais le coût en émission dépend de la puissance d'émission du signal radio, de débit binaire, de la taille des données à transmettre.

L'utilisation inutile de l'émetteur radio provient principalement des phénomènes de surécoute (Overhearing), de collisions, d'écoute passive (Idle listening), les envois infructueux et les messages de contrôle.

- La sur-écoute est la réception par un nœud d'une trame qui ne lui est pas destinée. L'énergie consommée pour la réception et le traitement des données de cette trame est perdue et sans aucun intérêt.
- Les collisions sont à la fois une source de dégradation des performances du réseau et de perte d'énergie. Les pertes de trames à cause des collisions forcent les nœuds à retransmettre le même paquet plusieurs fois et donc à rester actif pour le répéter et vérifier qu'il est bien reçu par la destination.
- L'écoute passive est l'attente d'une trame par le module radio. Cela arrive quand il a été demandé à un nœud d'être éveillé mais qu'il ne reçoit aucune trame et n'en transmet aucune non plus. Même si le nœud ne transmet pas et ne reçoit pas, le fait que son module radio soit activé et prêt pour recevoir consomme autant d'énergie que pour la réception.
- Les envois infructueux arrivent quand un nœud essaie de communiquer avec un autre nœud qui n'est plus accessible parce qu'il est en mode sommeil par exemple (ou hors de portée). Le nœud émetteur est en attente d'un acquittement,

et il retransmet donc la même trame plusieurs fois. Il consomme de l'´energie en le faisant du fait qu'il soit resté en mode transmission et en mode réception pour l'´eventuel acquittement.

De nombreuses solutions de conservation d'´energie pour les réseaux de capteurs sans fil ont été proposées, allant de la couche physique et des techniques de modulation, jusqu'à la couche application et le développement de logiciels spécialisés. Une classification des différentes approches de conservation d'énergie est présentée ainsi :

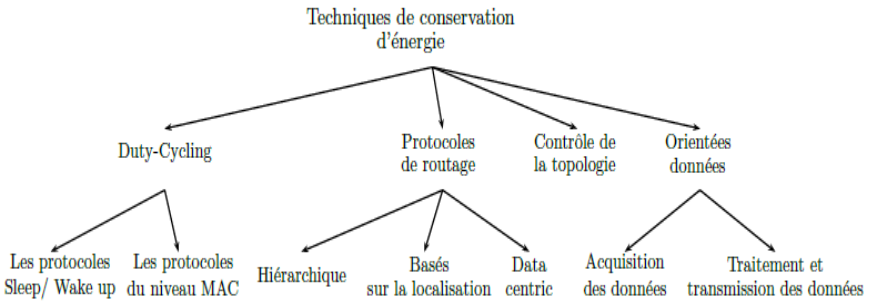

Figure 1.20 Techniques de la conservation de l'énergie

1. Réveil cyclique (Duty-cycling) : Le moyen le plus efficace pour conserver l'énergie, est d'éteindre la radio des nœuds quand la communication n'est pas nécessaire. L'idée est que les capteurs doivent éteindre leurs radios lorsqu'il n'y a pas d'activités sur le réseau et être prêt dés qu'ils ont un paquet à recevoir ou à transmettre. Ainsi, les nœuds alternent entre périodes actives et sommeil en fonction de l'activité.

2. ***Les protocoles de routage efficaces en énergie*** : Ces protocoles de routage vont déterminer les chemins jusqu'au puits en considérant dans le calcul du coût d'une route des métriques relatives à la consommation d'énergie. La solution la plus triviale est de sélectionner le chemin ayant le plus petit nombre de sauts. Mais d'autres métriques sont importantes, en particulier le niveau de fiabilité des liens radio (les erreurs de transmission entraînent des retransmissions qui coûtent cher en énergie), le débit de transmission sur les liens radios et le niveau de charge des batteries des nœuds. Le routage dans les réseaux de capteurs sans fil a été un champs d'étude et de proposition par plusieurs auteurs notamment Akkaya et Youness, Heinzelman et al, Singh et al, Xu et al., et Yu et al. Tous ces travaux convergent dans le but d'améliorer la consommation d'énergie.

3. ***Contrôle de la topologie*** : Le contrôle de la topologie consiste à éliminer du réseau les nœuds inutiles (par la mise en sommeil des nœuds redondants) et les liens inutiles (par l'ajustement de la puissance de l'émetteur radio, et donc de la portée de la communication) pour diminuer la dépense d'énergie dans le réseau. Il s'agit donc de faire une réduction de la topologie initiale du réseau tout en préservant la couverture de la zone d'intérêt et la connectivité du réseau.

4. ***Techniques de réduction des données*** : Les techniques de réduction des données dans les réseaux de capteurs sans fil visent à réduire la quantité des données à traiter et à transmettre. Les algorithmes suivants proposent des solutions à ce type de problème. On

cite F&G (Flooding and gossiping) , DD (Directed Diffusion), SPIN (Sensor protocol for information via negotiation), GBR (Gradient based routing), RR (Rumor routing), CADR (Constrained anisotropic diffusion routing), ACQUIRE (ACtive Query forwarding In sensor nEtworks).

1.8. La sécurité des RCSFs

Souvent déployés dans des environnements hostiles, les réseaux de capteurs sans fil peuvent être sujets à plusieurs types d'attaques. Dans cette section, on se propose de présenter un aperçu des attaques les plus connues au niveau de la couche routage. Pour des informations plus approfondies sur ces différentes attaques que ce soit au niveau de la couche routage ou des autres couches [16].

En effet, de nombreux chercheurs se sont particulièrement intéressés aux attaques au niveau de la couche de routage :

- Dans une attaque d'expédition sélective, l'attaquant transfère certains paquets qu'il intercepte et en supprime d'autres, engendrant ainsi une perte de donnée.
- Dans une attaque par trou de puits ("Sinkhole attack"), un attaquant tente de se faire passer pour un faux puits en se montrant très attractif aux nœuds avoisinants puis créée une topologie erronée du réseau.
- Dans une attaque Sybille, un nœud malveillant présente plusieurs identités dans le but d'attirer le plus de trafic possible et de gagner plus d'influence par rapport aux nœuds ordinaires.
- Dans une attaque d'inondation par paquets Hello, l'attaquant tente de convaincre des nœuds qu'il est dans leur voisinage même pour ceux qui sont hors de portée. Ainsi, le but de cette attaque est de faire en sorte que tous les nœuds redirigent leurs paquets vers l'attaquant.
- Dans une attaque par trou de ver, un adversaire connecte deux nœuds malveillants distants en utilisant un lien de communication directe à faible latence. Une autre forme de cette attaque est d'utiliser un nœud singulier qui relaie les paquets entre deux nœuds légitimes et distants dans le but de les convaincre qu'ils sont voisins.

1.9. Défis et perspectives de RCSF

Les acteurs industriels impliqués dans le domaine des réseaux de capteurs doivent être capables de développer rapidement des solutions fiables. Les entreprises qui conçoivent et déploient des réseaux de capteurs doivent le faire le plus rapidement possible pour faire face à la concurrence. L'enjeu économique lié à la conception des réseaux de capteurs est très important.

Cependant, concevoir un réseau de capteurs n'est pas une chose facile parce que ce sont des systèmes complexes qui combinent des caractéristiques propres aux systèmes distribués et aux systèmes embarqués. Les systèmes distribués sont difficiles à concevoir pour plusieurs raisons. Les communications entre les nœuds ne sont pas

fiables, par exemple les nœuds d'un réseau communiquent à l'aide de radios. On peut difficilement définir l'état global du système, et enfin l'exécution des processus (ici les nœuds) est asynchrone. Quant aux systèmes embarqués, ils ont des ressources (calcul, mémoire) très contraintes parce qu'ils doivent respecter des contraintes de coût. Et pour concevoir les systèmes embarqués, il faut prendre en compte les interactions fortes entre le logiciel et le matériel.

En plus des contraintes cumulées des systèmes distribués et embarqués, les applications auxquelles sont dédiés les réseaux de capteurs imposent des exigences supplémentaires de fiabilité et surtout d'économie d'énergie. A cause des difficultés d'accès aux nœuds, un problème matériel ou logiciel sera plus difficile à régler dans les réseaux de capteurs. Pour ces systèmes, publier une mise à jour encas de problème est beaucoup plus difficile que pour les logiciels destinés aux ordinateurs de bureau. Et quand bien même celle-ci serait faisable, elle aurait un coût énergétique pénalisant pour la durée de vie du réseau [17].

Aujourd'hui, de nombreux systèmes embarqués sont déjà contraints en énergie (téléphones, appareils photo), mais pour ces objets il s'agit simplement de maximiser le temps entre deux recharges de la batterie. Cette contrainte est beaucoup plus forte dans les réseaux de capteurs. Premièrement, on ne recharge pas un nœud qui n'a plus d'énergie parce ça coûterait aussi cher que de le remplacer par un nouveau nœud et deuxièmement, les clients demandent des garanties sur la durée de vie du réseau allant de 10 à 15 ans d'autonomie.

Voici, pour appuyer le besoin de méthodes de conception dédiées, quelques choix auxquels sont confrontés les concepteurs de réseaux de capteurs. Tout d'abord, il faut choisir les différents composants matériels qui constituent un nœud. Par exemple, il faut choisir un microcontrôleur basse consommation qui soit suffisamment puissant pour subvenir aux besoins de l'application.

Le choix de la radio dépendra de la fréquence d'émission choisie qui, elle-même, est fonction de la portée souhaitée. Il faut également choisir ou concevoir les logiciels. Les protocoles de communication, le protocole d'accès au médium(MAC) ou celui de routage, influencent beaucoup la consommation. Le domaine de recherche qui consiste à inventer des protocoles dédiés aux réseaux de capteurs est très actif. De ces protocoles dépend directement le temps pendant lequel la radio émet ou reçoit et donc la consommation d'énergie.

Pour tous les protocoles, il y a également souvent des paramètres à définir et ces paramètres peuvent interagir. Tous ces choix dépendent bien sûr de l'application. Le choix du protocole de routage dépend du type de communication le plus couramment utilisé. Il est inutile de concevoir un protocole efficace point-à-point si ce mode de communication n'est jamais utilisé. Les choix de conception d'un réseau de capteurs dépendent naturellement de l'environnement physique dans lequel il est déployé.

Dans ce contexte, trouver une méthode pour atteindre la solution optimale en énergie est probablement hors de portée. Trouver des méthodes et outils d'aide à la conception des réseaux de capteurs, semble plus accessible. Un point important que doivent prendre en

compte ces méthodes est la consommation d'énergie. Une méthode de conception pourrait consister à construire le système complet puis à l'évaluer [18].

Certes cette solution serait fiable puisqu'on évaluerait une solution complète mais, vu les contraintes de temps, elle paraît difficilement faisable. En effet, un réseau de capteurs peut nécessiter des solutions matérielles dédiées coûteuses à développer. Pour exécuter la même fonction, une solution matérielle dédiée peut être plus efficace en énergie. En contrepartie, elle est moins reconfigurable et sa conception est plus coûteuse. Ce coût élevé de conception ne permet pas de tester la solution matérielle pour décider si elle remplace avantageusement le logiciel. Il n'est pas envisageable non plus de comparer, en les testant, deux implantations matérielles différentes.

1.10Réseau de capteurs vidéo sans fil

Le développement des micro-caméras et microphones a observé une forte évolution au cours de la dernière décennie, avec les évolutions des téléphones mobiles. Ces dispositifs deviennent de plus en plus petits et bon marché, et fournissent de plus en plus de performances en termes de rapidité et de qualité du signal. Aujourd'hui, nous trouvons ces micro-caméras embarquées dans pratiquement tous les téléphones cellulaires et les assistants numériques personnels, sans augmentation significative du coût de l'équipement, de son poids et de sa forme.

Les réseaux sans fil n'ont pas été en dehors de ce progrès et aujourd'hui, nous pouvons déjà voir les résultats des dernières avancées de microphones et micro-caméras CMOS, sous la forme de cartes de capteurs compatibles avec des nœuds sans fil. Cela a permis d'envisager concrètement un nouveau type d'applications utilisant des *réseaux de capteurs sans fil multimédia.*

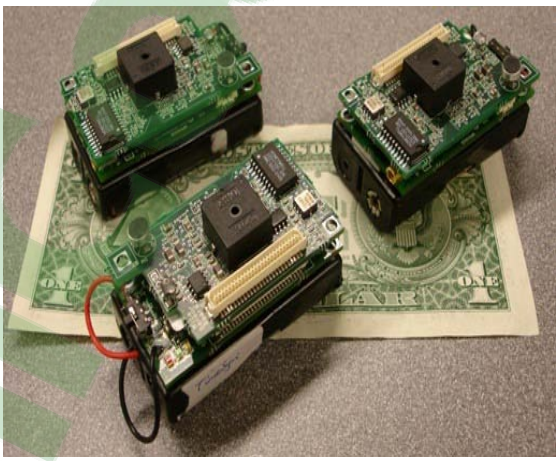

Figure 1.21 Nœud capteur vidéo sans fil

Parmi les nombreuses applications potentielles des réseaux de capteurs multimédia, celles utilisant des capteurs d'image sont appréciables pour tout ce qui concerne la reconnaissance, la localisation et le dénombrement d'objets par la vision. Certaines applications ont besoin d'identifier exactement le ou les objets qui traversent le champ

du réseau de capteurs. D'autres applications n'ont pas besoin directement d'images, mais la prise d'image peut servir à compléter et enrichir les mesures initiales [19].

En fonction des exigences imposées à l'application, et bien évidemment en fonction du type de technologie disponible, les réseaux de vision peuvent être de deux types :

Réseaux de capteurs d'images fixes : Des capteurs d'images numériques peuvent prendre des photos qui peuvent être mémorisées en format matriciel ou vectoriel. Ce type de capteur est facile à réaliser et peut être adapté facilement à des dispositifs avec des ressources limitées, tels que les nœuds de capteurs sans fil.

Réseaux de capteurs de vidéo : Des capteurs d'images numériques peuvent aussi envisager de prendre des séquences d'images et de transmettre le flux vidéo vers le puits. Cette application exige des nœuds avec des capacités de calcul, de mémoire et de communication d'un tout autre ordre de grandeur que pour les images fixes.

Figure 1. 22 Vidéosurveillance

Les défis en matière de recherche :

La vision est certainement le sens le plus puissant, mais aussi le plus complexe, généralement associées à des problèmes de traitement à coût élevé, pourraient être multipliés lorsque nous devons faire face à d'énormes limitations en ressources, comme dans le domaine des réseaux de capteurs sans fil. Au delà des défis traditionnels des réseaux de capteurs sans fil les applications des réseaux de capteurs d'images posent des défis particuliers, notamment [20] :

- *Des protocoles de transmission et des algorithmes de compression d'images du monde réel*
- *Temps réel*
- *Gestion de l'énergie*
- *Abstractions de la programmation*
- *Sécurité et confidentialité*

1.11 Conclusion

Ce chapitre a défini les réseaux de capteurs, les outils d'exploitation qui y sont associés, les technologies de communication utilisées dans ces réseaux émergents, les différentes applications les mettant en œuvre, les protocoles de routage, les attaques et les défis à surmonter.

La consommation d'énergie est un problème fondamental lorsque les capteurs sont déployés dans des zones inaccessibles ou encore déployés sur de grands espaces, c'est à-dire lorsqu'il est difficile voire impossible de remplacer les batteries des nœuds quand elles arrivent à épuisement. De ce fait, la durée de vie limitée des nœuds va avoir un impact sur la durée de vie du réseau tout entier.

En conclusion, la durée de vie de réseau de capteurs sans fil doit tenir compte de la connectivité et de la couverture si elles sont nécessaires aux besoins des applications. La connaissance des exigences de l'application aide les concepteurs à affiner la définition de la durée de vie du réseau afin d'aboutir à une évaluation beaucoup plus réaliste et plus précise pour les utilisateurs de l'application.

Le chapitre suivant traite les notions de bases sur les systèmes de détection d'intrusion et la sécurité dans les réseaux de capteurs sans fil.

Chapitre 2 : Sécurité et détection d'intrusion

2.1.Introduction

Les réseaux de capteurs sans fil sont constitués de nœuds déployés en grand nombre en vue de collecter et transmettre des données environnementales vers un ou plusieurs points de collecte, d'une manière autonome. Ces réseaux ont un intérêt particulier pour les applications militaires, environnementales, domotiques, médicales, et bien sûr les applications liées à la surveillance des infrastructures critiques. Ces applications ont souvent besoin d'un niveau de sécurité élevé. Or, de part de leurs caractéristiques (absence d'infrastructure, contrainte d'énergie, topologie dynamique, nombre important de capteurs, sécurité physique limitée, capacité réduite des nœuds,...), la sécurisation des réseaux de capteurs est à la source, aujourd'hui, de beaucoup de défis scientifiques et techniques.

Toutes ces applications ont des contraintes de sécurité très différentes. Cependant, dans la plupart d'entre elles, l'intégrité et l'authenticité des données doivent être fournies pour s'assurer que des nœuds non-autorisés ne puissent pas injecter des données dans le réseau. Le chiffrement des données est souvent requis pour des applications sensibles telles que les applications militaires ou les applications médicales.

Les réseaux de capteurs sont vulnérables à différents types d'attaques qui peuvent être lancées de façon relativement simple. En particulier, la nature des communications sans fil facilite l'écoute clandestine permettant ainsi une analyse facile du trafic réseau. Le manque d'une infrastructure fixe et l'hypothèse d'un environnement ouvert sans aucune surveillance humaine permettent des attaques dédiées comme l'usurpation d'identités ou bien la compromission des nœuds. Un attaquant ayant compromis un ou plusieurs nœuds peut ainsi accéder à tous les secrets enregistrés dans le nœud, et ainsi se comporter comme un nœud légitime, sans pour autant se faire détecter.

La sécurisation des réseaux de capteurs reste un problème difficile. Les solutions de sécurité qui existent aujourd'hui ne sont pas utilisables car elles sont souvent trop coûteuses en terme de ressources. Par exemple, l'utilisation de la cryptographie à clés publiques est souvent proscrite de ce type d'environnement. De nouveaux algorithmes et protocoles de sécurité sont nécessaires.

Plusieurs travaux de recherches sont intéressés aux IDS. L'auteur dans [21] a donnée une classification des différents types de systèmes de détection d'intrusion. L'auteur dans [22] a proposé une ontologie des IDS. Dans [23], l'auteur a axé ses recherches sur la sécurité des réseaux de capteurs. Dans [24], l'auteur a défini les différents types d'attaques.

Ce présent chapitre traite la problématique de la sécurité dans les réseaux de capteurs sans fil.

2.2. Système de détection d'intrusion (IDS)

Les systèmes de détection d'intrusion (IDS) sont des systèmes capables de déceler les attaques. Les IDS basés sur les scénarios sont des IDS avec pour base de connaissance des signatures d'attaques connues [24].

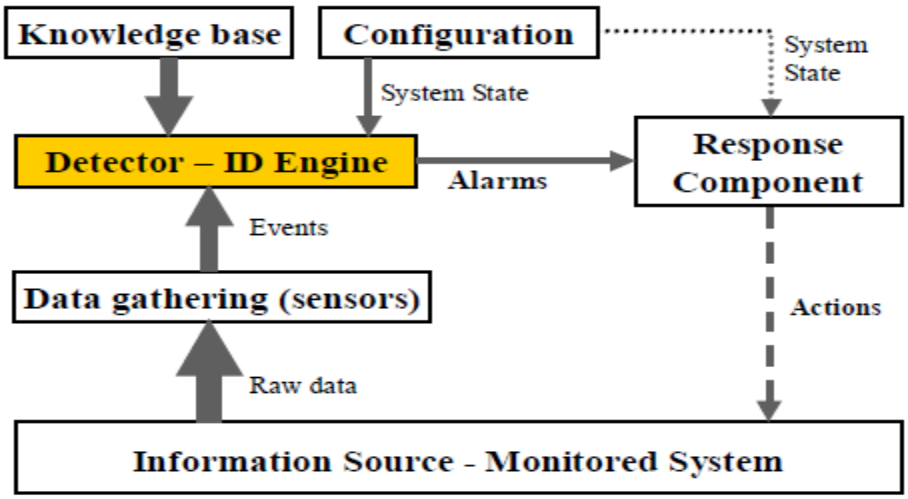

Figure 2.1 Architecture de base d'un IDS

Grâce à sa base de données, ce type de système détecte facilement et rapidement les attaques et menaces présentes dans un flux réseau ou sur une machine. Les IDS sont classifiés comme suit:

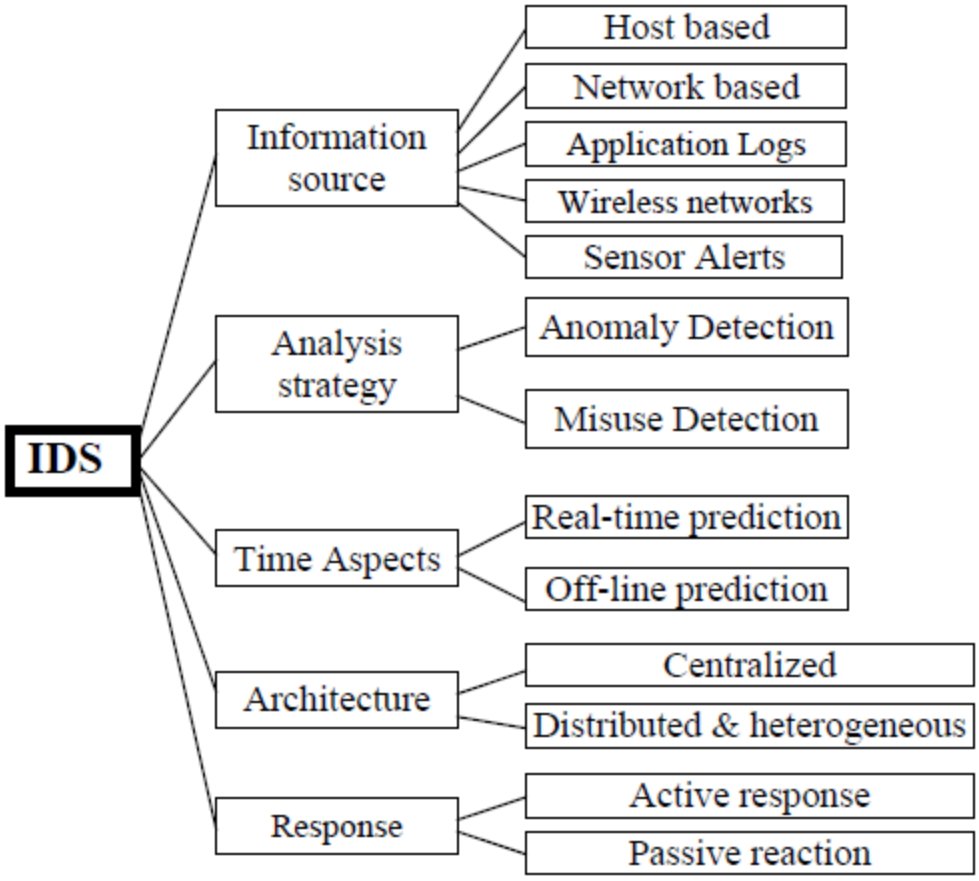

Figure 2.2 Classification des IDS

Les IDS basés sur un bon comportement sont, à contrario des IDS basé signature, des systèmes de détection d'intrusions sans base de connaissance [21].

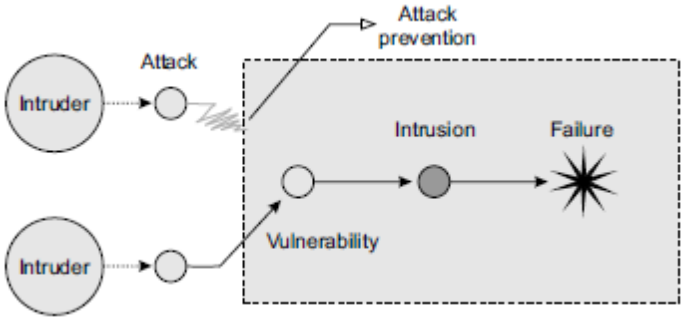

Figure 2.3 Système vulnérable aux attaques

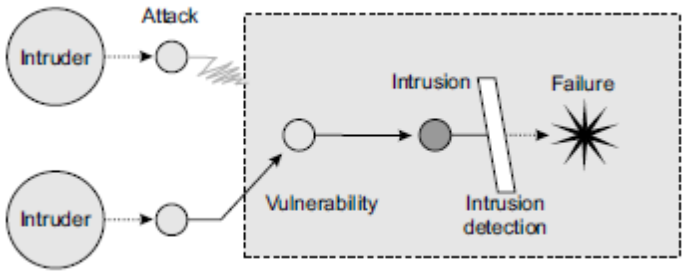

Figure 2.4 Système non vulnérable aux attaques

Il requiert cependant un entrainement fait à partir du comportement normal d'un trafic réseau. Ces IDS utilisent des méthodes de calcul probabiliste, qui associé à des méthodes de classifications de données, permettent de déterminer qu'une attaque a lieu ou non à partir d'un flux réseau.

2.2.1 Architectures des IDS :

Les architectures des SDI dans les réseaux ad hoc et les réseaux de capteurs sans fils peuvent êtres classées en trois catégories [22]:

- Architecture Autonome (Stand-alone);
- Architecture Distribué et coopératif (Distributed and Cooperative)
- Architecture Hiérarchique (Hierarchical).

Architecture Autonome (Stand-alone) : Dans cette catégorie, chaque nœud opère comme un SDI indépendant et il est responsable de la détection des attaques contre lui. Par conséquent, dans cette catégorie, les SDI ne coopèrent pas et ne partagent aucune information entre eux. Cette architecture exige que chaque nœud soit capable d'exécuter un SDI.

Architecture Distribuée et coopérative (Distributed and Cooperative) : Dans cette architecture chaque noeud exécute son propre SDI mais les SDIs coopèrent afin de créer un mécanisme de détection d'intrusion global.

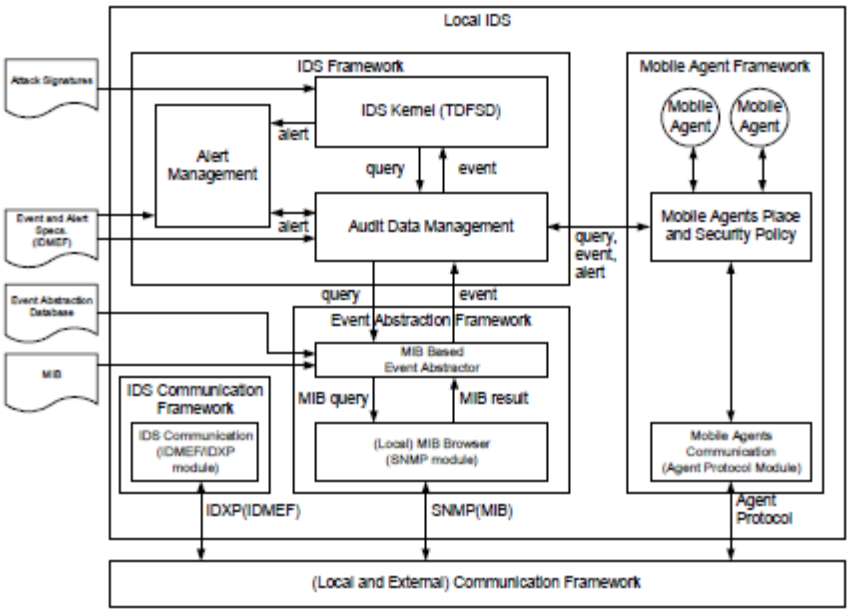

Figure 2.5 Architecture distribuée d'un IDS

Architecture Hiérarchique (Hierarchical) : Dans ce cas le réseau de capteur est divisé en groupes (clusters). Dans chaque groupe, un leader joue le rôle de cluster-head. Ce nœud est responsable du routage dans le groupe et doit accepter les messages des membres du groupe indiquant quelque chose de malveillant. De même le cluster-head doit détecter les attaques contre les autres cluster-heads du réseau.

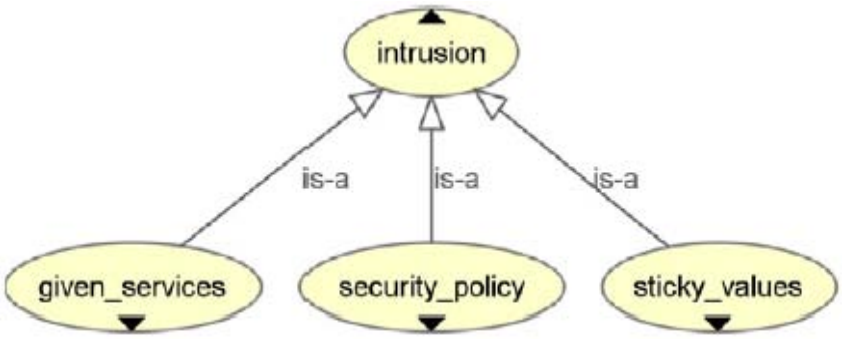

Figure 2.6 Ontologie d'intrusion

2.2.2 Propriétés des IDS

Dans les réseaux de capteurs sans fil un système de détection d'intrusion doit satisfaire les propriétés suivantes [25][56]:

Audit local (Localize auditing) : un SDI pour les réseaux de capteurs sans fil doit fonctionner avec des données d'audits locales et partielles car dans les réseaux de capteurs sans fil, il n'y a pas de points centralisés (à part la station de base) qui peut collecter les données d'audit globales.

Ressources minimales (Minimize resources): un SDI pour les réseaux de capteurs doit utiliser un nombre minimum de ressources car les réseaux sans fils n'ont pas de connexions stables. De plus les ressources physiques du réseau et des nœuds telles que la bande passante et la puissance sont limitées. La déconnexion peut survenir à tout moment. La communication entre les nœuds pour la détection d'intrusion ne doit donc pas prendre toute la bande passante disponible.

*Pas de nœud de confiance (Trust no node)***:** un SDI dans les réseaux de capteur ne doit faire confiance a aucun nœud car, contrairement aux réseaux filaires, les nœuds capteurs peuvent être compromis facilement.

*Distribué (Be truly distributed)**:*** veut dire que la collection et l'analyse de données doit se faire dans plusieurs endroits (locations). De plus l'approche distribuée s'applique aussi pour l'exécution de l'algorithme de détection et la corrélation d'alertes.

*Sécurisé (Be secure)***:** un SDI doit être capable de résister aux attaques.

2.2.3 Approches de détection d'intrusion

La détection d'intrusion peut être définie comme la détection automatique et la génération d'une alarme pour rapporter qu'une intrusion a eu lieu ou est en cours.

Approche comportementale : le comportement observé du système cible est comparé aux comportements normaux et espérés. Si le comportement du système est significativement différent du comportement normal ou attendu, on dit que le système cible présente des anomalies et fait l'objet d'une intrusion. L'avantage principal de cette approche est de pouvoir détecter de nouvelles attaques.

Cependant, elle génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours à l'occurrence d'une attaque.

Approche par scenarios : consiste à modéliser non plus des comportements normaux, mais des comportements interdits. Dans cette approche on analyse les données d'audits à la recherche de scénarios d'attaques prédéfinis dans une base de signatures d'attaque.

Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Par contre son inconvénient majeur est de ne pouvoir détecter que les attaques enregistrées dans la base de signatures.

2.2.4 Types de détection d'intrusion

2.2.4.1 Intrusion dues aux sticky values

La capacité d'un RCSF à effectuer ses tâches ne dépend pas uniquement de sa capacité à communiquer avec les autres nœuds du réseau, mais surtout de sa capacité à capter les grandeurs physiques de son environnement et des procédés de traitement des données collectées. L'agrégation des données provenant de multiples nœuds nécessite que l'on accorde une certaine confiance à ces nœuds, or les fortes contraintes en terme de ressources limitées rendent ceux-ci très peu fiables [25]. Les fautes les plus courantes

dans les RCSFs surviennent lors du déploiement. Ils sont ainsi classés dans la catégorie de sticky values. Ce sont des valeurs qui peuvent provenir soit des erreurs de mesure par les capteurs, soit des données hors limites, soit des dépassements de plage de lecture soit enfin de la similitude qui existe entre certaines valeurs de calibrage de la radio, de l'antenne, de la mote et des équipements de récupération des données.

2.2.4.2 Détection des intrusions comme service

Les RCSFs sont souvent utilisés comme équipements de surveillance. La détection de la cible (personne, véhicule, objet, ennemi dans un champ militaire,…) comme intrus est l'un des objectifs majeurs dans la surveillance. Plusieurs techniques sont mises en œuvre pour la détection des intrus dans un tel système de surveillance. L'utilisation d'un seuil fixe de valeur offre une détection efficace mais avec un fort taux de fausses alarmes. Le calcul de probabilité pour l'obtention d'un seuil dynamique de valeur est proposé comme alternative pour offrir un meilleur équilibre entre la quantité de fausses alarmes et le taux de détection.

2.2.4.3 Détection des intrusions comme politique de sécurité

Dans le domaine de la sécurité, est considérée comme intrusion, toute tentative de violation de la politique de sécurité d'un système. Notamment, il s'agit de la violation d'une des propriétés de confidentialité, d'intégrité ou de disponibilité du système. Pour la plupart, elles sont causées par des nœuds corrompus ou par des nœuds externes usurpant des privilèges de sécurité. Le réseau devrait continuer son fonctionnement malgré l'apparition d'un comportement inconnu susceptible de gêner le bon fonctionnement de celui-ci.

2.3. Contraintes dans un RCSF

Les réseaux de capteurs possèdent des caractéristiques et des contraintes uniques comparées aux réseaux traditionnels rendant l'exécution des mesures de sécurité existantes irréalistes. La figure suivante montre les différents défis à surmonter dans la construction d'un IDS orienté réseau de capteurs sans fil.

Figure 2.7 Contraintes à satisfaire dans un RCSF

Ces contraintes sont classées en 2 catégories : contraintes du nœud et contraintes réseau.

- *Contraintes matérielles* : ces contraintes sont liées aux capacités matérielles et physiques d'un nœud capteur, ce qui représente un handicap pour les besoins en sécurité qui nécessite en général des ressources additionnelles : mémoire limitée, énergie limitée, capacité de calcul limitée, radio limitée et faible débit.
- *Contraintes réseau* : Les communications sans fil sont en général incertaines car des paquets peuvent être perdus ou endommagés à cause de la transmission radio. Un paquet peut être renvoyé suite à une perte de données. Dans le cas d'un réseau de capteurs, le manque en énergie limitera le renvoi des paquets dans ces conditions.

2.4. Vulnérabilités dans un RCSF

Les mécanismes de défense dans un réseau de capteurs ne doivent pas juste tenir en compte de la nature de l'attaque, mais doivent également tenir compte de la nature de l'attaquant et de ses caractéristiques.

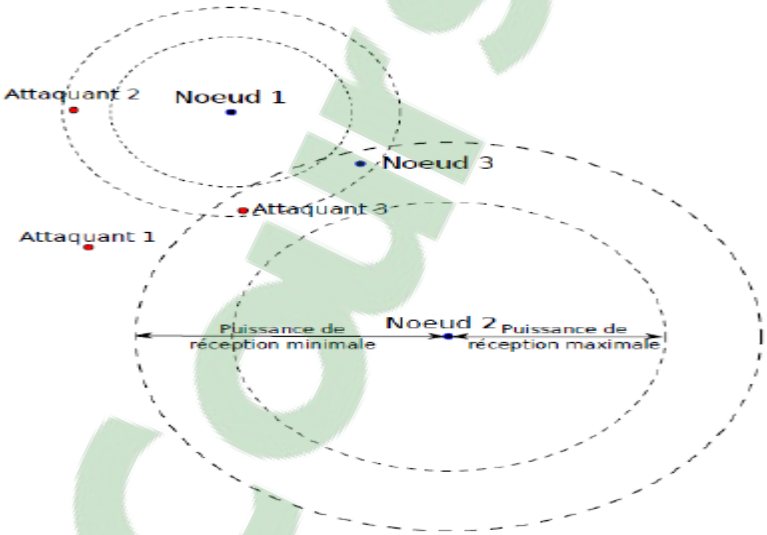

Figure 2.8 Attaques dans un RCSF

Ainsi, un attaquant peut être classifié selon son intention, localisation, capacité et sa mobilité [26].

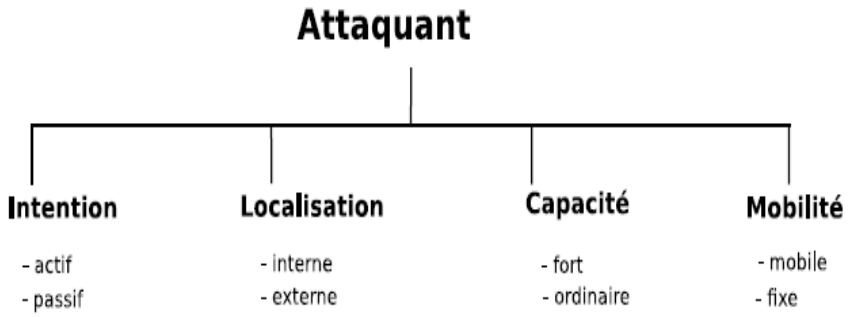

Figure 2.9 Classification des attaquants

Selon son intension :
Attaquant passif : ici l'attaquant essaye de collecter des données sur le réseau sans affecter son fonctionnement. Par exemple, une écoute passive des messages sur le canal sans fil.
Attaquant actif : ici l'attaquant essaye de détruire le fonctionnement du réseau d'une manière partielle ou bien totale. Plusieurs attaques, qui seront détaillées dans la section.

Selon sa position par rapport au réseau:
Attaquant externe : ici l'attaquant est considéré comme un "étranger" par rapport au réseau, il s'agit d'un utilisateur non autorisé qui s'introduit depuis l'extérieur du périmètre de sécurité du réseau.
Attaquant interne : ici l'attaquant se manifeste comme une entité légitime du réseau autorisée à accéder aux ressources fournies par le système. L'attaquant est ainsi authentifié et reconnu par l'ensemble des éléments du réseau.

Selon sa capacité :
Attaquant fort : ici l'attaquant est équipé d'extra-ressources par rapport à l'ensemble des nœuds présents dans le réseau. Par exemple, un attaquant utilise un PC portable avec un médium radio sophistiqué.
Attaquant ordinaire : ici l'attaquant possède les mêmes caractéristiques que les autres nœuds.

Selon sa mobilité :
L'attaquant peut être fixe ou mobile: Un attaquant mobile dans un réseau est plus difficile à détecter par rapport à un attaquant fixe.

2.5. Exigences en sécurité

Les applications n'ont pas les mêmes besoins de sécurité, mais en général, les besoins primaires à considérer lors de l'étude de la sécurité dans les RCSFs sont [25]:

Authentification : Un nœud doit savoir et vérifier la légitimité du nœud qui essaye d'établir une connexion avec lui. Par conséquent, l'authentification est un mécanisme fondamental pour assurer le contrôle d'accès dans le réseau.

Contrôle d'accès : Il représente est la capacité des nœuds du réseau (ou bien d'une unité centrale comme la station de base) à accorder l'accès approprié aux ressources (connectivité, données,...) en fonction d'informations sûres.

Confidentialité : Le canal radio est particulièrement vulnérable à l'écoute clandestine. Par conséquent, la confidentialité des informations échangées est également une condition importante pour assurer la sécurité du réseau.

Intégrité : Comme le canal radio est également fortement vulnérable aux attaques actives, l'intégrité des données doit être convenablement protégée. Le nœud doit s'assurer que le message n'a pas été modifié en cours de route.

Vie privé : Dans un réseau la protection de la vie privée (en anglais privacy) est exigée. Le réseau ne devrait pas indiquer l'endroit des nœuds dans le réseau, ni l'identité des autres nœuds avec lesquels ils communiquent.

Non-répudiation (garantie par la signature numérique) : elle permet d'assurer la source d'un paquet. Ainsi un nœud ne peut pas nier l'envoi d'un paquet dans le passé.

2.6. Défis de la sécurisation des réseaux de capteurs

La sécurisation des réseaux de capteurs reste un problème difficile pour les raisons suivantes [26]:

Capacités limitées : Les ressources de calcul et de mémoire des nœuds sont relativement faibles. L'énergie limitée des capteurs est probablement la caractéristique la plus pénalisante. Le plus grand des défies dans le domaine des réseaux de capteurs reste de concevoir des protocoles, entre autre de sécurité, qui minimisent l'énergie afin de maximiser la durée de vie du réseau. En d'autres mots, l'énergie est sans aucun doute la ressource qui convient de gérer avec la plus grande attention.

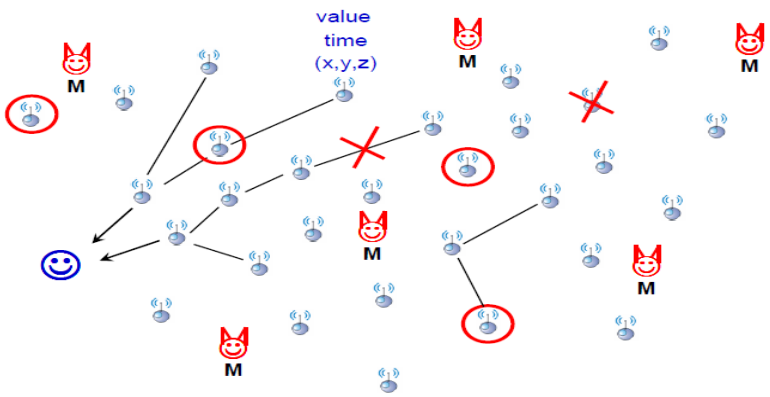

Figure 2.10 Vulnérabilité de RCSF

Les solutions de sécurité qui existent aujourd'hui ne sont pas utilisables car elles sont souvent trop coûteuses en terme de ressources. Par exemple, l'utilisation de la

cryptographie à clés publiques est souvent proscrite de ce type d'environnement. De nouveaux algorithmes et protocoles de sécurité sont nécessaires.

Agrégation des données : La transmission d'un bit est équivalente, en terme d'énergie, à l'exécution de millier d'instructions. Cette valeur augmente avec la portée de la radio. Plus le capteur devra transmettre loin, et par conséquent augmenter sa puissance d'émission, plus il va consommer de l'énergie, et par conséquent réduire sa durée de vie.

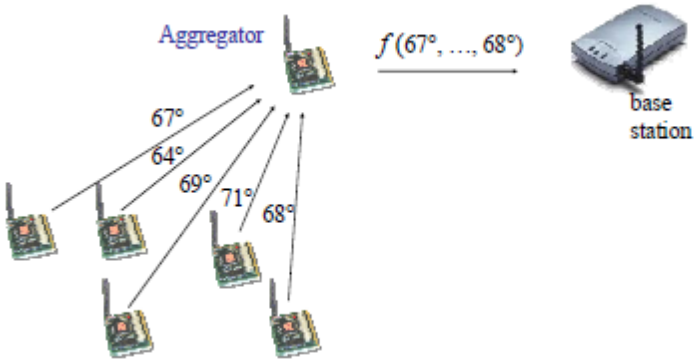

Figure 2.11 Agrégation des données dans RCSF

Les techniques d'agrégation des données, c'est à dire de traitement des données par le réseau, permettent de réduire le nombre de messages et par conséquent réduire la consommation en énergie.

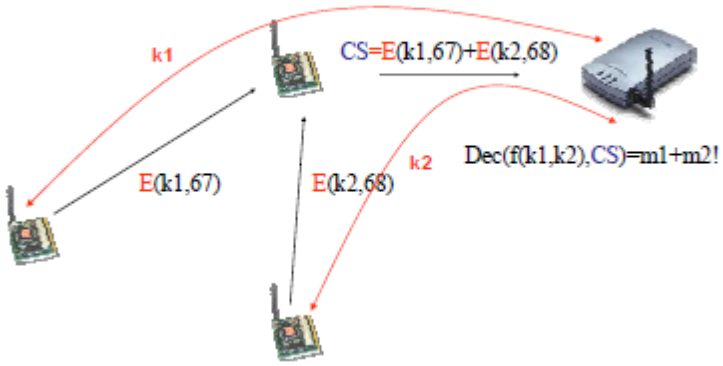

Figure 2.12 Agrégation sécurisée dans RCSF

Les techniques d'agrégation sont souvent difficiles à mettre en œuvre lorsque les données sont chiffrées car le traitement des données devient alors très délicat.

Echelle de dynamicité : Les réseaux de capteurs sans fil sont souvent peu stables et très dynamiques. Les capteurs, qui ont consommé leur pile, disparaissent et des nouveaux nœuds doivent être déployés pour assurer une certaine connectivité.

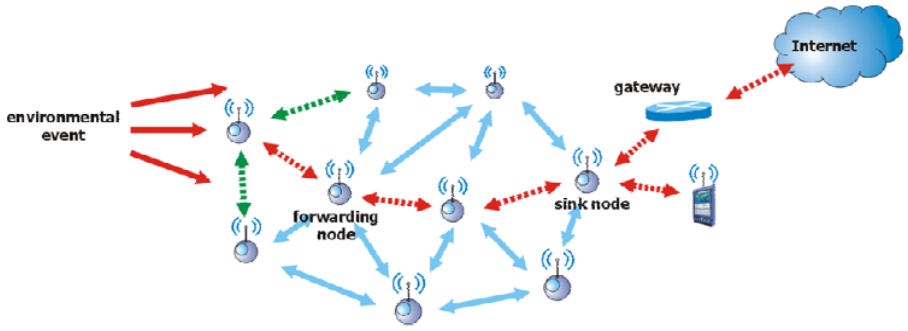

Figure 2.13 Passage à l'échelle du RCSF

Protection physique faible : Les capteurs sont souvent déployés dans des environnements non-protégés (montagnes, forêts, champs de bataille,...). Par conséquent, ils peuvent facilement être interceptés et corrompus. De plus, à cause de leur faible coût, ils utilisent rarement des composants électroniques anti-corruption.

2.7. Les attaques dans RCSF

Les attaques se font sur toutes les couches de communication: sur la couche physique, sur la couche MAC (liaison), sur la couche réseau (routage) et sur la couche application. La figure suivante illustre l'évolution des techniques de détection des attaques [27].

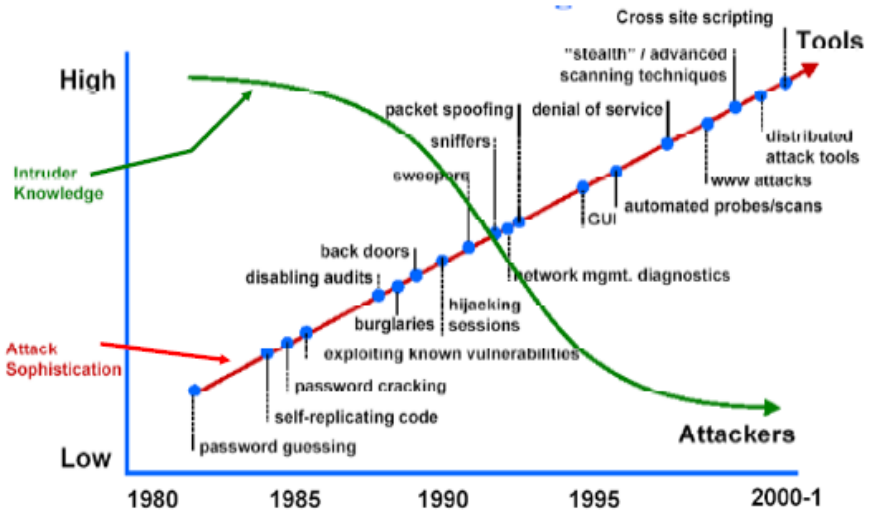

Figure 2.14 Evolution des techniques de détection des attaques

La figure suivante résume les plus importantes attaques:

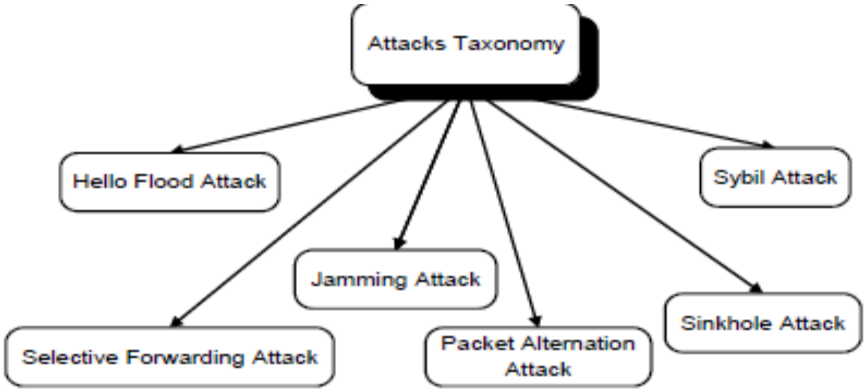

Figure 2.15 Classification des attaques

Jamming : C'est une attaque de type Deni de Service (DoS) dont le but est de perturber la communication. L'attaquant bloque la réception du canal radio d'un nœud en transmettant sur sa bande de fréquence à fin de provoquer des interférences radio.
Tampering : Elle consiste à la capture et à l'accès physique au nœud à fin d'extraire toutes les informations présentes comme les clés de cryptage.
Collision : Elle est comparable au jamming, l'adversaire envoie son signal quand il entend un nœud légitime entrain de transmettre à fin de provoquer des interférences (attaque DoS).
Expédition sélective : Dans cette attaque, un nœud malveillant agira comme un nœud normal en transférant des messages mais va sélectivement jeter certains.
Sinkhole/ Blackhole : Un nœud peut devenir un trou noir en informant qu'il a le plus court chemin (meilleurs métriques de routage) vers la station de base et ainsi toute l'information lui sera acheminée. Les nœuds victimes le choisiront comme un transitaire pour les paquets et lui peut faire ce qu'il veut avec toutes les informations reçues.
Boucle de routage : La coopération de plusieurs nœuds peut créer une boucle dans le mécanisme de routage entre une source et un nœud destinataire.
Sybille : Dans cette attaque, un nœud malveillant peut prétendre être plusieurs nœuds (identités multiples) légitimes (contrecarrant le processus de collaboration d'une tâche distribuée comme l'agrégation des données ou le vote) ou inexistants (remplir la liste de voisinage des nœuds voisins avec des nœuds inexistants).
Réplication de nœuds : C'est une variante de l'attaque sybille. Elle consiste à capturer un nœud, construire des copies légitimes de ce dernier et les ajouter partout au réseau créant ainsi des identités multiples utilisant la même cryptographie que le nœud légitime original.
Hello flood : Dans cette attaque de type DoS, les paquets sont envoyés pour la découverte d'un voisin. Un dispositif sophistiqué qui utilise un signal radio puissant à longue portée pourrait envoyer des paquets de ce genre et ainsi inonder une partie du réseau tout en provoquant de fausses listes de voisins.
Wormhole : Dans l'attaque de trou de ver, un nœud compromis enregistre les paquets et les envoie via un lien ou tunnel de faible latence vers un autre nœud malicieux dans le réseau.

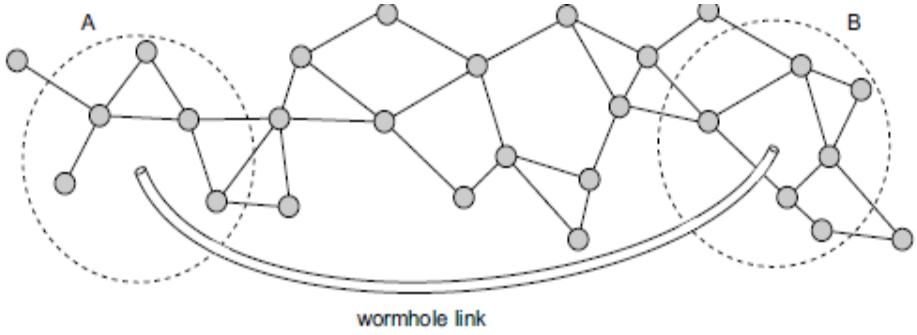

Figure 2.16 Attaque Wormhole

Innondation au niveau applicatif : Cette attaque est mise en œuvre soit par un ou plusieurs nœuds ou un ordinateur portable. Elle vise à épuiser les ressources limitées (mémoire et énergie) d'un nœud légitime. L'attaquant envoie successivement des demandes de connexions à un nœud légitime jusqu'à ce que ce dernier meure.
Forced delay : Un nœud malveillant retarde délibérément les paquets à l'intérieur de son élément de transmission à fin de retarder la transmission des événements importants.
Désynchronisation : L'attaque consiste à perturber la communication déjà établie entre deux nœuds en les poussant à rompre leur synchronisation.

2.8. Primitives cryptographiques utilisées dans RCSF

2.8.1 Cryptographie :

On distingue deux grandes formes de cryptographie permettant de garantir chacune un certain nombre de propriétés : la cryptographie symétrique ; la cryptographie asymétrique.

1. La cryptographie symétrique :
Elle également dite à clé secrète, est la plus ancienne forme de cryptographie. Elle nécessite pour fonctionner que les deux parties en présence est au préalable échangées une clé commune connue seulement d'eux.

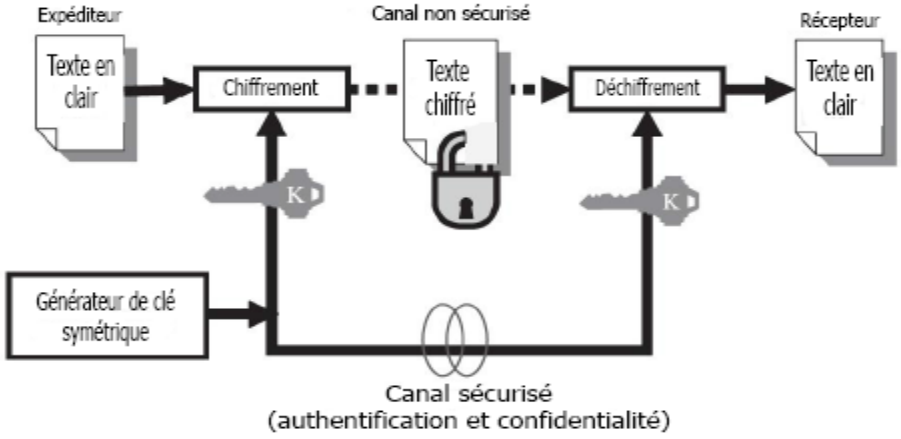

Figure 2.17 Chiffrement symétrique

La cryptographie symétrique permet de garantir la confidentialité, l'intégrité et la signature bipartie via l'utilisation de code d'authentification de messages.

2. La cryptographie asymétrique :
Elle est également appelée cryptographie à clé publique, repose sur l'utilisation de deux clés différentes pour chiffrer/déchiffrer, signer/vérifier. Ces deux valeurs de clés sont certes différentes mais reliées entre elles : une clé publique (qui est diffusée) et une clé privée (gardée secrète), l'une permettant de chiffrer/signer un message et l'autre de le déchiffrer/vérifier. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour chiffrer un message que seul le destinataire (en possession de la clé privée) peut déchiffrer, garantissant la confidentialité du contenu.

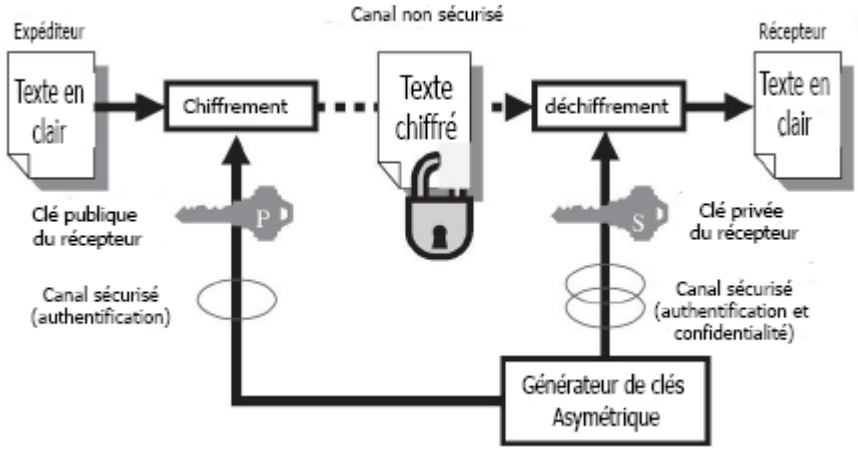

Figure 2.18 Chiffrement asymétrique

Inversement, l'expéditeur peut utiliser sa propre clé privée pour signer un message et le destinataire peut vérifier la signature du message à l'aide de la clé publique correspondante; Ce dernier mécanisme permet de faire de la signature numérique pour authentifier l'auteur d'un message.

2.8.2 Fonction de hachage :
Une fonction de hachage cryptographique consiste en général à l'application d'une fonction de compression à sens unique sur un bloc de données de taille quelconque pour générer une sortie de taille fixe de n bits. La valeur n représente le degré de sécurité de la fonction de hachage.

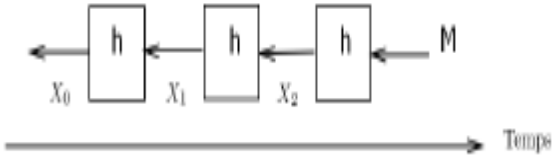

Figure 2.19 Chaine de hachage de taille 3

La fonction de hachage doit être en général facile à calculer et connue publiquement mais très difficile à inverser.

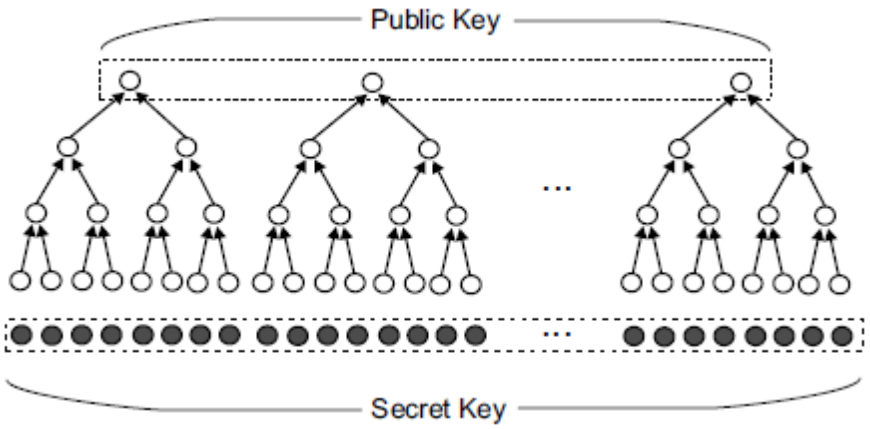

Figure 2.20 Construction d'une clé publique par hachage

Les fonctions de hachage sont généralement utilisées comme première étape pour vérifier l'intégrité d'un message ou bien pour générer des signatures numériques.

2.9. Protocoles de sécurités dans RCSF

2.9.1 Mécanismes de gestion des clés

La sécurisation des opérations au sein d'un réseau de capteurs nécessite la protection des messages échangés entre les nœuds. Intuitivement, chaque message doit être prouvé intègre et doit être identifié et éventuellement chiffré [28].

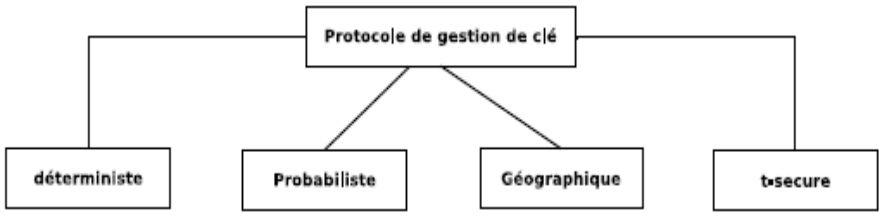

Figure 2.21 Protocoles de gestion des clés

- Les protocoles déterministes : ils utilisent une clé maître pour dériver les clés entre paires de capteurs;
- Les protocoles probabilistes : ils supposent que deux nœuds voisins vont partager une clé avec une certaine probabilité;
- Les protocoles géographiques : ils utilisent des informations de positions géographiques pour construire les clés partagées;
- Les protocoles t-Secure : ils résistent à la compromission de t noeuds dans le réseau.

Par conséquence, la gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Alors que les nœuds capteurs sont potentiellement exposés aux attaques physiques et ne peuvent compter sur une intervention humaine. Un attaquant qui capture un nœud peut extraire toutes ses clés secrètes et déclencher tout type d'attaques sans qu'il soit identifié.

Les protocoles de gestion de clés doivent être résistants aux attaques contre les capteurs. Une stratégie de distribution sécurisée des clés est également à prévoir afin de pouvoir assurer un certain niveau de sécurité.

2.9.2 Protocoles de routage sécurisés

Le problème du routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance comme la consommation énergétique. Une attaque simple de déni de service sur un protocole de routage consiste pour un nœud à refuser arbitrairement de transférer certains messages ou de supprimer un paquet en transit de façon aléatoire.

Plusieurs propositions ont été faites pour sécuriser différents algorithmes de routage, essentiellement les algorithmes de routage à la demande dans les réseaux ad-hoc ou les réseaux de capteurs. Il est donc nécessaire de sécuriser les protocoles de routage conçus initialement pour un environnement sans risque ou même de concevoir de nouveaux algorithmes robustes afin de mener à bien l'opération de l'acheminement des données même en présence des nœuds malicieux.

2.9.3 Mécanismes d'agrégations sécurisés

Le but d'un réseau de capteurs sans fil est de collecter et de transmettre des données physiques captées par les nœuds vers un ou plusieurs points de collecte (qui pourrait être la station de base), et ce, de façon autonome.

Les applications où les nœuds envoient les données vers la station de base en utilisant une approche multi-saut. Dans ce type de modèle, l'opération la plus coûteuse est celle d'envoi des paquets d'informations. Ainsi, diminuer le nombre de bits transmis afin d'augmenter la durée de vie du réseau est un défi permanent pour ce type de réseau. Une approche répandue consiste à agréger les paquets lors de leurs acheminements vers la station de base.

L'agrégation des données permet de réduire de façon significative la quantité de données échangées dans le réseau. Garantir la sécurité conjointement à des techniques d'agrégation est problème difficile à résoudre.

2.9.4 Mécanismes de synchronisation sécurisés

La sécurité est une brique vitale qui doit être prise en compte dans les protocoles de synchronisation : n'importe quel protocole qui ne met pas à jour une seule horloge d'un nœud peut influencer le comportement de tout le réseau. Les attaques contre les protocoles de synchronisation sont généralement exécutées à l'aide de l'attaque de compromission des nœuds, qui permettra d'introduire des erreurs au niveau des valeurs des horloges et ainsi de faire échouer le protocole en entier.

2.9.5 Mécanismes de localisation sécurisés

La tâche de positionnement des nœuds est le but des systèmes de localisation. Ces systèmes de localisation sont aussi à la base du fonctionnement d'autres protocoles comme le routage ou bien le contrôle de densité et de topologie. Ainsi, les systèmes de localisation peuvent être des cibles pour plusieurs attaques permettant ainsi de compromettre tout le fonctionnement du réseau.

La connaissance des positions des capteurs dans l'environnement surveillé est souvent indispensable pour une grande majorité des applications (militaires, suivis des animaux, ...), afin de pouvoir déterminer l'origine des événements détectés. La sécurisation des protocoles de localisation est nécessaire pour protéger le réseau des ancres malicieux et des attaquants qui tentent de perturber le processus de localisation.

2.10. Conclusion

La conception de réseaux de capteurs autonomes, reliés par des liens sans fil, est un domaine de recherche très actif. Les applications basées sur ces réseaux ont souvent besoin d'un niveau de sécurité élevé car ils fournissent des services essentiels, voire vitaux.

La sécurité est un domaine très vaste et représente un défi scientifique à cause des caractéristiques spécifiques des réseaux de capteurs. Les recherches dans cette problématique ont révélé plusieurs axes de recherche. Il devient donc urgent de se pencher sur les problèmes de sécurité et de protection de la vie privée qu'ils engendrent avant qu'ils envahissent nos vies et environnements.

Dans ce chapitre nous avons présenté les différentes problématiques de la sécurité dans les réseaux de capteurs sans fils.

Chapitre 3 : Techniques de la redondance

3.1Introduction

La *redondance* se rapporte à la qualité ou à l'état d'être en surnombre, par rapport à la normale ou à la logique. Ce qui peut avoir la connotation négative de superflu, mais aussi un sens positif quand cette redondance est voulue afin de prévenir un dysfonctionnement. La redondance est conçue comme le déploiement d'un éventail de versions différentes d'une même structure (redondance structurelle) ou d'une même fonction (redondance fonctionnelle).

Ce présent chapitre a pour objectif de donner les notions de bases sur la redondance, exploitation de la redondance, les problématiques liées à son usage, les travaux existants, définition du contexte de notre travail sur la redondance dans les réseaux de capteurs images sans fil pour la surveillance.

3.2 Définitions

La redondance d'informations est le concept de base des systèmes de diagnostic. Plusieurs informations différentes sur une même variable du système sont fournies par cette redondance de connaissances. A ce moment, on aura la possibilité de vérifier la cohérence de l'information obtenue par des tests de cohérence. Cette redondance d'informations se divise en deux : la *redondance physique* et la *redondance analytique*.

La *redondance physique* : Le principe de cette redondance est de disposer de plusieurs capteurs afin d'obtenir plusieurs informations sur une même variable. Pour obtenir deux mesures d'une même température, on double tout simplement le capteur de température. La redondance physique montre un désavantage majeur qui est le coût. En doublant le nombre de capteur ça revient à doubler le prix d'achat de ce dernier. De plus, les contraintes ergonomiques liées à l'installation de ces capteurs peuvent limiter leurs utilisations. Traditionnellement, la sûreté de fonctionnement du système dynamique est assurée en utilisant la redondance physique.

La *redondance analytique* : c'est la redondance à base de modèles. Par la notion de modèle on entend une reproduction formelle réalisant les mêmes performances que le système étudie [29].

Le *diagnostic* est défini comme une exploitation de toute la connaissance accessible existant sur le système. La connaissance peut être *globale* ou *instantanée*. La connaissance globale est l'ensemble des modes de fonctionnement sous lesquels un système peut exister. De la modélisation de ces modes de fonctionnement dépendra la stratégie du diagnostic. La connaissance instantanée est l'ensemble des éléments dont on dispose à un instant donné pour répondre à une décision.

Le diagnostic est la notion de base de l'observation du système dans le but de la surveillance. Il s'agit de vérifier un contrôle de cohérence entre les informations recueillies sur le système par observation et celles prédites par un modèle. Le principe de la connaissance s'articles sur les trois activités suivantes : La *détection*, la *localisation* et l'*identification* [30].

La *détection* permet de détecter un dysfonctionnement dans le système. Un dysfonctionnement se caractérise par l'éloignement des paramètres des procédés de ceux du modèle de bon fonctionnement. En présence de dysfonctionnement, la détection identifie clairement le défaut connu à priori.

La *localisation* permet de remonter à l'origine du défaut lorsqu'une panne a été détectée. En effet, il n'est pas rare de constater que la propagation d'un défaut dans le système physique génère à bon tour de nouveaux défauts. Ces pannes en cascade masquent la cause réelle de la panne empêchant toute action de maintenance.
L'*identification* détermine l'instant d'apparition du défaut, sa durée ainsi que son amplitude. La connaissance de l'amplitude de la défaillance permet de concevoir un système tolérant aux fautes ou auto adaptatif.

La *tolérance aux fautes* [22] est la capacité d'un système de continuer à fournir ses services spécifies en dépit de ses composants. Elle est basée sur les techniques de redondance qui sont l'utilisation et le déploiement efficace des ressources supplémentaires dans le temps et dans l'espace pour détecter, corriger, et masquer les effets des pannes.

Deux causes majeures sont à l'origine des défaillances des capteurs : leur *production* quasi industrielle conduisant à des fonctionnements plus graves d'une partie non négligeable d'entre eux, et des comportements malveillants à l'origine d'*intrusions* difficilement détectables.

Un premier défi sera donc d'identifier et de modéliser formellement les modes de défaillances des capteurs, puis de repenser les techniques de tolérance aux fautes à mettre en œuvre sur le terrain. En particulier les mécanismes traditionnels de détection de défaillances devront tenir compte des composantes, mobilité et autonomie en énergie en particulier dans le cas des réseaux de capteurs.

3.3 Problématique de la redondance

La télésurveillance est employée dans de nombreuses situations, généralement pour des raisons de sécurité: dans le cadre de la sécurité, au moyen de caméras spécialisées ou des capteurs à proximité voire noyés dans la chaussée permettent d'évaluer la densité du trafic, les ralentissements qui peuvent en découler, la présence de personnes sur les bandes d'arrêt d'urgences, etc. Pour la surveillance des machines : divers capteurs permettent d'évaluer l'état de la machine, ces informations peuvent alors être envoyées à un poste de surveillance.

L'épuisement de consommables, une anomalie de fonctionnement ou même un acte de malveillance serait alors détecté à distance ;dans le cadre de la prévention de la délinquance (avec notamment la vidéosurveillance);pour la surveillance de lieux sensibles (banques, centrales nucléaires, etc.) et d'habitations, afin de prévenir les intrusions, les cambriolages et les actes de vandalisme; dans le cadre de la télémédecine, et en particulier pour la surveillance des patients à distance ;pour la surveillance à distance des enfants et des personnes vulnérables [32].

Des caméras de surveillance permettent de visualiser et d'enregistrer les images du lieu à protéger en les transmettant par liaison vidéo, réseau IP ou sans fil à un moniteur vidéo ou informatique, généralement installé dans un centre de télésurveillance.

À l'autre bout de la chaîne, l'opérateur en télésurveillance, travaillant dans un centre de télésurveillance, réagit en fonction des consignes données : appel aux services compétents ou aux personnes concernées, intervention sur place, etc.

Dans le cas de la télésurveillance d'un local d'habitation ou d'une société, la transmission des alertes peut être envoyée au PC de télésurveillance soit par un transmetteur téléphonique classique relié à une ligne téléphonique RTC ou dégroupée, soit par un transmetteur téléphonique GSM utilisant une liaison GSM.

Dans le cas d'une capture vidéo, la redondance pose d'autres problèmes, traitement de filtrage pour diminuer la masse d'information, capacité de traitement, de stockage, et de bande passante dans un nœud, auto-organisation.

***Redondance des nœuds* :** Lorsqu'une panne survient dans un réseau ad hoc, différentes politiques de recouvrement peuvent être envisagées. Il existe trois stratégies de base qui sont : le recouvrement lien par lien, le recouvrement de bout en bout et le recouvrement par segment de route. Dans le premier type de recouvrement, en cas de panne, le trafic est basculé sur le lien alternatif, tandis que pour les deux autres, le trafic est redirigé soit sur une route entière secondaire soit sur un segment de route secondaire.

La mise en œuvre d'une politique de recouvrement dépend de la topologie du réseau. Dans les réseaux de faible densité, où la probabilité d'obtenir un grand nombre de routes disjointes est faible, la robustesse obtenue avec un recouvrement de bout en bout n'est pas très intéressante.

La redondance des nœuds est exploitée au sens de la couverture en RCSFs. Plusieurs nœuds potentiels sont candidats pour couvrir une même zone. Une partie de ces nœuds est laissée en mode actif et le reste des nœuds basculent en mode veille. Ceci permet de faire une auto-organisation en cas de changement de topologie du réseau afin de maximiser la durée de vie du réseau. On fait référence à la redondance spatiale dans le cas où un nœud capteur collecte une même grandeur physique.

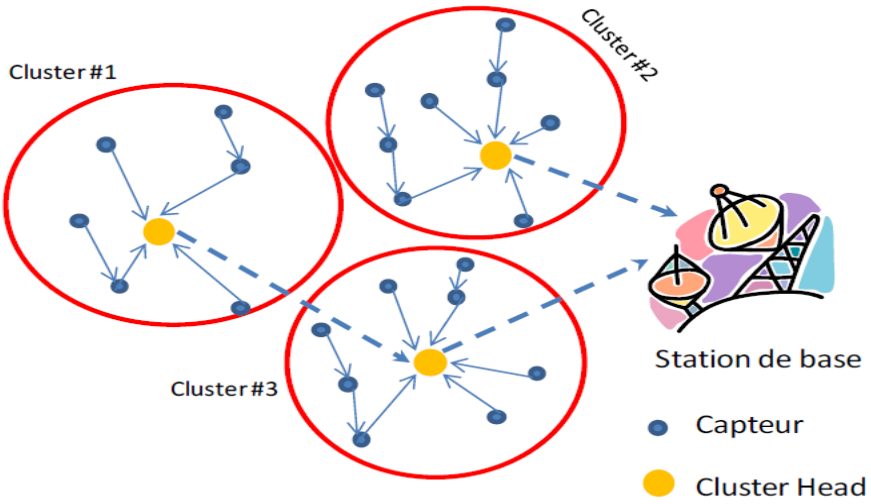

Figure 3.1 Technique de Clustering

La figure 3.1 illustre l'organisation d'un réseau sous forme de clusters. Chaque cluster regroupe un ensemble de nœuds. Le cluster est représenté par un nœud dit chef du cluster. Cette organisation en cluster peut être vue en mode mono-saut dans le cas où le chef du cluster est à un pas du Sink, et elle peut être utilisée en mode multi-saut dans le cas où le chef du cluster se trouve à plusieurs pas du Sink.

Le rôle d'un nœud peut être: représentant (Cluster Head), Liaison (Gateway), ou Ordinaire (simple membre); L'affectation du rôle se fait relativement à une zone (Cluster ou groupe) qui est défini par le 1-voisinage d'un capteur [3].

Redondance Temporelle **:** Les images dont une séquence se compose sont similaires les unes aux autres. Cette technique est utilisée en particulier pur l'estimation de mouvement. Elle est ainsi exploitée pour l'identification de la cohérence des données. Pour réduire la redondance temporelle un élément commun à plusieurs images consécutives n'est transmis qu'avec la première image. Pour les autres images, on ne transporte que sa position dans image.

Redondance des chemins et équilibrage : Les protocoles de routage *multipath* [33][38] assurent une protection de niveau routage (protection de route) ; contrairement aux protocoles de routage réactifs classiques (*unipath*), ils établissent deux ou plusieurs routes entre une source et une destination en fonction de la topologie du réseau. Une façon simple d'améliorer la probabilité de livraison des paquets est d'envoyer des copies multiples d'un même paquet sur des chemins différents. Cependant, cette approche n'est pas très efficace en termes de bande passante et de consommation d'énergie en raison de la grande quantité de messages inutiles transmis.

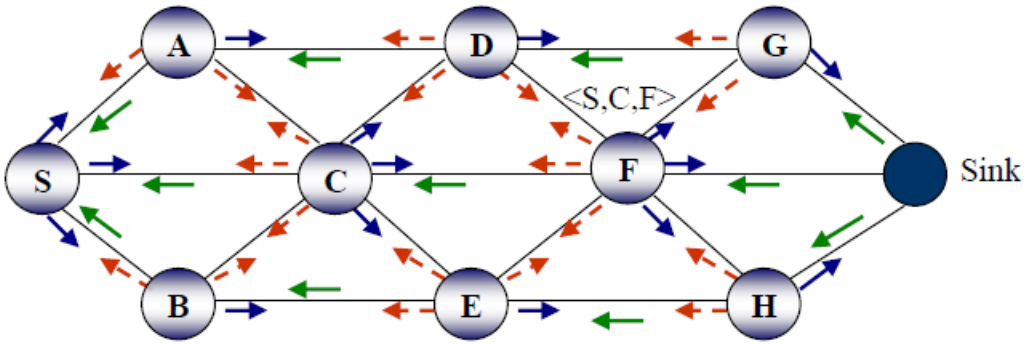

Figure 3.2 Routage Multipath

Une autre approche consiste à utiliser le routage *multipath* uniquement pour assurer une reprise rapide du trafic après une rupture de route. Ainsi, lors de la découverte de route, le protocole établira un ensemble de routes classées selon un critère spécifique. La meilleure route construite appelée route primaire sera utilisée pour envoyer le trafic jusqu'à ce qu'une panne (de liens ou de nœuds) survienne sur celle-ci. Après la détection de la panne, le trafic sera basculé sur la première route secondaire. L'intérêt de la redondance de route dépend de la probabilité qu'une route secondaire soit en bon état, lorsque la route primaire tombe en panne.

Un graphe est un dessin géométrique défini, par un ensemble de points appelés sommets ou nœuds reliés par des arêtes ou arcs. Un graphe planaire est un graphe dont il existe une représentation et où il n'y a pas d'intersection entre les arêtes. L'extraction des graphes planaires à partir des graphes non planaires fait appel à plusieurs techniques notamment :

- Graphe de voisins relatifs (RNG : Relative Neighborhood Graph) ;
- Graphe de Gabriel (GG : Gabriel Graph)
- Triangulation Delaunay (DT : Delaunay Triangulation).

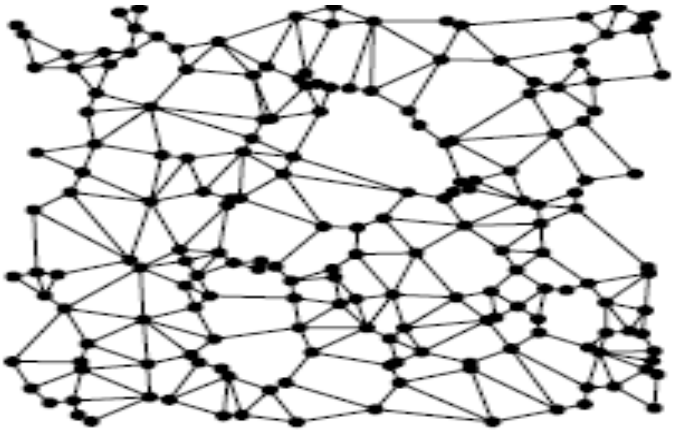

Figure 3.3 Graphe de voisins relatifs

Avec ces techniques le graphe planaire peut être déduit localement par chaque nœud en employant seulement la distance avec ses voisins distants. Ces techniques sont largement exploitées dans la partition naturelle du plan (espace), pour résoudre de nombreux problèmes de géométrie algorithmique, construction de maillage irréguliers, modèles biologiques et physiques : cellules d'un tissu, alvéoles des abeilles ; et la génération d'un réseau régulier à une topologie dynamique avec création et disparition d'espace.

3.4 Effets indésirables de la redondance

Interférences Radio et collision de Paquets : En radio, une interférence est la superposition de deux ou plusieurs ondes. Il est fréquent, pour les fréquences supérieures à quelques centaines de kilohertz, qu'une antenne de réception reçoive simultanément l'onde directe en provenance de l'émetteur et une (ou plusieurs) onde réfléchie par un obstacle. Les deux signaux vont se superposer et, en fonction de la différence de phase entre eux, voir leurs amplitudes s'additionner ou se soustraire. Ce genre d'interférence est responsable du fading, terme anglo-saxon désignant une variation plus ou moins rapide de l'amplitude du signal reçu [34]. Mais le phénomène ne se limite pas aux seules ondes radio.

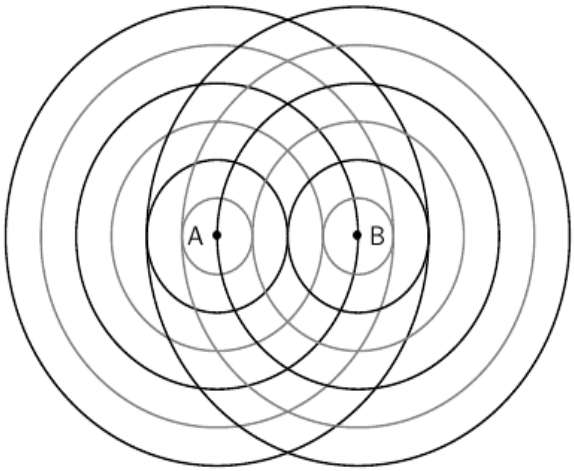

Figure 3.4 Interférences radios

Envoie de la même information plusieurs fois : La source diffuse son message à tous ses voisins. Chaque mobile retransmet le paquet reçu. La diffusion continue après réception par le destinataire. Tous les mobiles risquent de recevoir le message. Ce phénomène génère une consommation inutile de la bande passante, d'énergie, réceptions simultanées, et réceptions multiples en boucles infinies. La redondance physique présente des inconvénients en matière de coût de l'installation et en plus elle est encombrante. Alors que la redondance analytique, elle est synonyme aux problèmes de la complexité.

3.5 Approche distribuée pour la surveillance

L'approche centralisée pour la surveillance s'articule sur le principe qu'une seule entité surveille le réseau. Cette technique présente des inconvénients majeurs notamment la circulation d'un nombre important de messages sur le réseau, traitement compliqué et lent, trop d'énergie consommée, et une forte possibilité de panne au niveau du nœud central.

Comme une solution à ces problèmes, l'orientation vers une approche distribuée [36] pour la surveillance en exploitant la redondance des nœuds. Chaque nœud contribue localement à la surveillance, alors les messages sont échangés localement en nombre restreint, traitement simple et rapide et moins d'énergie consommée. En plus le réseau devient tolérant au pannes et étendre sa durée de vie.

Cette technique distribuée est établie ainsi, les *n* nœuds du RCSF sont déployés aléatoirement pour collecter l'information dans un champ déterminé et la transmettent au Sink. Initialement tous les capteurs sont à l'état actif; Une procédure d'organisation et d'affectation de rôle est déclenchée par le Sink (diffusion d'un message d'initialisation). Chaque nœud recevant ce message décide de prendre un rôle selon un algorithme d'élection.

La procédure d'élection de représentant permet de choisir parmi l'ensemble des nœuds d'une zone un nœud représentant. On trouve aussi un nœud liaison qui est un nœud appartenant à plusieurs zones en même temps (2 ou plus). Une zone (cluster) sera formée d'un représentant, quelques nœuds liaisons, et un nœud ordinaire (les autres endormis).

La gestion de la redondance est gérée par le représentant d'un groupe. Le choix du nœud ordinaire qui reste actif dans une zone se fait en fonction de son énergie. Le choix du nœud liaison qui reste actif se base sur le nombre de zones auxquelles appartient ce dernier.

Les nœuds d'un groupe échangent périodiquement des messages *Hello* pour détecter le bon fonctionnement du réseau. Tout nœud actif recevant un *Hello* de son représentant répond en fournissant son identificateur, son rôle et son niveau d'énergie. En cas de non réponse, il est déclaré défaillant, le représentant réveille un autre si possible sinon, une réorganisation des groupes est déclenchée. Dans le cas où un nœud non représentant ne reçoit pas périodiquement le message *Hello* ; il procède par envoyer un message Hello au représentant ; si ce dernier ne répond pas il est déclaré défaillant. Une procédure d'élection de représentant par le nœud détecteur de panne.

Un mauvais comportement (*Misbehaviour*) [23] dans un réseau étant défini comme l'arrivée potentielle d'événements qui peuvent provoquer des disfonctionnements. On trouve le cas des nœuds (*Selfishnodes*) qui refusent de transférer les paquets vers les autres nœuds pour préserver ses ressources. On trouve aussi des nœuds ne participent pas lorsque la procédure de découverte de la route est exécutée. Ces nœuds refusent de

faire passer les paquets pour les autres nœuds (*forwarderles*). La présence d'attaque est envisageable dans un réseau. Elle est définie comme un ensemble de techniques informatiques opérées par des nœuds attaquants (*Maliciousnodes*) visant à causer des dommages à un réseau en exploitant les failles de ce dernier.

La nature des RCSFs favorise les traitements distribués de la redondance. Ce traitement distribué permet d'équilibrer les charges, diminuer le nombre de messages, passer du traitement en local à celui global de la supervision, efficacité énergétique et tolérance aux pannes. La redondance favorise l'exploitation de la vidéosurveillance, la localisation, la détection d'intrusion, et la réduction du cout d'accès aux services. Elle assure aussi la robustesse, la réactivité et l'adaptabilité du réseau aux différentes circonstances.

La gestion autonome « *Self-Management* » du RCSF est un défi majeur. Il nécessite de concevoir des solutions efficaces qui permettent aux réseaux de capteurs de se gérer d'une manière autonome sans l'intervention d'un superviseur. Ceci nécessite donc que le réseau possède des fonctions d'auto-configuration, d'autoréparation, d'autoprotection et d'auto-optimisation. Parmi les solutions actuelles déployées, on trouve l'intégration des systèmes multi-agents [36][37].

3.6Travaux existants

La surveillance par réseau de capteurs en utilisant la redondance a été un champ fertile pour les recherches scientifiques. L'auteur dans sa thèse [11] a traité le problème de la sociabilité par l'application de la redondance en tenant en compte le problème de la surveillance par réseau de capteur sans fil. Ceci dans le cas d'un nœud corrompu ou endommagé (pour une raison énergétique ou autre), le réseau doit être capable de prendre en considération cette modification tout en assurant une qualité de service égale. La redondance des capteurs peut être un moyen d'assurer cette fonction. La notion de sociabilité est alors utilisée pour dire que l'architecture et les protocoles de communications du réseau doivent s'adapter et prendre en compte l'entrée ou la perte de nœuds dans le réseau.

L'auteur dans sa thèse [6] a proposé une approche systématique basé sur la redondance, capable de concevoir le réseau de capteurs, au moindre coût, d'identifier les variables clés d'un procédé sans dépasser une certaine imprécision sur les mesures, et de générer un système de mesures valides même si un des capteurs tombe en panne. Cette méthode se base sur un modèle linéaire dérivant directement d'un modèle de validation de données non linéaire. Un algorithme génétique est utilisé pour choisir les types de capteurs et leur position dans le procédé.

L'auteur dans sa thèse [5] a proposé un protocole de routage basé sur l'agrégation de données pour résoudre le problème de la redondance. Car les capteurs proches peuvent capter la même donnée en transmettant ces données redondantes aux nœuds relais, elles peuvent être une source de congestion.

Dans [10] les auteurs ont traité le problème de la redondance en proposant un mécanisme d'adressage logique dans un voisinage visant à améliorer la robustesse à tout type de protocole unicast. Cette technique se base sur la notion de relai implicite, elle utilise des informations topologiques du réseau.

D'autres travaux exploitent la redondance en proposant un protocole d'ordonnancement d'activité dans les réseaux de capteurs. Ce protocole vise à constituer un sous-ensemble de nœuds devant être actifs pour une période donnée, permettant aux autres de passer dans un mode passif moins consommateur d'énergie. La décision d'activité peut se faire selon divers critères. La couverture de surface multiple, ou *k*-couverture; est considérée alors tout point physique de la zone de déploiement doit être couvert par au moins *k* nœuds actifs.

D'autres propositions évoquent l'exploitation de la redondance dans les techniques de codage. Ces codes consistent en une redondance d'informations permettant de retrouver les données corrompues. Cette redondance s'exprime par des taux d'encodage, qui indiquent la proportion d'informations uniques sur la somme d'informations totales transmises.

Dans les travaux de laboratoire LIUPPA [39] en France un modèle de surveillance à base du réseau de capteur vidéo sans est proposé en s'articulant sur la redondance. Il est défini ainsi, un réseau de capteur (RdC) vidéo sans-fils consiste en un ensemble de nœuds autonomes dotés d'une petite caméra embarquée. Ce type de réseau permet de déployer un grand nombre d'applications et dans cet article nous nous intéressons plus particulièrement aux applications de surveillance.

Les applications sur RdC qui sont orientées surveillance ont des besoins spécifiques du fait de leur criticité. Par exemple, la qualité des images capturées et transmises doit être en adéquation avec les besoins et objectifs de l'application. De telles infrastructures de surveillance perdent très rapidement leurs intérêts si les scènes importantes ne sont pas correctement capturées.

Un aspect important en surveillance est la couverture et son maintien. Ce problème a été largement étudié dans les systèmes multi-robots et les RdCs de type scalaire en considérant une capacité de capture omnidirectionnelle. Ainsi deux nœuds sont considérés comme redondants s'ils sont proches l'un de l'autre. Dans les RdCs vidéo, les caméras possèdent un champ de vision (CdV) et éventuellement des capacités de zoom. Deux nœuds peuvent ainsi être redondants même s'ils sont relativement éloignés l'un de l'autre. Parfois plusieurs vues sont souhaitables pour résoudre les ambiguïtés, parfois les nœuds éloignés peuvent fournir des informations mieux exploitables en fonction des conditions météo par exemple.

Un autre aspect très important est celui de la gestion de l'énergie. La rareté de cette ressource va avoir un impact très fort sur la couverture puisqu'il n'est pas réaliste que tous les nœuds puissent être actifs en même temps. Lorsque le déploiement est aléatoire, il peut y avoir une grande redondance entre les nœuds et une approche couramment utilisée est de définir un sous-ensemble de nœuds qui seront actifs pendant que d'autres seront inactifs.

Le résultat est un ordonnancement de l'activité des nœuds qui maintient la couverture et la connectivité de la zone à surveiller. De plus, il est souhaitable de pouvoir définir plusieurs niveaux d'activité qui peuvent correspondre au nombre d'images qui seront capturées par unité de temps. Par exemple, certaines applications se focalisent sur la surveillance de la zone frontière plutôt que de la zone intérieure. Dans ce cas, les nœuds se situant à la frontière doivent capturer les images à un rythme plus soutenu que ceux se situant à l'intérieur, qui, à la rigueur, peuvent même se mettre en veille.

Disposer de plusieurs niveaux d'activité est aussi nécessaire car les applications de surveillance comme la détection d'intrusion doivent pouvoir être opérationnelles sur le long terme puisque personne ne sait quand une intrusion se produira.

En ce qui concerne les nœuds vidéo qui sont l'objet de cet article, la capacité à avoir plusieurs niveaux d'activité est encore plus indispensable que dans les réseaux de capteurs scalaires traditionnels (température, pression,. . .) car capturer et transmettre des images consomme beaucoup plus d'énergie.

Couverture et ordonnancement des nœuds vidéo :

Le problème de la couverture dans les réseaux de capteurs vidéo est défini en deux catégories comme suit :

- Couverture des cibles prédéterminées, qui consiste à trouver un sous-ensemble de nœuds connexes et qui assure la surveillance d'un ensemble de cibles dont la position est connue à priori.
- Couverture d'une zone, qui consiste à trouver un sous-ensemble de nœuds connexes et qui assure la surveillance de toute la zone de déploiement.

L'utilisation d'un modèle directionnel considère qu'un nœud vidéo peut ajuster la direction de son CdV [14]. L'idée est de trouver un sous-ensemble minimal de directions parmi les nœuds redondants qui couvre le plus grand nombre de cibles.

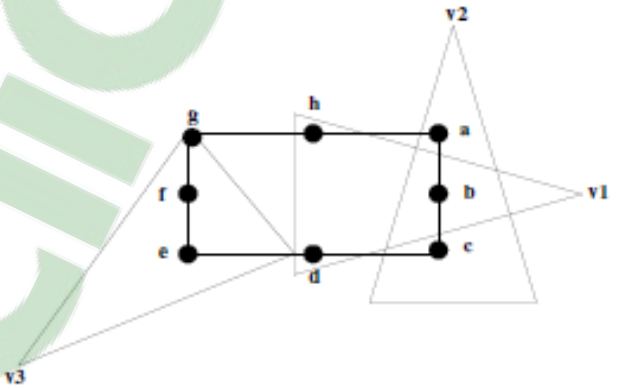

Figure 3.5 Modèle directionnel d'un nœud vidéo

Autrement, ordonner les nœuds dans des sous-ensembles non-disjoints sachant que chacun d'eux couvre la totalité des cibles. Le problème de la couverture d'une zone 2D se base sur l'étude du déploiement des nœuds afin de réduire le taux de chevauchement (zones couvertes plusieurs fois par plusieurs capteurs). Cette réduction peut être basée sur un modèle probabiliste qui précise le pourcentage de la couverture demandée. Dans d'autre situation les caméras pouvant tourner afin d'augmenter la surface de surveillance.

Device Type	Frequency Band	Number of Channels	Channel Spacing	Data Rate	Modulation Type
IEEE 802.11b	2.4 GHz	11 (DSSS)	5 MHz	1 Mbit/s	BPSK
	⋮	⋮	⋮	2 Mbit/s	QPSK
	⋮	⋮	⋮	5.5 Mbit/s	CCK
	⋮	⋮	⋮	11 Mbit/s	⋮
IEEE 802.15.4	868 MHz	1	–	20 kbit/s	BPSK
	915 MHz	10	5 MHz	40 kbit/s	⋮
	2.4 GHz	16	⋮	250 kbit/s	OQPSK
Bluetooth1.2 + Basic Data Rate	2.4 GHz	79 (FHSS)	1 MHz	1 Mbit/s	GFSK
Bluetooth2.0	⋮	⋮	⋮	2 Mbit/s	$\frac{\pi}{4}$DQPSK
Bluetooth2.0 + Enhanced Data Rate	⋮	⋮	⋮	3 Mbit/s	8 – DPSK
MICA2	300 – 900 MHz	4/50	⋮	38.4 kbit/s	FSK
MICAz	2.4 GHz	16/83	5/1 MHz	250 kbit/s	OQPSK

Tableau 3.1 Tableau comparatif entre différents capteurs multimédia

Le tableau 3.1 donne un aperçu sur les différents capteurs multimédia supportés par les normes IEEE 802.11b, IEEE 802.15.4, Bluetooth1.2, Bluetooth2.0, Mica2 et MicaZ.

Device Name	Manufacturer	Processor	Memory	Multimedia Support	Wireless
Stargate[2]	Crossbow	Intel PXA-255 Xscale processor at 400 MHz	32 MByte Flash 64 MByte RAM	High computation power, embedded linux OS	802.11 Compact Flash, 802.15.4 through MICA2/z interface
Imote2[3]	Intel	32 – bit PXA271 Marvell processor at 13 – 416 MHz	32 KByte Flash 64 KByte RAM	MMX co-processor for audio/ video imaging acceleration	Integrated 802.15.4
CMUcam3 [18]	CMU	32 – bit NXP LPC2106 microcontroller at 60 MHz	128 KByte Flash 64 KByte RAM	On-board cc3-open source image processing library	–
MeshEye [19]	Stanford Univ.	32 – bit ARM7TDMI RISC processor at 55 MHz	128 KByte Flash 64 KByte RAM	Multiple resolution support	–
WiCa [20]	XNP and Philips Research	IC3D Xetal II processor at 84 MHz	10 Mbit RAM	Dedicated parallel processor, multiple camera modules	–
Cyclops [21]	Agilent Technologies	8 – bit ATMEL ATmega128L microcontroller	512 KByte Flash 512 KByte RAM	On-board image processing, low power, cost and size	–

Tableau 3.2 Caractéristiques pysiques des différents capteurs multimédia

Le tableau 3.2 étale les différentes caractéristiques physiques de ces capteurs par constructeur notamment la vitesse de traitement, la capacité mémoire et le système d'exploitation supporté.

Chaque nœud vidéo doit définir plusieurs sous-ensembles non disjoints parmi ses voisins, sachant que chaque sous-ensemble couvre la totalité de la surface de son CdV. Cependant, un nœud peut décider d'être actif ou inactif selon l'activité de ses voisins.

3.7 Techniques de la redondance appliquées sur l'image

Les techniques de la redondance sont largement utilisées dans les réseaux de capteurs image sans fil pour des fins de la compression [40]. Le volume d'information associé à une image est de plusieurs ordres de grandeurs supérieur à une information scalaire simple, et cela change tout. En effet, les données fournies par un capteur traditionnel sont codées généralement sur quelques bits (sur la carte d'acquisition MTS 400 de Crossbow par exemple, les valeurs de température et l'humidité sont fournies sur 14 bits par le convertisseur analogique/numérique, les valeurs de luminosité sur 12 bits). Par conséquent, elles peuvent être transportées sur un seul paquet et la compression des données n'a donc pas vraiment d'intérêt.

3.7.1 Notions de base sur l'image

Une image numérique est une matrice de pixels. Chaque pixel a de composantes spatiales dans le plan réel. La résolution d'une image est définie par le nombre de pixels par unité de longueur de la structure à numériser (classiquement en dpi (dots per inches) ou ppp (points par pouce)).

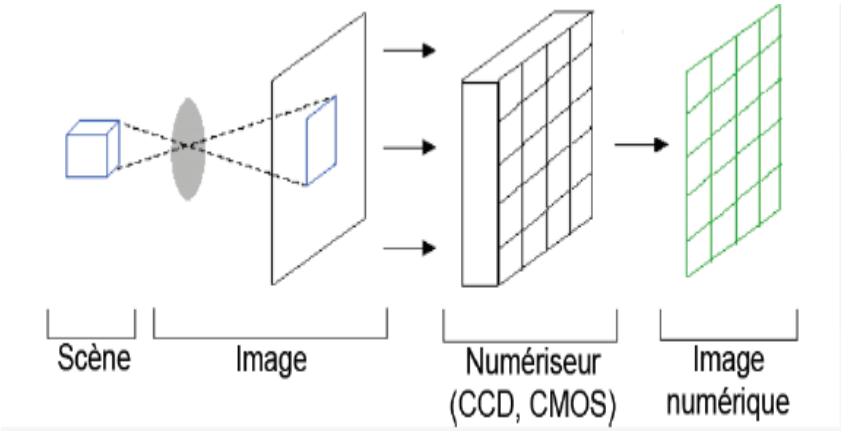

Figure 3.6 Acquisition d'une image

Plus le nombre de pixels est élevé par unité de longueur de la structure à numériser, plus la quantité d'information qui décrit cette structure est importante et plus la résolution est élevée.

Une image avant numérisation est un signal 2D continu (même si elle correspond souvent à une scène 3D...). Une image numérique est une matrice de nombres représentant le signal continu.

Une image peut donc être vue comme une fonction [16] :

$$I : S \rightarrow \Omega$$
$$(i,j) \rightarrow x = I(i,j)$$

Dans le domaine continu, une image est représentée ainsi :

$$S = [0, nl - 1] * [0, nc - 1]$$
$$\Omega = [0, ValMax]$$

Dans le domaine discret, elle est représentée ainsi :

$$S = \{0, 1, ..., nl - 1\} * \{0, 1, ..., nc - 1\}$$
$$\Omega = 0, 1, ..., 255$$

3.7.2 Prétraitement sur l'image

Le traitement, souvent appelé *prétraitement*, regroupe toutes les techniques visant à améliorer la qualité d'une image. De ce fait, la donnée de départ est l'image initiale et le résultat est également une image. L'idéal est d'obtenir un résultat sans bruit. La qualité d'une image n'est pas forcément la même pour un ordinateur ou pour un opérateur humain. C'est la raison pour laquelle les techniques ne sont pas les mêmes.

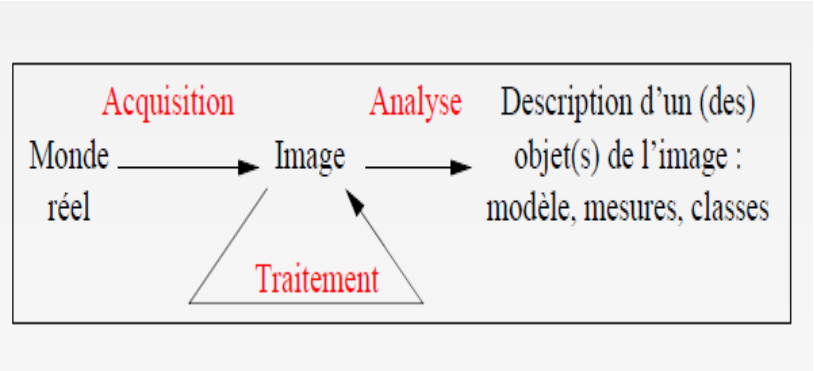

Figure 3.7 Traitement d'une image

La notion de qualité est une notion très subjective, assujettie à la réalisation d'un objectif. La qualité d'une image n'est pas forcément la même pour un ordinateur ou pour un opérateur humain.

L'échantillonnage est une étape fondamentale qui doit tenir compte du contenu informationnel pertinent de l'image à analyser. Avec un échantillonnage adapté, l'image numérique fait apparaître des structures conformes à l'information présente dans l'image. Comme pour l'échantillonnage, il existe des règles pour déterminer la bonne quantification (le bon nombre de bits) pour coder les images numériques. La quantification peut également faire apparaître des distorsions dans les images.

Les capacités de vision de l'être humain étant limitées, il est indispensable d'adapter la dynamique de l'image à notre vision.

Le prétraitement suit les étapes suivantes [41]:

- *Restauration* : La restauration a pour but d'inverser l'effet du phénomène dégradant. Il s'agit donc de produire une image la plus proche de la réalité physique de la scène observée. Le plus souvent, cette étape est la première dans la chaîne de traitements constituant un système de vision.
- *Amélioration* : L'amélioration a pour but de satisfaire l'œil de l'observateur humain. C'est pourquoi l'image produite peut être différente de la réalité. Cette amélioration peut servir dans un premier temps à faciliter la visualisation de l'image sur un écran d'ordinateur. Dans les deux cas, la qualité a été accrue.
- *Compression* : On classe les techniques de compression par extension du fichier informatique. Il s'agit là de faciliter le traitement et surtout le stockage des images par une réduction adéquate de leur volume d'information. On perd ou on gagne une caractéristique optique.
- *Segmentation* : Il existe deux grandes catégories de segmentations : la segmentation de région et la segmentation de contour. Les pixels présentant une même caractéristique sont décrits par un niveau de gris compris dans un certain intervalle ou dérivée seconde supérieure à un certain seuil.

3.7.3 Filtrage et restauration

Les techniques d'*amélioration* des images numériques, pour augmenter la qualité de leur rendu visuel, ou pour faciliter leur analyse, cherchent à atténuer, sinon supprimer une certaine *dégradation*. Celle-ci n'est pas forcément connue *a priori*, mais elle peut parfois être estimée *a posteriori*. On distingue:

- les dégradations liées au *bruit* : $g(x) = f(x)+b(x)$ ou $g(x) = f(x)b(x)$ liées au capteur, à la quantification, à la transmission. Elles se traitent en tirant parti des informations locales par le *filtrage*. Par différenciation, les techniques de filtrage permettent en outre de calculer ou amplifier les contrastes locaux.

- les dégradations *convolutives* : $g(x) = f(x)*b(x)$ liées à un mouvement du capteur ou un défaut de mise au point. Elles se traitent en inversant un opérateur linéaire, donc supposé connu : ce sont les techniques dites de *restauration*.

Les filtres de lissage sont des opérateurs qui éliminent des éléments perturbateurs / non significatifs dans les images numériques, soit pour améliorer leur visualisation, soit pour les simplifier en but d'un traitement postérieur [42]:

Filtrage dans l'espace de Fourrier :

- Filtrage passe-bas : Il représente la multiplication dans le domaine fréquentiel par une fonction porte.
- Filtrage coupe-bande : Il représente la multiplication dans le domaine fréquentiel par une *fonction bande complémentaire,* fonction indicatrice de l'ensemble

Filtrage dans l'espace fréquentiel :

- Filtre moyenneur
- Filtre gaussien
- Filtre exponentiel

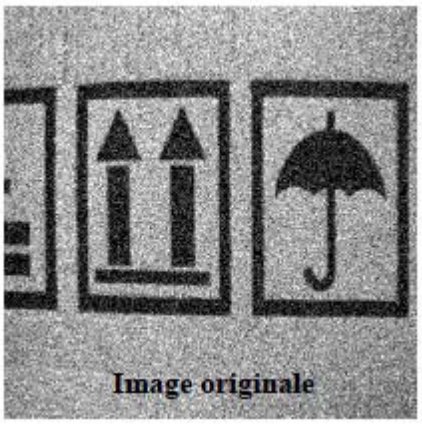

Figure 3.8 Image originale

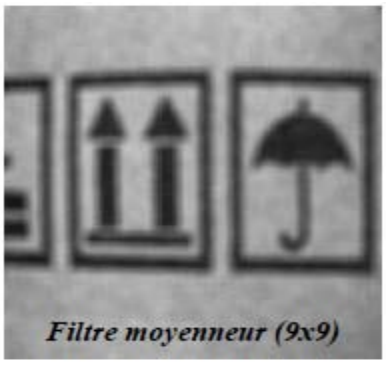

Figure 3.9 Filtre moyenneur sur image originale

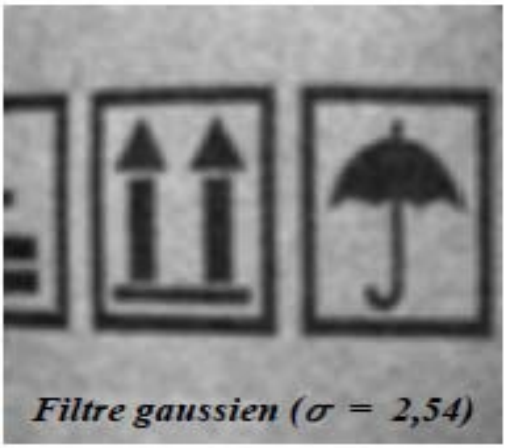

Figure 3.10 Filtre gaussien sur image originale

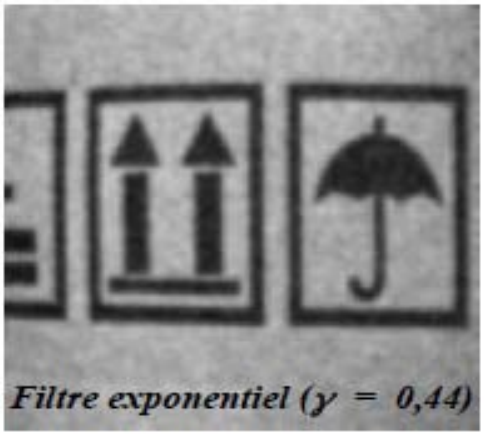

Figure 3.11 Filtre exponentiel sur image originale

L'analyse d'images regroupe plusieurs disciplines que l'on classe en deux catégories :

- Les processus de bas-niveaux, qui nécessitent très peu d'informations sur le contenu des images. Il s'agit ici des processus de filtrage, d'amélioration et de restauration d'images, processus du *traitement d'images*, ainsi que d'extraction d'indices.
- Les processus de haut-niveaux, qui fonctionnent en aval de ceux de bas niveaux, et qui peuvent nécessiter des informations sur le contenu des images. Il s'agit de la reconstruction tridimensionnelle, la reconnaissance de formes, les processus cognitifs de façon générale.

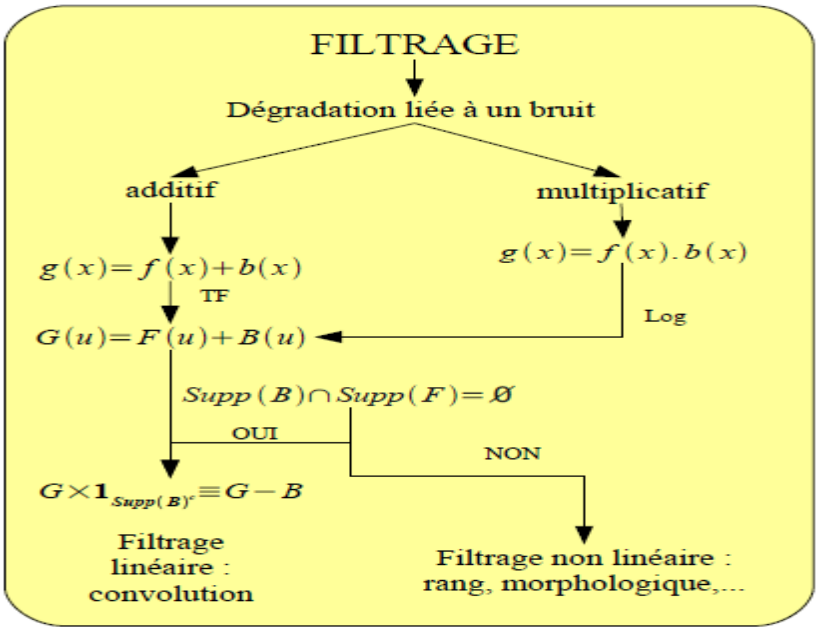

Figure 3.12 Processus de filtrage

3.7.4 Compression d'image

Le principe est toujours de détecter des corrélations dans les données. Ces corrélations sont en quelque sorte des informations redondantes, qui peuvent être représentées plus économiquement. Dans les images, des corrélations spatiales sont cherchées : des formes qui se répètent, des motifs qui peuvent être décrits par quelques coefficients d'une transformée.

L'intérêt d'utiliser la compression est de réduire au maximum la chaîne de données du bitmap qui peut rapidement devenir très longue. Il existe plusieurs types de compression, c'est à dire qu'il existe plusieurs manières de réécrire les données bitmap pour qu'elles prennent moins de place. Les méthodes de compression et de codage réduisent le nombre de bits par pixel à stocker ou à transmettre, en exploitant la redondance des informations dans l'image.

Les méthodes de compression opèrent différemment. Elles sont classées de la manière suivante : non-destructrices ou destructrices.

Compression non-destructrices : Elles ne modifient en rien l'apparence des images. Elles modifient uniquement le codage des couleurs. Elles permettent de retrouver exactement les pixels de l'image numérique originale. On cite:

- RLE *(Run Length Encoding)*
- LZW (Lempel-Ziv-Welch) ou LZ77
- Codage de HUFFMAN

Compression destructrices : Ces méthodes permettent de retrouver une approximation de l'image numérique. Les pertes de qualité sont généralement invisibles à l'œil nu mais cela dépend aussi de l'image.

- Transformation discrète en cosinus (TDC)
- Fractale
- Ondelettes

La méthode de compression dépend intrinsèquement du type de données à compresser : on ne compresse pas de la même façon une image qu'un fichier audio. Elle cherche à éviter de coder des informations redondantes dans l'espace, le temps ou l'espace des couleurs.

Un compresseur utilise un algorithme qui sert à optimiser les données en utilisant des considérations propres au type de données à compresser. Un décompresseur est donc nécessaire pour reconstruire les données originelles grâce à l'algorithme inverse de celui utilisé pour la compression.

La compression peut se définir par :

- Quotient de compression : rapport des nombres de bits de l'image compressée et d'origine.
- Taux de compression. Souvent utilisé. C'est l'inverse du quotient de compression.
- Gain de compression. Complément à un (1) du taux de compression.

La compression peut être symétrique ou non symétrique. Elle dite symétrique si la même méthode est utilisée pour compresser et décompresser l'information : il faut donc la même quantité de travail pour chacune de ces opérations. Ce type de compression est généralement utilisé dans les transmissions de données. La compression asymétrique demande plus de travail pour l'une des deux opérations. On recherche souvent des algorithmes pour lesquels la compression est plus lente que la décompression. Des algorithmes plus rapides en compression qu'en décompression peuvent être utiles pour obtenir des fichiers compacts auxquels on accède peu.

Figure 3.13 Image avec perte de données

Une image est au contraire représentée sur plusieurs milliers d'octets et donc son transport nécessite typiquement plus d'un paquet. La compression des données d'image est une nécessité pour réduire le nombre de paquets à émettre, d'autant qu'en pratique, le nombre de paquets générés par une image est très grand car la contrainte énergétique propre aux réseaux de capteurs impose de construire de paquets de petite taille.

Figure 3.14 Image sans perte de données

La raison vient du fait que transmettre des paquets de grande taille, bien que cela réduit la surcharge de trafic relative aux entêtes des protocoles, augmente la probabilité d'erreurs de transmission dues aux imperfections de la liaison radio.

• Redondances Spatiales (codage intra-image) : Elle est utilisée dans les codages prédictifs.
• Redondances temporelles (codage inter-image) : Elle est utilisée dans l'estimation et compensation de mouvement.
• Redondances statistiques : Elle est utilisée dans le codage en entropie (Huffman, arithmétique) [43].
• Redondances psycho-visuelle : Elle est utilisée dans le sous-échantillonnage des couleurs, dans la transformation et dans la quantification.

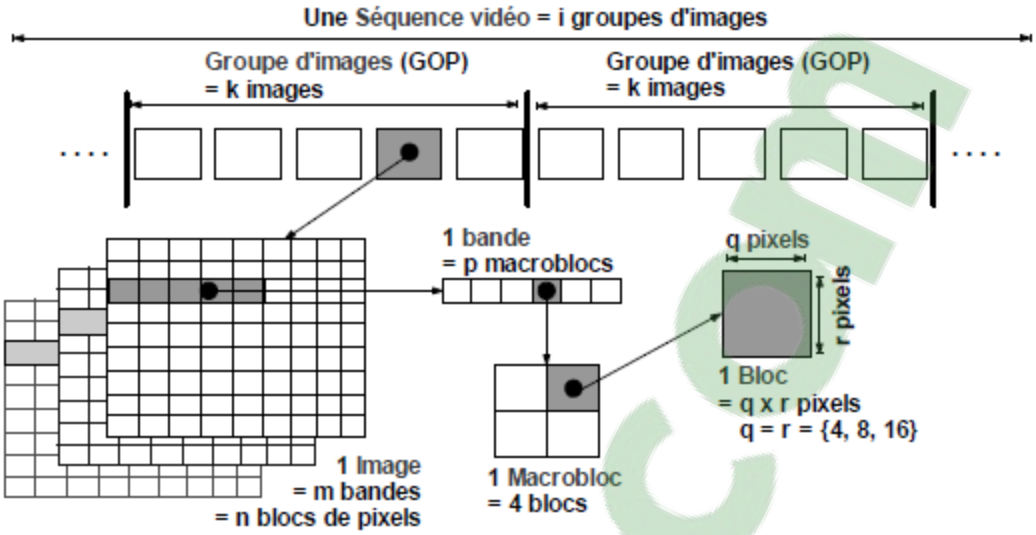

Figure 3.15 Structure des flux video numerique

Le schéma de principe d'un encodeur d'image souvent utilisé pour décrire le fonctionnement des algorithmes de compression est celui présenté dans la Figure 3.15.

Figure 3.16 Schema général de compression avec perte.

La première étape est une transformation, ayant pour but de réaliser un changement de l'espace de représentation du domaine spatial. L'étape de quantification réalise une réduction de nombre de valeurs représentées, et fait partie uniquement des algorithmes irréversibles. Le codage permet de passer d'une représentation de données vers une autre sans perte sur les valeurs quantifiées.

3.8 Conclusion

La redondance d'informations est très sollicitée dans le domaine de la surveillance. La comparaison des grandeurs redondantes permet de décider si une défaillance est présente ou non. En connaissance de ces informations, la phase de détection d'anomalie devient triviale. Avec la redondance le système répond convenablement à la tolérance aux fautes. Les réseaux de capteurs sans fil dédiés à la surveillance se basent pleinement sur ce principe pour accomplir correctement ces objectifs.

Avec l'application des techniques de la redondance pour optimiser la collecte et le transfert des images dans la zone de déploiement de réseau de capteurs sans fil, de une

nouvelles méthodes de compression d'image satisfaisant à l'une des contraintes induite par les réseaux de capteurs sans fil sont proposées. Cette compression d'image permet de réduire la taille des informations transmises tout en offrant une bonne qualité d'image et une faible consommation en énergie.

Le prochain chapitre est consacré à nos contributions et suggestions dans le domaine de la vidéosurveillance à base de réseau de capteurs image sans fil.

Chapitre 4 : Contributions et résultats

4.1 Introduction

Les applications sur les réseaux de capteurs image sans fil qui sont orientées surveillance ont des besoins spécifiques du fait de leur criticité. Les images capturées et transmises doivent être en adéquation avec les besoins et les objectifs de l'application, si les scènes importantes ne sont pas correctement capturées de telle application perde ses intérêts. Un autre aspect très important est celui de la gestion de l'énergie car les applications sur les réseaux de capteurs image sans fil sont particulièrement gourmandes en énergie puisque les nœuds engagent des volumes de données très largement supérieurs aux mesures scalaires classiques.

Au delà des défis traditionnels des réseaux de capteurs sans fil les applications des réseaux de capteurs d'images posent des défis particuliers, notamment, des protocoles de transmission et des algorithmes de compression d'images du monde réel, temps réel, et sécurité et confidentialité.

Lors de la détection d'une intrusion à base d'un réseau de capteurs image sans fil dédié à une application de surveillance de haute criticité les messages d'alertes sont diffusés par inondation ceci provoque une implosion. Par conséquent, le nœud-capteur va devoir générer beaucoup de paquets pour transmettre l'image entière, et donc consommer beaucoup d'énergie. La rareté de cette ressource va avoir un impact très fort sur la couverture et par la suite sur la durée de vie du réseau.

L'objectif de cette thèse est de traiter la problématique de la diffusion des messages d'alertes pour réduire de manière considérable le nombre de message d'alerte circulant dans le réseau sans compromettre les objectifs de la surveillance. Notre contribution dans ce domaine est de proposer un algorithme dit *selectiveFoV* permettant la gestion de la diffusion d'alerte suite à la détection d'intrusion en se basant sur la propriété champ de vision de la caméra (field of view : FoV) et sur la redondance des nœuds capteurs. La propagation des alertes sera réduite vers le sous ensemble des nœuds capteurs qui sont dans le champ de vision du capteur ayant détecté l'intrusion.

Notre contribution est testée sur le modèle développé par l'université de Pau, France ; sous la plate forme de simulation Omnetpp/Castalia. Les résultats de simulation de notre algorithme apportent une valeur ajoutée dans le domaine de la gestion des alertes dans un réseau de capteurs image sans fil dédié à une mission de surveillance.

Ce présent chapitre présente l'environnement Omnetpp/Castalia utilisé dans nos simulations ; ensuite, il expose le modèle *Wireless Image Sensors Network* (WISN) ; puis, il étale nos contributions et la discussion des résultats trouvés.

4.2 Modèle du réseau de capteurs image sans fil

Le modèle WISN (Wireless Image SensorsNetwork) développé par le LIUPPA [44] a subi beaucoup d'évolutions. Il passait par plusieurs versions. Au départ, il a été conçu sous le simulateur Omnetpp, puis une extension de ce modèle a été développée pour fonctionner sous le simulateur Castalia. Cette dernière version du modèle permet d'exploiter les outils de la gestion de l'énergie fournis par le simulateur. La gestion de l'énergie sur toutes les couches de la pile protocolaire est effectuée d'une façon très efficace par rapport au simulateur Omnetpp. En plus, Castalia simule le routage d'une façon très réaliste par rapport au simulateur Omnetpp, tous les paquets passent par un module spécialisée dit *routingModule*.

Dans ce modèle, la zone de surveillance d'un nœud image *v* est généralement représentée par son champ de vision (field of view : FoV). Un modèle 2D est considéré qui définit le capteur image par le 4-uplet *v*(P, Rs, V, alpha) ; où P représente la position, Rs le rayon de couverture, V le vecteur de direction de la camera qui sera en mode capture image, et alpha le demi-angle de vision du capteur image. La figure 4.1 illustre ce modèle [45].

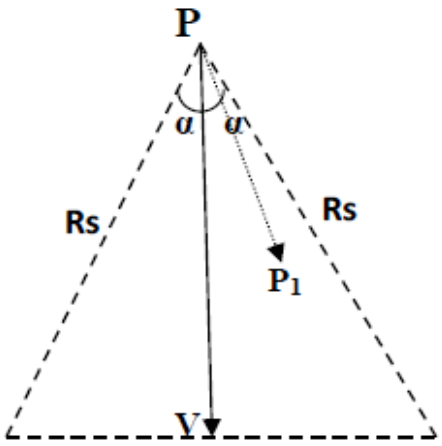

Figure 4.1 Champ de vision du camera

Chaque nœud doit assurer sa propre couverture indépendamment des autres. Un nœud *v* couvre également une surface triangulaire grâce à son champ de capture. Cependant son objectif est d'assurer tant qu'il est vivant la couverture de cette surface soit par lui-même soit par les nœuds redondants comme il est montré dans la figure 4.2.

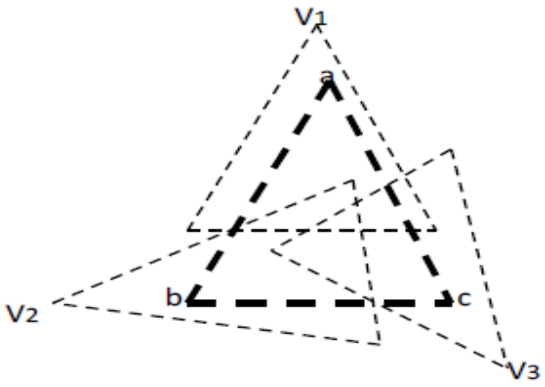

Figure 4.2 Couverture du champ de vision

Cette surface triangulaire représente le champ de vision de la camera (FoV) d'un nœud capteur image. Cette surface est couverte par un sous ensemble de nœud capteur. On peut trouver plusieurs sous ensembles redondants qui couvrent le même champ de vision. Ceci est noté comme élément couvrant redondant.

Lors du déploiement du réseau chaque nœud cherche à trouver ses éléments couvrants alors il diffuse sa position P et sa direction à ses voisins et reçoit leurs informations. Une fois ces éléments couvrants sont établis, chaque nœud décide d'être actif ou non selon l'activité de ses voisins et son niveau d'énergie. Il commence à ordonner ses ensembles couvrants selon leur cardinalités, en donnant la priorité à ceux qui contiennent le moins d'éléments. Dans le cas où deux ou plusieurs ensembles ont le même cardinal, ils seront classés selon leurs niveaux d'énergie. Un nœud *v* reçoit les messages d'activité de ses voisins et teste si un de ses ensembles couvrants est satisfait ou non. Si il trouve que l'un de ses couvrant est actif, ce nœud *v* s'endort et diffuse sa décision à ses voisins. D'un autre côté si aucun de ces couvrants n'est satisfait, il décide de rester actif et diffuse également sa décision. La technique de calcul des ensembles couvrants *CoverSet* est donnée en détail dans les travaux [44] et [46]. La technique de l'ordonnancement des nœuds est donnée par l'algorithme suivant :

v est actif
v ordonne ses ensembles couvrants $Co_i(v) \in Co(v)$ i = 1, 2, ...$|Co(v)|$
i ← 1
Tantque i ≤ $|Co(v)|$ **faire**
v commence par l'ensemble couvrant ayant la plus grande priorité´e $Co_i(v)$
Si voisin *v'* décide d'être inactif **alors**
Si $v' / \in Co_i(v)$ **alors**
continue avec $Co_i(v)$
Finsi
sinon
v choisit l'ensemble couvrant suivant $Co_{i+1}(v)$
i ← i + 1
Finsi
Si *v'* décide d'être actif **alors**
Si $v' \in Co_i(v)$ **alors**
continue avec $Co_i(v)$
Finsi
finsi
Si ∀*v'*, $v' \in Co_i(v)$, *v'* est actif **alors**
v devient inactif et diffuse sa décision à ses voisins
Finsi

Fin tantque
Si aucun $Co_i(v)$ n'est satisfait **alors**
v reste en mode actif et diffuse sa décision à ses voisins
Finsi

Une application ayant pour but la détection d'intrusion doit avoir une vitesse de capture assez élevé afin d'éviter de manquer une intrusion. Dans le but d'exploiter de manière optimale la capacité du réseau de capteur en terme d'énergie, la vitesse de capture d'un nœud *v* est variée en fonction de la taille de ses couvrants. Plus la zone d'un capteur est couverte, plus ce dernier peut se permettre de capturer rapidement, et inversement, si la zone n'est pas suffisamment couverte le nœud responsable de celle-ci doit se préserver pour prolonger, le plus longtemps possible la couverture globale.

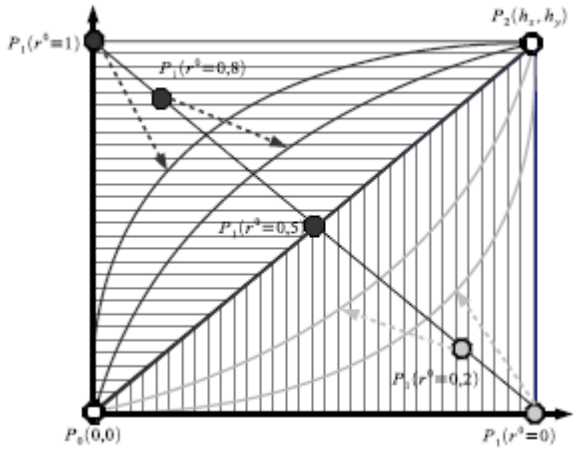

Figure 4.3 Vitesse de capture en fonction de la criticité

Le comportement de l'application est modélisé à l'aide de courbes qui vont d'une forme convexe (peu critique) à une forme concave (très critique) [46], comme expliqué dans la figure 4.3. Le point de comportement P1(b_x, b_y) qui se déplace sur l'anti-diagonale afin de faire passer la courbe d'une forme concave à une forme convexe. La criticité d'une application définie de manière directe le comportement de celle-ci en terme de vitesse de capture.

Il est couramment admis que le *transcepteur* radio est un des composants les plus gourmands en énergie, et donc que la plupart de l'énergie dissipée dans un nœud concerne la transmission et la réception de données. Si l'application le permet, il est donc préférable de transmettre des mesures quand un événement est détecté dans la zone de perception du nœud capteur (c'est-à-dire un changement considérable dans un phénomène mesuré) ou par demande directe plutôt que de transmettre les mesures périodiquement.

Au delà du mode de fonctionnement de l'application, une des techniques les plus utilisées pour diminuer l'énergie dépensée pour la transmission des données est *l'agrégation des données*. D'autres solutions existent pour diminuer la consommation d'énergie, comme par exemple l'adaptation des cycles d'endormissement ou de la puissance du *transceiver* radio.

Ils sont très intéressants dans les applications de surveillance, étant donné que la vision est certainement le plus puissant des sens humains. Mais les réseaux de capteurs d'images posent des problèmes supplémentaires par rapport aux réseaux de capteurs traditionnels en raison des caractéristiques particulières de l'information qui est mesurée.

Une image est généralement représentée sur plusieurs milliers d'octets ; par conséquent, le nœud capteur va devoir générer beaucoup de paquets pour transmettre l'image entière, et donc consomme beaucoup d'énergie. Une solution évidente pour diminuer la quantité de données envoyée, et donc l'énergie consommée dans le réseau, est de compresser l'image à la source.

Dans la littérature plusieurs travaux se penchent notamment sur l'amélioration de la consommation de l'énergie au niveau des réseaux de capteurs image sans fil déployés pour des fins de la sureviallance. Enyan Sun et al. dans [47] proposent un algorithme de compression d'image à énergie optimale. Cet algorithme se base sur la division de l'image en plusieurs régions. La région de haut intérêt se traite différemment par rapport aux autres régions. Pinar Sarisaray dans [48] propose un algorithme robuste dédié à la transmission d'image dans un réseau de capteurs sans fil. Il se base sur les techniques de la restauration de l'image en cas d'erreur de transmission ou en cas de panne au niveau d'un nœud capteur. Huamig Wu et al. dans [49] proposent une solution pour l'introduction de la rotation des nœuds cameras. Cette technique se base sur la gestion de la couverture en préservant l'énergie. Zhen Zuo et al. dans [50] proposent un algorithme basé sur l'ajustement du rayon de transmission des cameras.

Plusieurs travaux de recherches traitent, de différentes manières, la problématique de la détection d'intrusion. Deux techniques principales sont mises en place dans la détection d'attaques. La première consiste à détecter des signatures d'attaques connues dans les paquets circulant sur le réseau. La seconde, consiste quant à elle, à détecter une activité suspecte dans le comportement de l'utilisateur. Ces deux techniques, aussi différentes soient-elles, peuvent être combinées au sein d'un même système afin d'accroître la sécurité.

Les travaux de Lindqvist et al. dans [51] se basent sur la détection de signatures. Une fois qu'un événement soit détecté, son comportement sera comparé directement avec une base de signature d'une liste d'attaques déjà établie. Une alarme sera déclenchée dans le cas d'une identification d'une intrusion. Cette technique n'est pas toujours efficace surtout dans le cas de l'apparition d'une nouvelle attaque qu'on n'a pas déjà répertorié sa signature.

Les travaux de Javitz et al. dans [52] proposent une détection d'intrusion basée sur la détection d'anomalie. Dans l'absence d'anomalie, le système est dit en fonctionnement normal, alors qu'en présence d'anomalie le système bascule vers un comportement anormal. Cette technique se base sur la comparaison de ces deux comportements du système. Son inconvénient majeur est la génération de fausses alarmes, en confondant un disfonctionnement, suite à une défaillance, avec une détection d'intrusion.

Les travaux de Ko et al. dans [53] proposent une solution hybride pour réduire les fausses alertes. Cette technique est basée sur l'étude des causes de la déviation du système depuis son comportement normal vers un comportement dit anormal.

4.3 Contributions

Nos contributions sont accentuées sur la proposition d'une solution à la diffusion d'alerte suite aux détections d'intrusion dans le modèle *WVSN model* (Wireless VideoSensor Network) de surveillance. On a supposé au départ que toutes les caméras basculent en mode de fonctionnement capture d'image au lieu du mode de fonctionnement enregistrement vidéo. Dans ce cas, on obtient une dérivée du modèle dite *WISN model* à partir du *WVSN model*. Avec ce passage, on gagne surtout en terme d'énergie car quand les caméras fonctionnent en mode capture d'image au lieu du mode vidéo continu, elles consomment moins d'énergie. La capture d'image est conditionnée par la détection d'intrusion, et en fonction de l'ampleur de l'alerte un renforcement est établi pour accélérer la prise de photos.

Nos contributions se résument ainsi [55] :

- Proposition d'un algorithme de diffusion sélective de l'alerte ;
- Proposition d'un algorithme de mode de fonctionnement de cette diffusion.

L'algorithme de notre approche selectiveFov est défini comme suit :

Algorithm selectiveFoV:

Input: intrusion detected
Output: alert packet
Begin
List := ""
If node *V* detects intrusion **Then**
Begin
index := id_Sender
V := neighbors[index].p
Fori:=0 to nbNeighbors**Do**
Begin
If (neighbors[i].p is_inside(*V*.fov) **Then**
Begin
If (neighbors[i].isActive=True) **Then**
Begin
Increase AlertCriticalitylevel
SetAlertCriticalityLevel
list := list + "#" + neighbors[i].id
End
Else
Begin
neighbors[i].status := Active
Endif
Endif
Add list to Alert packet
Send Alert packet to RoutingModule
Enddo
Endif
// Comportement des nœuds recevant un paquet d'alerte.
list_id := Packet.list
For each node *V'* receives Alert Packet **Do**
Begin
If*V'*.id is in list_id**Then**

```
   Begin
     If (V'.Alerted==False) Then
Alerted := True
     Else
     Begin
       Increase AlertCriticalitylevel
SetAlertCriticalityLevel
Endif
   Send Alert to neighbors
Endif
Enddo
End
```

Cette solution se base sur l'envoie d'alerte vers les nœuds qui sont dans le champ de vision du nœud capteur ayant détecté l'intrusion. Elle vient pour résoudre le problème de l'inondation comme défini dans la figure 4.4

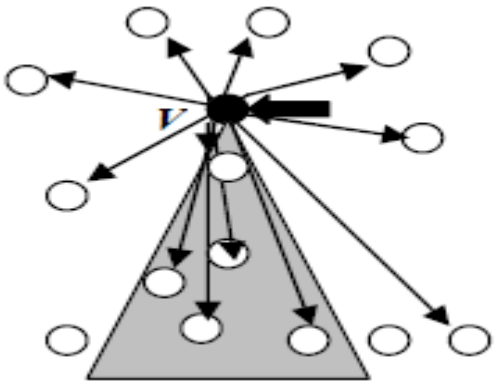

Figure 4.4 Diffusion d'alerte par la technique noSelectiveFov

La figure 4.5 montre le fonctionnement de notre algorithme. On remarque qu'il réduit considérablement l'effet d'inondation. Il propage l'alerte vers le sous ensemble de nœuds se trouvant dans son champ de vision.

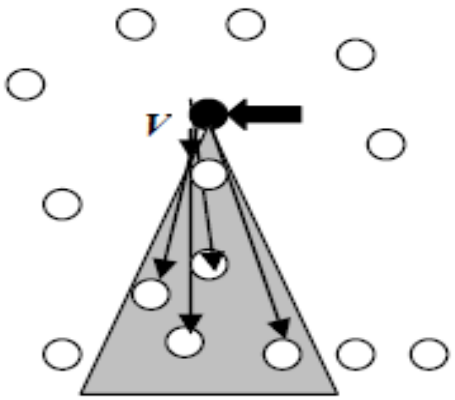

Figure 4.5 Diffusion d'alerte par la technique SelectiveFov

La figure 4.6 montre une autre variante de notre algorithme. Cette variante peut étendre le nombre de nœuds recevant l'alerte en augmentant l'angle de vue du capteur image. Cet angle est variable, alors en fonction de la criticité de l'application on peut jouer sur la variation de cet angle.

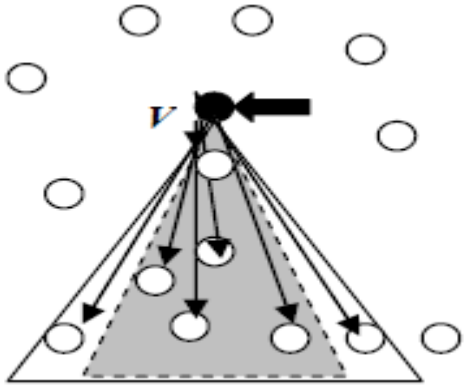

Figure 4.6 Diffusion d'alerte par la technique VirtualSelectiveFov

L'algorithme n°2 suivant propose un passage d'une stratégie vers une autre dans la même application. Si l'application a un niveau de criticité élevé l'algorithme choisi sera par inondation c'est-à-dire noSelectiveFov sera opérationnel. Si l'application a un niveau modéré de criticité, la gestion des alertes sera gérée par la technique SelectiveFov sinon on peut passer d'un temps à autre vers la stratégie virtualFov.

Algorithme2 :

Algorithm scheduling Alert:
Begin
Level :=Current_CriticalityLevel;
If Level = "Low" **Then**
Uses *SelectiveFov* algorithm for routing alert
Else
if Level = "Medium" **Then**
Uses *VirtualFov* algorithm for routing alert
Else
Uses *NoselectiveFov* algorithm for routing alert
Endif
Endif
End.

4.4 Outils de développement

4.4.1 Environnement d'Omnetpp :

Omnetpp est un simulateur à événement discret permettant la modélisation des systèmes sous forme de modules communiquant entre eux, notamment les réseaux de capteurs sans fil, voir [9].Les modules communiquent entre eux via des messages à travers des ports (In, Out). La figure 4.7 schématise cette vue comme suit :

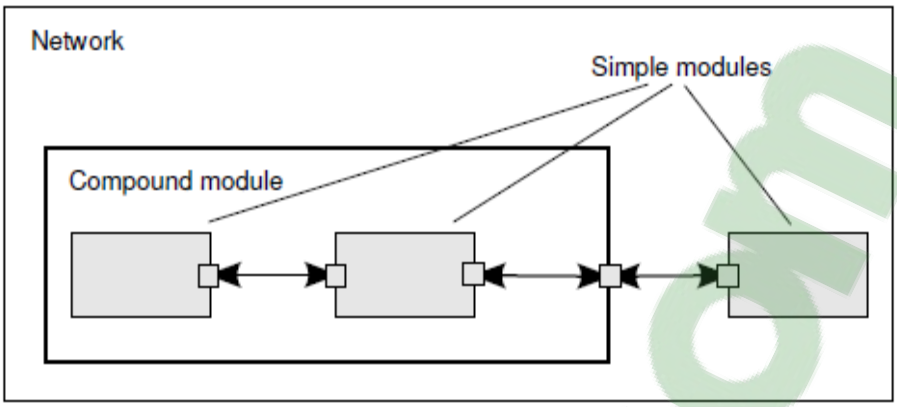

Figure 4.7 Modélisation d'un réseau sous Omnetpp

Sous Omnetpp, un nœud capteur est modélisé sous forme d'un module simple. Le réseau de capteurs sans fil est alors défini comme un ensemble de modules simples.

La figure 4.8 suivante présente l'interface de développement d'Omnetpp.

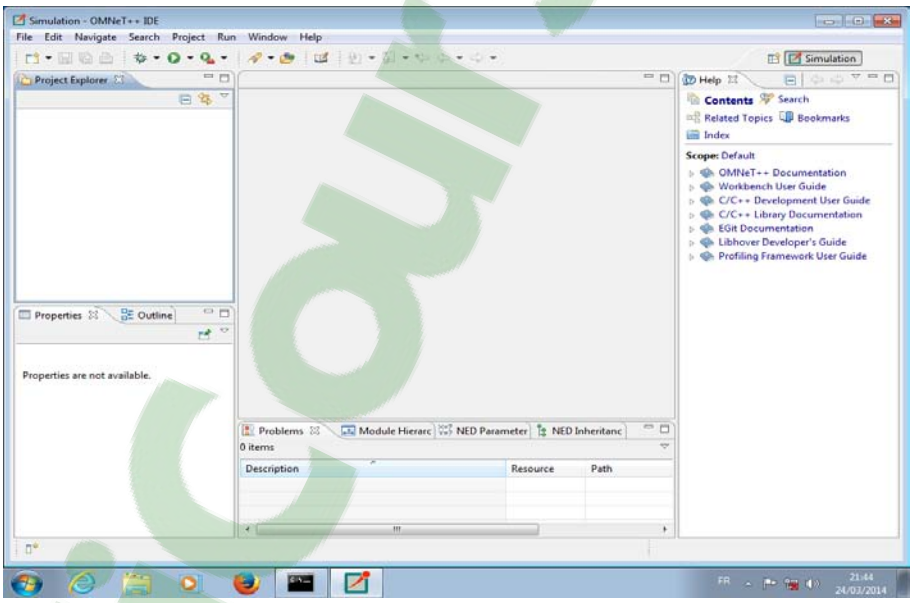

Figure 4.8 Interface de développement du simulateur Omnetpp

Le lancement de la simulation visualise le comportement du réseau suite à l'échange de messages entre ses différents nœuds en communication. L'interface graphique suivante illustrée par la figure 4.9 affiche les différents comportements intermédiaires des nœuds.

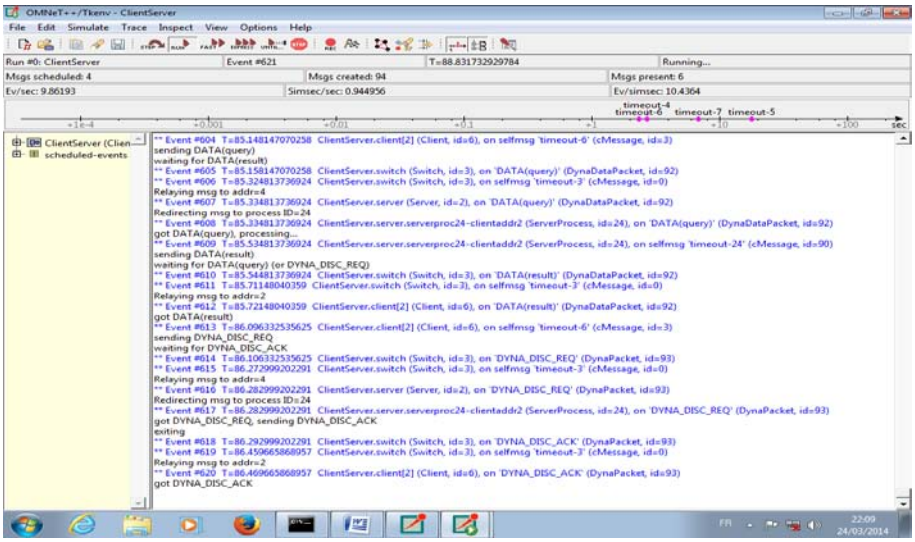

Figure 4.9 Exemple de lancement d'une simulation sous Omnetpp

Une simulation doit contenir les fichiers suivants, comme indiqué dans la figure 4.10:

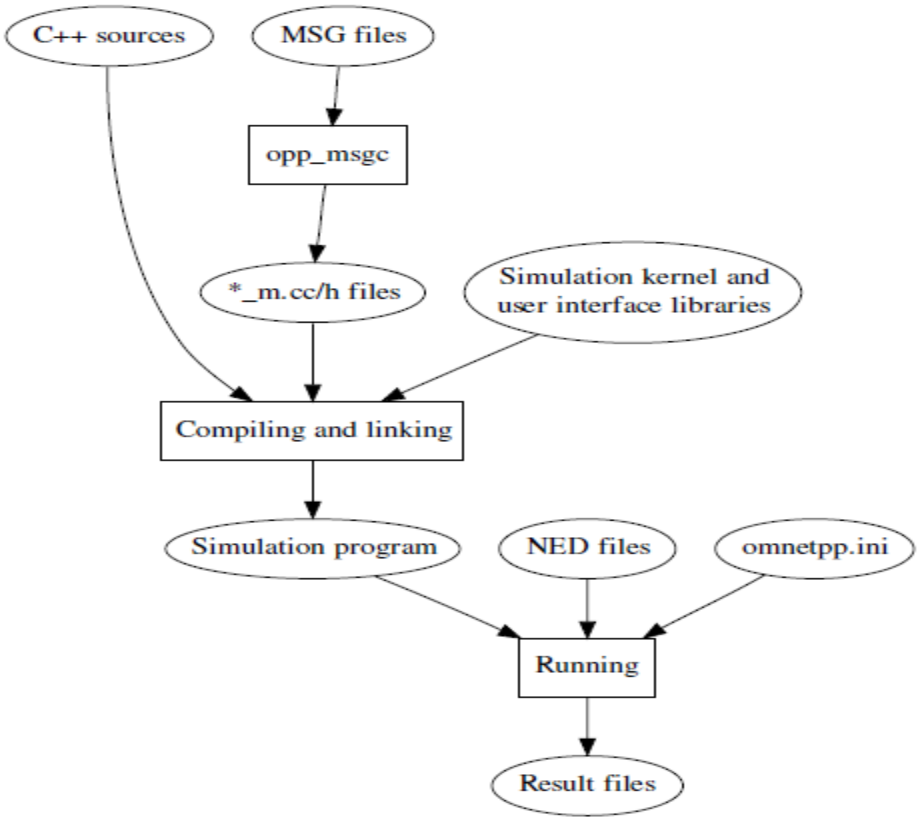

Figure 4.10 Processus de création d'une simulation sous Omnetpp

- fichier.ned : Le fichier avec l'extension ‘’.ned’’ est utilisé pour la description des nœuds formant le réseau.
- fichier.ini : Le fichier avec l'extension ‘’.ini.’’ est utilisé pour contenir les conditions initiales pour les différents scénarios des simulations. Il spécifie le nom du réseau à exécuter.
- fichier.c : Les fichiers ayant l'extension ‘’.c’’ sont utilisés pour programmer les comportements des nœuds suite à la réception d'un message.
- fichier.h : Les fichiers ayant l'extension ‘’.h’’ contiennent les entêtes des méthodes utilisées dans les fichiers ‘’.c’’.
- fichier.msg : Les fichiers avec l'extension ‘’.msg’’ indiquent les fichiers contenant les structures des messages. Ils seront transformés en fichiers ‘’.c’’ grâce à la commande opp_msgc.
- fichier.vec : Les résultats des simulations sont sauvegardés dans un fichier ‘’.vec’’. c'est un fichier trace de type *vector*. Ce fichier sera par la suite utilisé pour l'analyse et la génération des courbes.
- fichier.sca : Les résultats des simulations sont sauvegardés dans un fichier ‘’.sca’’. c'est un fichier trace de type *scalar*. Ce fichier sera par la suite utilisé pour l'analyse et la génération des courbes.

Les comportements des nœuds dans une simulation sont programmés à l'aide des méthodes suivantes:

- Void initialize() : Pour toute simulation la méthode ‘’*initialize ()*’’ de chaque nœud se lance qu'une seule fois pour initialiser les propriétés de chaque nœud. Puis elle passe le contrôle à la méthode ‘’*handleMessage ( )*’’ suivante.
- Void handleMessage (cMessage *msg) : Chaque réception de message par le nœud provoque le lancement de la méthode ‘’*handleMessage ( )*’’. Cette méthode doit contenir les différents traitements à réaliser par le nœud suite au type de message reçu.
- Void activity () : Cette méthode représente une autre variante de la méthode ‘’*handleMessage ( )*’’. Elle contient la programmation des comportements des nœuds.

- Void finish () : L'appel de cette méthode provoque l'arrêt de la simulation. Dans une simulation on peut ne pas avoir cette méthode ; la simulation sera arrêtée quand il n'y aura plus de message à traiter. Cette méthode contient souvent l'appel aux fichiers traces pour la sauvegarde des résultats de la simulation.

4.4.2 Environnement de Castalia :

Le simulateur Castalia représente une extension des fonctionnalités d'Omnetpp notamment dans les phases de la transmission de paquets et la gestion de l'énergie [10]. Dans Omnetpp le paquet est transmis via le canal de communication en utilisant les ports des modules. Or que dans Castalia le canal de communication représente le canal sans fil ‘’Wireless Channel’’ comme indiqué dans la figure 4.11.

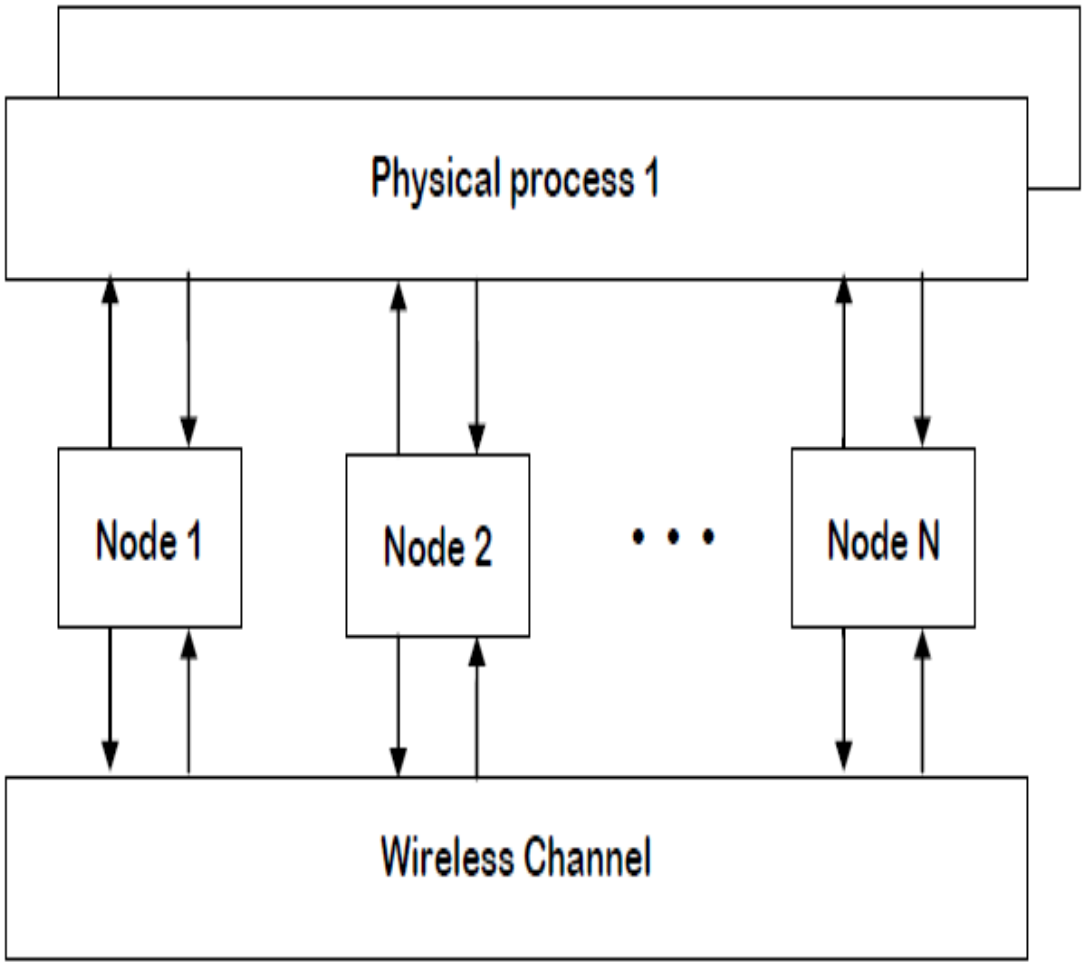

Figure 4.11 Les Noeuds et leurs connections en Castalia

Dans Castalia, chaque nœud est formé d'un ensemble de modules. Un paquet généré par un nœud est transmis directement vers le module de communication comme indiqué dans la figure 4.12.

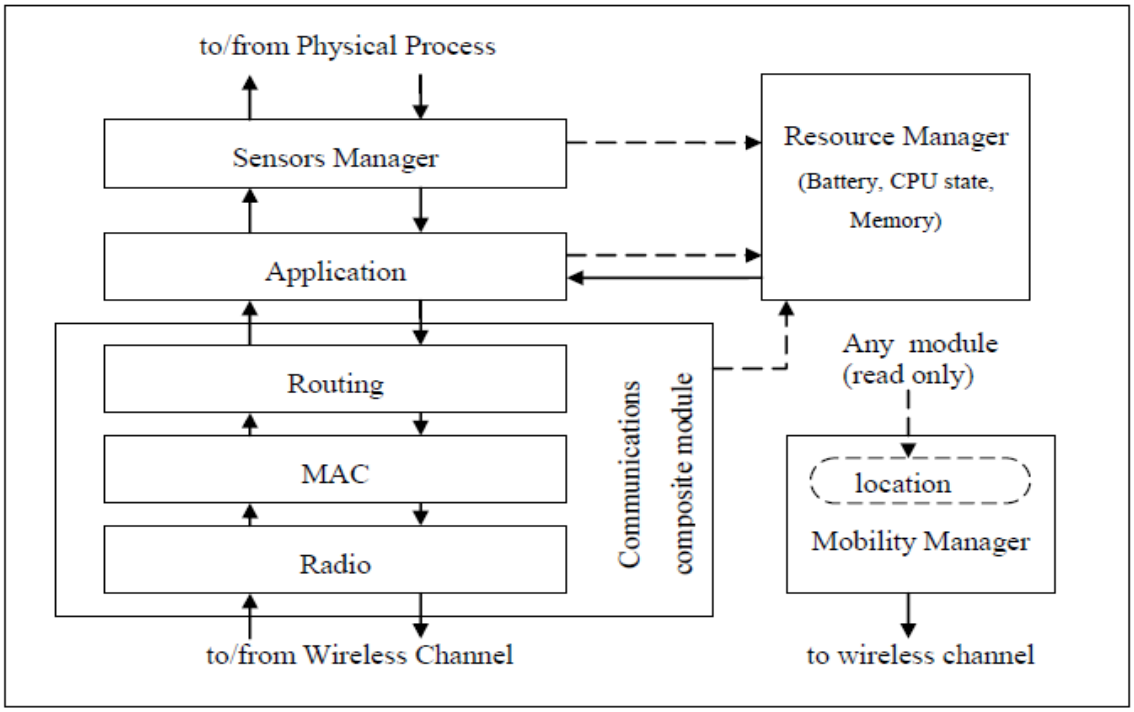

Figure 4.12 La vue d'un nœud sous Castalia

Lors de l'installation de Castalia, chaque module sera représenté par un répertoire. La figure 4.13 montre les répertoires de base du simulateur Castalia.

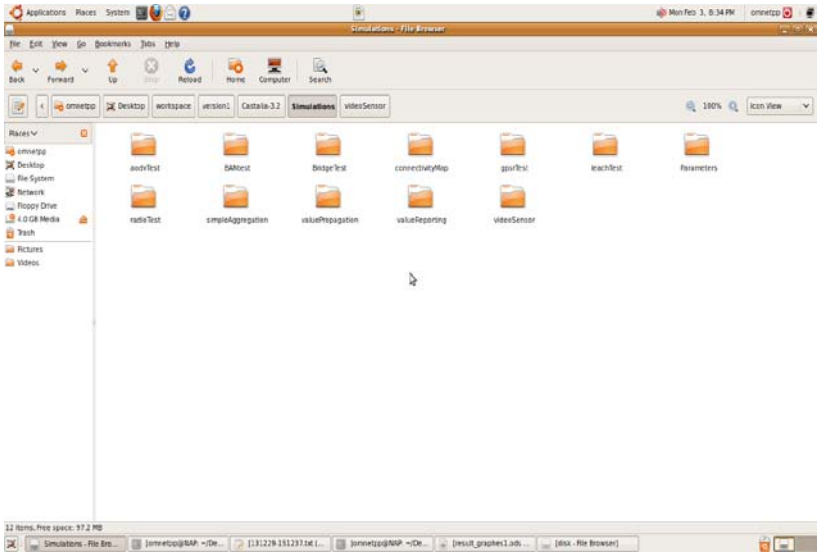

Figure 4.13 Les répertoires de base de Castalia

4.5 Résultats et discussion

Les simulations sont établies sur un champ de 75mx75m avec un nombre de 300 nœuds sous Castalia. La couche application est représentée par le modèle du capteur image sans fil. La couche routage est représentée par le protocole Bypass de Castalia. Dans la couche Mac on trouve CSMA (carrier sense multiple access). Les simulations sont répétées 10 fois aléatoirement. Les résultats des simulations sont enregistrés dans un fichier résultat sous Castalia comme il est montré dans la figure 4.14 et la figure 4.15 selon le format voulu.

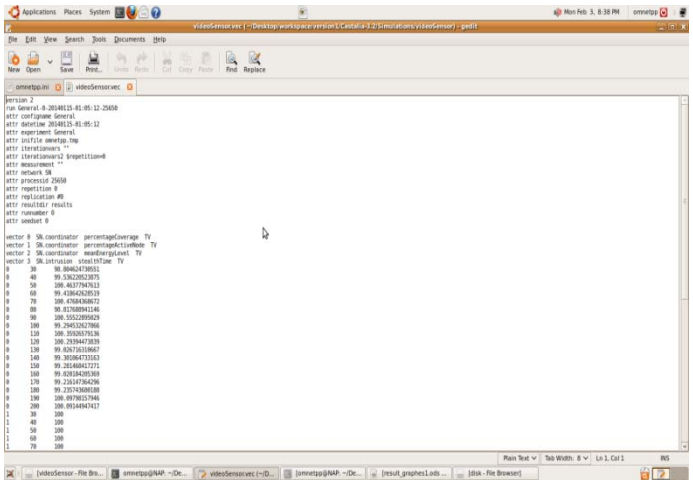

Figure 4.14 Fichier résultat du Castalia en mode *vector*

Le fichier résultat en mode *vector* contient une série de données produites durant la simulation. C'est un fichier texte dont chaque ligne résume le comportement d'un nœud suite à un événement. Une ligne est composée des colonnes suivantes : numéro du nœud, temps de simulation actuel, et la donnée enregistrée.

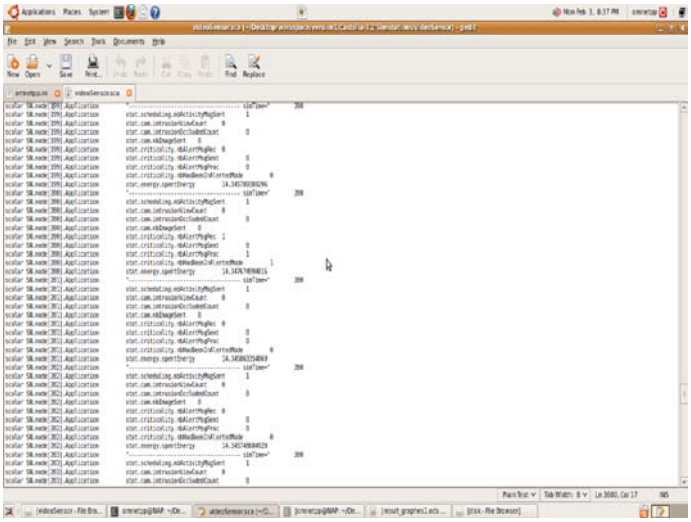

Figure 4.15 Fichier résultat du Castalia en mode *Scalar*

Les données scalaires sont enregistrées dans un fichier résultat en mode scalaire grâce à la commande *recordScalaire()* appelée par la fonction *finish()*. Le formatage de la sauvegarde des résultats en mode scalaire est laissé au programme utilisateur.

La figure 4.16 et la figure 4.17 montrent que l'algorithme selectiveFov a donné de bons résultats en matière de nombre de message envoyé par rapport à l'algorithme noSlectiveFov.

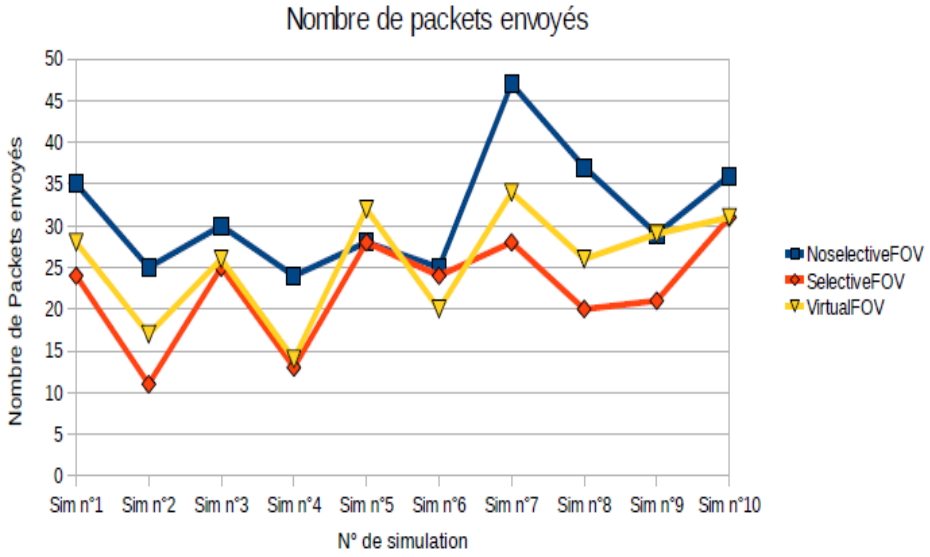

Figure 4.16 Nombre de paquets envoyés

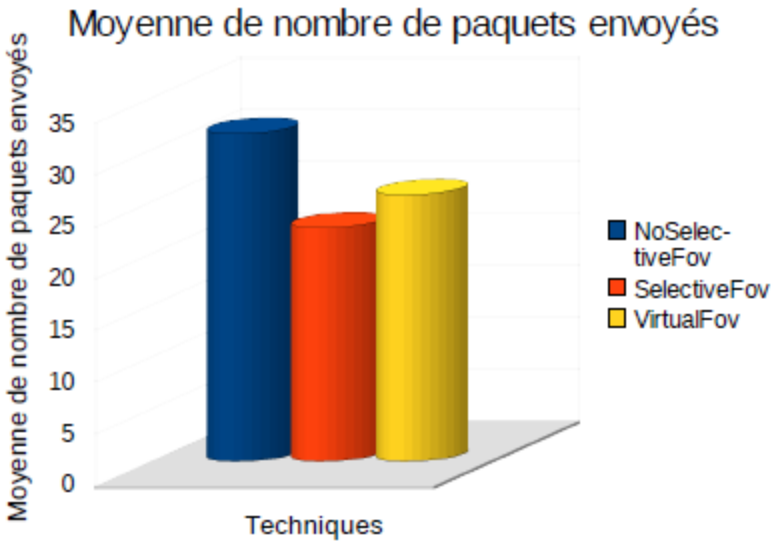

Figure 4.17 Moyenne de nombre de paquets envoyés

La figure 4.18 et la figure 4.19 montrent que la techniques selectiveFov a réduit considérablement le nombre de paquet reçu par rapport à la technique noSelectiveFov.

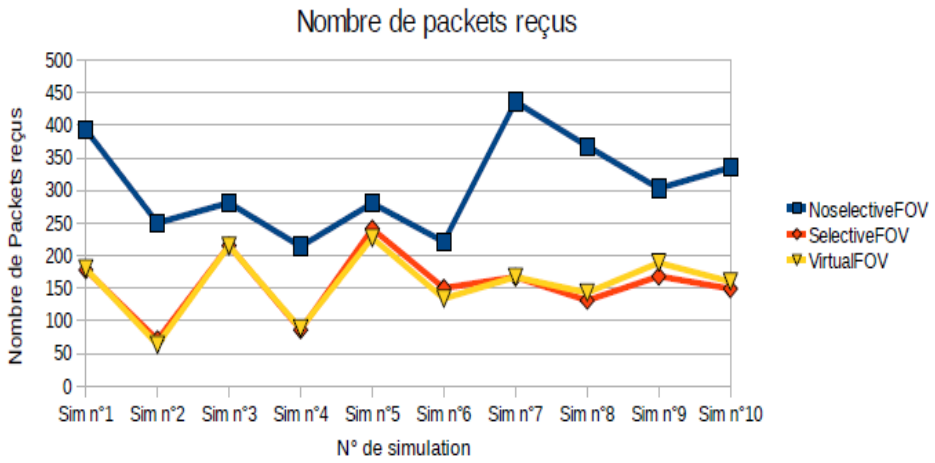

Figure 4.18 Nombre de paquets reçus

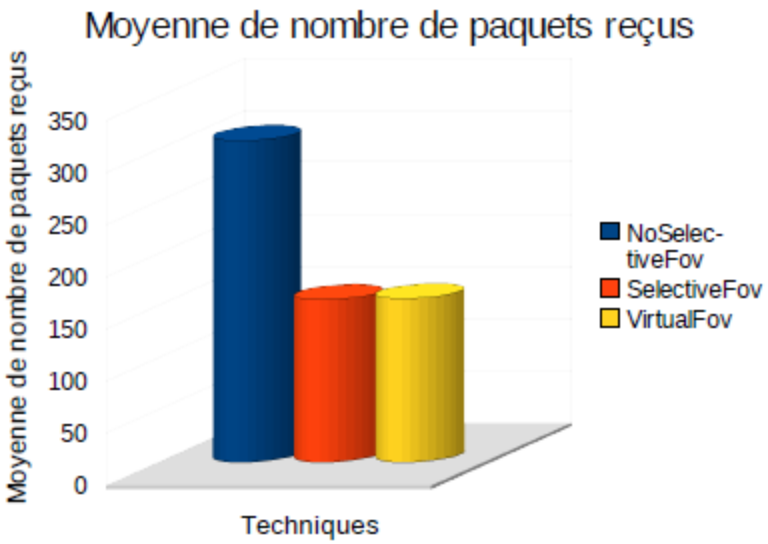

Figure 4.19 Moyenne de nombre de paquets reçus

La figure 4.20 montre que la stratégie noSelectiveFov a donné de meilleurs résultats concernant le nombre de détection d'intrusion par rapport à la technique SelectiveFov. Comme la technique noSelectiveFov a pour rôle d'alerter tous les nœuds voisins, ceci a réduit considérablement le passage inaperçu d'un intrus.

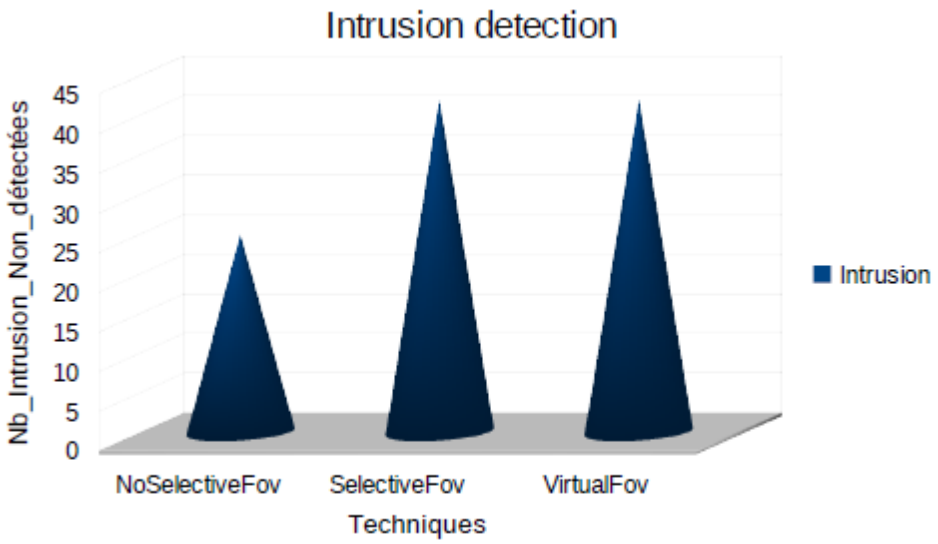

Figure 4.20 Détection d'intrusion

La figure 4.21 montre que la technique selectiveFov a bien contribué dans la préservation de la consommation de l'énergie par rapport à la technique noSelectiveFov.

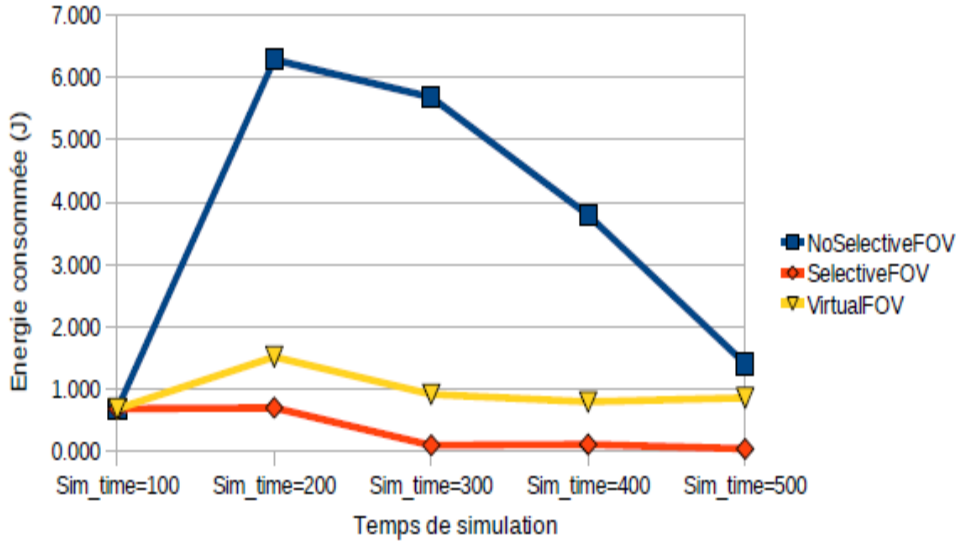

Figure 4.21 Consommation d'énergie

Nous avons appliqués notre technique selectiveFoV sur un algorithme de routage multi-chemins (MultipathRouting : MPR) et sur un algorithme de routage GPSR avec 300 nœuds, les résultats de la simulation de la figure 4.22 montre le taux de paquets échoués et le taux de paquets reçus sans interférences.

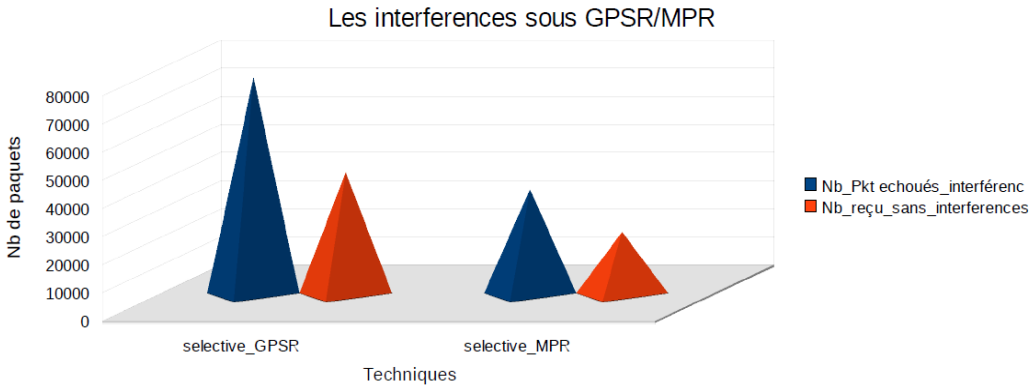

Figure 4.22 Les interférences sous selective_GPSR /MPR

La figure 4.23 montre le taux de paquets échoués et le taux de paquets reçus sans interférences sous les techniques selective_AODV et selective_MPR.

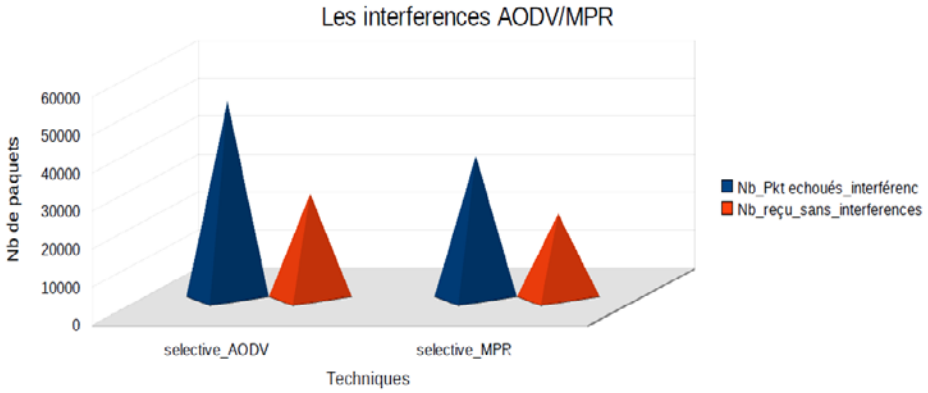

Figure 4.23 Interférences sous selective_AODV/MPR

Notre algorithme selectiveFov a donné de bons résultats dans la conservation de l'énergie du réseau et il a réduit considérablement le nombre de paquets circulant dans le réseau. La technique noSelectiveFov, veut dire inondation, elle épuise l'énergie du réseau en procédant par une diffusion d'alerte pour tous les nœuds du réseau. La technique virtualFov représente une autre variante de la stratégie selectiveFov avec possibilité de varier le champ de vision du capteur.

4.6 Conclusion

Au delà des défis traditionnels des réseaux de capteurs sans fil, les applications des réseaux de capteurs d'images posent des défis particuliers, notamment, des protocoles de transmission et des algorithmes de compression d'images du monde réel, temps réel, et sécurité et confidentialité. Lors de la détection d'intrusion, des alertes sont envoyées.

L'envoie de ces alertes se fait sous forme de diffusion générale pour tous les nœuds du réseau. Ceci créée une inondation du réseau par des messages d'alertes avec possibilité d'implosion. Ce phénomène est très néfaste pour le réseau de capteurs image sans fil car il épuise rapidement l'énergie du réseau or que ce dernier est destiné à assurer des objectifs très critiques de la surveillance.

Lorsque le déploiement est aléatoire, il peut y avoir une grande redondance entre les nœuds et une approche couramment utilisée est de définir un sous-ensemble de nœuds qui seront actifs pendant que d'autres seront inactifs. Le résultat est un ordonnancement de l'activité des nœuds qui maintient la couverture et la connectivité de la zone à surveiller.

Notre contribution dans ce domaine a permis de réduire considérablement la propagation des messages d'alertes en se basant sur la propriété champ de vision de la caméra (field of view : FoV) et sur la redondance des nœuds capteurs. La propagation des alertes se fait de manière à acheminer les paquets uniquement vers le sous ensemble des nœuds capteurs qui sont dans le champ de vision du capteur ayant détecté l'intrusion.

Conclusion générale

Lorsque les capteurs sont déployés dans des zones inaccessibles ou encore déployés sur de grands espaces, c'est à-dire lorsqu'il est difficile voire impossible de remplacer les batteries des nœuds quand elles arrivent à épuisement alors la consommation d'énergie devient un problème fondamental. De ce fait, la durée de vie limitée des nœuds va avoir un impact sur la durée de vie du réseau tout entier. Par la suite, elle aura des conséquences négatives sur la connectivité et la couverture du réseau.

Dans ce présent travail, plusieurs travaux de recherches ont été cités ayant pour but l'amélioration de la consommation de l'énergie au niveau du réseau de capteur. La majorité des propositions données concluent que ce domaine de recherche reste toujours ouvert pour de nouvelles idées.

Un autre défi scientifique dans le domaine des réseaux de capteurs sans fil ne cesse de sonner l'alarme. Ce domaine est celui de la sécurité. Les applications basées sur ces réseaux ont souvent besoin d'un niveau de sécurité élevé car ils fournissent des services essentiels, voire vitaux. Alors, il faut se pencher d'urgence sur les problèmes de sécurité et de protection de la vie privée.

La redondance d'informations est très sollicitée dans le domaine de la surveillance. La comparaison des grandeurs redondantes permet de décider si une défaillance est présente ou non. Avec la redondance le système répond convenablement à la tolérance aux fautes. Les réseaux de capteurs sans fil dédiés à la surveillance se basent pleinement sur ce principe pour accomplir correctement ces objectifs.

Avec l'application des techniques de la redondance pour optimiser la collecte et le transfert des images dans la zone de déploiement de réseau de capteurs sans fil, de une nouvelles méthodes de compression d'image satisfaisant à l'une des contraintes induite par les réseaux de capteurs sans fil sont proposées. La compression d'image permet de réduire la taille des informations transmises tout en offrant une bonne qualité d'image et une faible consommation en énergie.

Au delà des défis traditionnels des réseaux de capteurs sans fil, les applications des réseaux de capteurs d'images posent des défis particuliers, notamment, des protocoles de transmission et des algorithmes de compression d'images du monde réel, temps réel, et sécurité et confidentialité. Lors de la détection d'intrusion, des alertes sont envoyées. L'envoie de ces alertes se fait sous forme de diffusion générale pour tous les nœuds du réseau. Ceci créée une inondation du réseau par des messages d'alertes avec possibilité d'implosion. Ce phénomène est très néfaste pour le réseau de capteurs image sans fil car il épuise rapidement l'énergie du réseau or que ce dernier est destiné à assurer des objectifs très critiques de la surveillance.

Notre contribution dans ce domaine a permis de réduire considérablement la propagation des messages d'alertes en se basant sur la propriété champ de vision de la caméra (field of view : FoV) et sur la redondance des nœuds capteurs. La propagation des alertes se fait de manière à acheminer les paquets uniquement vers

le sous ensemble des nœuds capteurs qui sont dans le champ de vision du capteur ayant détecté l'intrusion.

Perspectives :

Dans nos prochains travaux on envisage de travailler sur la problématique de la mobilité des cameras en sens de rotation pour la surveillance d'une zone. Dans cette thématique le travail sera focalisé sur l'envoi d'une partie dite de haut intérêt d'une image captée suite à une intrusion. Cette technique aura sans doute un impact sur la consommation de l'énergie au niveau du réseau.

Un autre axe de rechercher à envisager dans ce même contexte est d'introduire les techniques de la reconnaissance de forme pour améliorer la détection d'intrusion.

Références bibliographiques

[1] Lionel Barrère, 'Étude et proposition de services dans les réseaux mobiles militaires de type MANet ', Thèse de doctorat, Université de Bordeaux, 2009.

[2] Damien Roth, 'Gestion de la mobilité dans les réseaux de capteurs sans fil', Thèse de doctorat, Université de Strasbourg, 2012.

[3] Kamal Beydoun, 'Conception d'un protocole hiérarchique de routage pour les réseaux de capteurs', Thèse de doctorat, Université de Franche-Comté France, 2009.

[4] Jason Lester Hill , 'System Architecture for Wireless Sensor Networks ', PhD Thesis, University of California, Berkeley, 2003.

[5] Elyès Ben Hamida, 'Modélisation stochastique et simulation des réseaux sans fil multi-sauts', Thèse de doctorat, Institut National des Sciences Appliquées de Lyon France, 2009.

[6] Ludovic SAMPER, 'Modélisations et analyses de réseaux de capteurs', Thèse de doctorat, Laboratoire Verimag, Institut National Polytechnique de Grenoble France, 2008.

[7] Yan Grunenberger, 'Réseaux sans fil de nouvelle génération : architectures spontanées et optimisations inter-couches', Thèse de doctorat, Institut Polytechnique de Grenoble, 2008.

[8] Muhammad Ullah, Waqar Ahmad , 'Evaluation of Routing Protocols in Wireless Sensor Networks', Master Thesis, Blekinge Institute of Technology , Sweden, 2009.

[9] Yousef Yaser, 'Routage pour la Gestion de l'Energie dans les Réseaux de Capteurs Sans Fil', Thèse de doctorat, Université de la haute Alsace, 2010.

[10] Bouabdellah KECHAR, 'Problématique de la consommation d'énergie dans les réseaux de capteurs sans fil', Thèse de doctorat, Université d'Oran, 2010.

[11] Rahim KACIMI , 'Techniques de conservation dénergie pour les réseaux de capteurs sans fil', Thèse de doctorat, Université de Toulouse, 2009.

[12] Muhammad Ullah, Waqar Ahmad, 'Evaluation of Routing Protocols in Wireless Sensor Networks', Master thesis, Blekinge Institute of Technology SWEDEN , 2009.

[13] Ali Chamam, 'Mécanisme optimisés de planification des états des capteurs pour la maximisation de la durée de vie dans les réseaux de capteurs sans fil', Thèse doctorat, Département de génie informatique et dénie logiciel, Ecole polytechnique de Montréal, 2009.

[14] Jin Wang , 'Hop-based Energy Aware Routing Scheme for Wireless Sensor Networks', PhD Thesis, Kyung Hee University , Seoul, Korea, 2010.

[15] Saoucene Mahfoudh , 'Energy efficiency in wireless ad hoc and sensor networks: routing, node activity scheduling and cross-layering', PhD Thesis, University Paris 6-Pierre et Marie Curie, 2012.

[16] ZNAIDI Wassim , 'Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil', Thèse de doctorat, Institut National des sciences appliquées de Lyon, 2010.

[17] Gérard Chalhoub, 'MaCARI: Une méthode d'accès déterministe et économe pour les réseaux de capteurs sans fil', Thèse de doctorat, Université Blaise Pascal, 2009.

[18] Denis Dessales, 'Conception d'un réseau de capteurs sans fil, faible consommation, dédié au diagnostic in-situ des performances des bâtiments en exploitation', Thèse de doctorat, Université de Poitiers, 2011.

[19] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, 'Wireless Multimedia Sensor Networks: Applications and Testbeds', Proceedings of the IEEE, Vol. 96, No. 10, October 2008.

[20] Aleksandra Karimaa , 'Mobile and Wireless Access in Video Surveillance System', International Journal of Digital Information and Wireless Communications (IJDIWC) 1(1): 267-272 , The Society of Digital Information and Wireless Communications, 2011(ISSN 2225-658X) , 2011.

[21] Hassen Mohammed Abduallah Alsafi, Saeed Salem Basamh , 'A Review of Intrusion Detection System Schemes in Wireless Sensor Network', Journal of Emerging Trends in Computing and Information Sciences , ISSN 2079-8407 , Vol. 4, No. 9, September 2013.

[22] Oliver Poblete , 'An Overview of the Wireless Intrusion Detection System', SANS Institute InfoSec Reading Room , January 2005 .

[23] C.Karlof and D. Wagner, 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures', In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[24] J. Newsome, E. Shi, D. Song and A. Perrig, 'The Sybil Attack in Sensor Networks: Analysis and Defenses', In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004), April 2004.

[25] LABRAOUI Nabila , 'La sécurité dans les réseaux de capteurs sans fil Ad Hoc', Thèse de doctorat, Université de Tlemcen, 2012.

[26] A.Perrig, J. Stankovic and D. Wagner, 'Security in Wireless Sensor Networks', In Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53-57.

[27] Yongguang Zhang , Yi-An Huang , 'Intrusion Detection Techniques for Mobile Wireless Networks', Mobile Networks and Applications, (2003) 1–16.

[28] L.Zhou and Z. J. Haas, 'Securing ad hoc networks'. IEEE Network, 13(6):24–30, Nov/Dec 1999.

[29] Rim Mrani Alaoui, 'Conception d'un module de diagnostic à base des suites de bandes temporelles en vue de la supervision des procédés énergétique. Application en ligne à un générateur de vapeur', Thèse Doctorat, Université de Lille, France. Année 2004.

[30] Gilles ZWINGELSTEIN,'Sûreté de fonctionnement des systèmes industriels complexes'. Thèse de doctorat, Ecole nationale supérieure d'électrotechnique, d'électronique, d'informatique et d'hydraulique de Toulouse (ENSEEIHT), France, 1996.

[31] Kevin M. Somervill , 'Fault-Tolerance and recovery in Wireless Sensor Networks', Master Thesis, Old Dominion University, 2009.

[32] Khaled FAWAZ , 'Contribution à la Télésurveillance des Systèmes Contrôlés en Réseau : Application à la Robotique', Thèse de doctorat, Université des Sciences et Technologies de Lille, 2009.

[33] Zahia BIDAI, 'Routage Multi-chemin avec qualité de service pour le transport d'un trafic scalaire/multimédia dans les réseaux de capteurs sans fil', Thèse de doctorat, Université d'Oran, 2013.

[34] Kazem Sohraby, Daniel Minoli, Taieb Znati, 'Wireless sensor networks: Technology, Protocols, and Applications', Wiley Interscience Publication , 2007.

[36] S. Nath, Y. Ke, P.B. Gibbons, B. Karp and S. Seshan, 'A distributed filtering architecture for multimedia sensors', Intel Research Technical Report IRP-TR-04-16, August, 2004.

[37] W. Hairui, W. Hua, 'Research and design of multi-agent based intrusion detection system on wireless network', International Symposium on Computational Intelligence and Design, Vol.1, Wuhan, China, 2008, pp. 444–447.

[38] S. Dulman, T. Nieberg, J. Wu, P. Havinga,'Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks', WCNC Workshop, New Orleans, Louisiana, USA, March 2003.

[39] C. Pham, 'Coverage and activity management of wireless video sensor networks for surveillance applications', International Journal of Sensor Networks, Vol. 11, No. 3, 2012, pp. 148-165.

[40] Johannes Karlsson, 'Image Compression for Wireless Sensor Networks', PhD Thesis, Umeä University, 2007.

[41] Cristian Duran-Faundez , 'Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie', Thèse de doctorat, Université Henri Poincaré, Nancy 1, 2009.

[42] Johan DEBAYLE, 'Traitement d'image à voisinages adaptatifs généraux', Thèse de doctorat, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2005.

[43] Marc ANTONINI, 'Compression des images et des vidéos numériques', Habilitation à Diriger des Recherches, Université de Nice-Sophia Antipolis, 2003.

[44] C. Pham, A. Makhoul, 'Performance study of multiple cover-set strategies for mission-critical video surveillance with wireless video sensors', Proc. 6th IEEE Conf. on Wireless and Mobile Computing, Networking and Communications, Niagara Falls, Canada, 2010, pp. 208-216.

[45] C. Pham, A. Makhoul, R. Saadi, 'Risk-based adaptive scheduling in randomly deployed video sensor networks for critical surveillance applications', Journal of network and computer applications, Vol. 34, No. 2, 2011, pp. 783-795.

[46] C. Pham, 'Coverage and activity management of wireless video sensor networks for surveillance applications', International Journal of Sensor Networks, Vol. 11, No. 3, 2012, pp. 148-165.

[47] Enyan Sun, Xuanjing Shena,Haipeng Chen, 'A Low Energy Image Compression and Transmission in Wireless Multimedia Sensor Networks', Procedia Engineering 15 (2011) 3604 -3610.

[48] Pinar Sarisaray Boluk · Sebnem Baydere ·A. Emre Harmanci, 'Robust Image Transmission Over WirelessSensor Networks', Springer Science+Business Media, LLC 2010, 14 December 2010.

[49] Huaming Wu, Alhussein A. Abouzeid, 'Energy efficient distributed image compression in resource-constrained multihop wireless networks', Computer Communications 28 (2005) 1658–1668.

[50] Zhen Zuo, Qin Lu , Wusheng Luo, 'A two-hop clustered image transmission scheme for maximizing network lifetime in wireless multimedia sensor networks', Computer Communications 35 (2012) 100–108.

[51] U. Lindqvist, P. A. 'Porras. Detecting computer and network misuse through the production-based expert system toolset (p-BEST)', In IEEE Symposium on Security and Privacy, pp. 146-161. 1999.

[52] H. S. Javitz, A. Valdes, 'The NIDES statistical component: Description and justification', Annual report, Computer Science Laboratory, SRI International, Menlo Park, CA, March 1994.

[53] C. Ko, M. Ruschitzka, K. Levitt, 'Execution monitoring of security critical programs in distributed systems: A specification-based approach', In SP '97: Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 175-187. 1997.

[54] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, 'Wireless Multimedia Sensor Networks: Applications and Testbeds', Proceedings of the IEEE, Vol. 96, No. 10, October 2008.

[55] Y. Benabbassi, H. Haffaf, C. Pham, 'Optimized Alert Routing In Wireless Image Sensor Networks for Mission-Critical Applications', Mediterranean Journal of Computers and Network (MEDJCN), Vol. n°9 issue n°4, 2013.

[56] S.Ahmed SEDJELMACI, 'Mise en œuvre de mécanisme de sécurité basés sur les IDS pour les réseaux de capteurs sans fil', Thèse de doctorat, Université de Tlemcen, 2013.

Liste des publications :

Y. Benabbassi, H. Haffaf, C. Pham, ’Proposed Algorithm for Surveillance Applications’, International Journal of Computer Applications Technology and Research (IJCATR), Vol n°3, issue n°1, January 2014.

Y. Benabbassi, H. Haffaf, C. Pham, ’Optimized Alert Routing In Wireless Image Sensor Networks for Mission-Critical Applications’, Mediterranean Journal of Computers and Network (MEDJCN), Vol. n°9 issue n°4, 2013.

Y. Benabbassi, H. Haffaf, C. Pham,’Alert Routing in Wireless Video Sensor Networks for Monitoring Applications’, International Journal of Computer Applications Technology and Research (IJCATR), Vol. n°2, issue n°6, December 2013.

Grammaire du langage Ned.

```
nedfile
: definitions
|
;
definitions
: definitions definition
| definition
;
definition
: packagedeclaration
| import
| propertydecl
| fileproperty
| channeldefinition
| channelinterfacedefinition
| simplemoduledefinition
| compoundmoduledefinition
| networkdefinition
| moduleinterfacedefinition
| ';'
;
packagedeclaration
: PACKAGE dottedname ';'
;
dottedname
: dottedname '.' NAME
| NAME
;
import
: IMPORT importspec ';'
;
importspec
: importspec '.' importname
| importname
;
importname
: importname NAME
| importname '*'
| importname '**'
| NAME
| '*'
| '**'
;
propertydecl
: propertydecl_header opt_inline_properties ';'
| propertydecl_header '(' opt_propertydecl_keys ')' opt_inline_properties ';'
;
propertydecl_header
```

```
: PROPERTY '@' PROPNAME
| PROPERTY '@' PROPNAME '[' ']'
;
opt_propertydecl_keys
: propertydecl_keys
|
;
propertydecl_keys
: propertydecl_keys ';' propertydecl_key
| propertydecl_key
;
propertydecl_key
: property_literal
;
fileproperty
: property_namevalue ';'
;
channeldefinition
: channelheader '{'
opt_paramblock
'}'
;
channelheader
: CHANNEL NAME
opt_inheritance
;
opt_inheritance
:
| EXTENDS extendsname
| LIKE likenames
| EXTENDS extendsname LIKE likenames
;
extendsname
: dottedname
;
likenames
: likenames ',' likename
| likename
;
likename
: dottedname
;
channelinterfacedefinition
: channelinterfaceheader '{'
opt_paramblock
'}'
;
channelinterfaceheader
: CHANNELINTERFACE NAME
opt_interfaceinheritance
```

```
;
opt_interfaceinheritance
: EXTENDS extendsnames
|
;
extendsnames
: extendsnames ’,’ extendsname
| extendsname
;
simplemoduledefinition
: simplemoduleheader ’{’
opt_paramblock
opt_gateblock
’}’
;
simplemoduleheader
: SIMPLE NAME
opt_inheritance
;
compoundmoduledefinition
: compoundmoduleheader ’{’
opt_paramblock
opt_gateblock
opt_typeblock
opt_submodblock
opt_connblock
’}’
;
compoundmoduleheader
: MODULE NAME
opt_inheritance
;
networkdefinition
: networkheader ’{’
opt_paramblock
opt_gateblock
opt_typeblock
opt_submodblock
opt_connblock
’}’
;
networkheader
: NETWORK NAME
opt_inheritance
;
Moduleinterfacedefinition
: moduleinterfaceheader ’{’
opt_paramblock
opt_gateblock
’}’
```

```
;
moduleinterfaceheader
: MODULEINTERFACE NAME
opt_interfaceinheritance
;
opt_paramblock
: opt_params
| PARAMETERS ':'
opt_params
;
opt_params
: params
|
;
params
: params paramsitem
| paramsitem
;
paramsitem
: param
| property
;
param
: param_typenamevalue
| pattern_value
;
param_typenamevalue
: param_typename opt_inline_properties ';'
| param_typename opt_inline_properties '=' paramvalue opt_inline_properties ';'
;
param_typename
: opt_volatile paramtype NAME
| NAME
;
pattern_value
: pattern '=' paramvalue ';'
;
paramtype
: DOUBLE
| INT
| STRING
| BOOL
| XML
;
opt_volatile
: VOLATILE
|
;
paramvalue
: expression
```

```
| DEFAULT ’(’ expression ’)’
| DEFAULT
| ASK
;
opt_inline_properties
: inline_properties
|
;
inline_properties
: inline_properties property_namevalue
| property_namevalue
;
pattern
: pattern2 ’.’ pattern_elem
| pattern2 ’.’ TYPENAME
;
pattern2
: pattern2 ’.’ pattern_elem
| pattern_elem
;
pattern_elem
: pattern_name
| pattern_name ’[’ pattern_index ’]’
| pattern_name ’[’ ’*’ ’]’
| ’**’
;
pattern_name
: NAME
| NAME ’$’ NAME
| CHANNEL
| ’{’ pattern_index ’}’
| ’*’
| pattern_name NAME
| pattern_name ’{’ pattern_index ’}’
| pattern_name ’*’
;
pattern_index
: INTCONSTANT
| INTCONSTANT ’..’ INTCONSTANT
| ’..’ INTCONSTANT
| INTCONSTANT ’..’
;
property
: property_namevalue ’;’
;
property_namevalue
: property_name
| property_name ’(’ opt_property_keys ’)’
;
property_name
```

```
: '@' PROPNAME
| '@' PROPNAME '[' PROPNAME ']'
;
opt_property_keys
: property_keys
;
property_keys
: property_keys ';' property_key
| property_key
;
property_key
: property_literal '=' property_values
| property_values
;
property_values
: property_values ',' property_value
| property_value
;
property_value
: property_literal
|
;
property_literal
: property_literal CHAR
| property_literal STRINGCONSTANT
| CHAR
| STRINGCONSTANT
;
opt_gateblock
: gateblock
|
;
gateblock
: GATES ':'
opt_gates
;
opt_gates
: gates
|
;
gates
: gates gate
| gate
;
gate
: gate_typenamesize
opt_inline_properties ';'
;
gate_typenamesize
: gatetype NAME
```

```
| gatetype NAME ’[’ ’]’
| gatetype NAME vector
| NAME
| NAME ’[’ ’]’
| NAME vector
;
gatetype
: INPUT
| OUTPUT
| INOUT
;
opt_typeblock
: typeblock
|
;
typeblock
: TYPES ’:’
opt_localtypes
;
opt_localtypes
: localtypes
|
;
localtypes
: localtypes localtype
| localtype
;
localtype
: propertydecl
| channeldefinition
| channelinterfacedefinition
| simplemoduledefinition
| compoundmoduledefinition
| networkdefinition
| moduleinterfacedefinition
| ’;’
;
opt_submodblock
: submodblock
|
;
submodblock
: SUBMODULES ’:’
opt_submodules
;
opt_submodules
: submodules
|
;
submodules
```

```
: submodules submodule
| submodule
;
submodule
: submoduleheader ';'
| submoduleheader '{'
opt_paramblock
opt_gateblock
'}' opt_semicolon
;
submoduleheader
: submodulename ':' dottedname opt_condition
| submodulename ':' likeexpr LIKE dottedname opt_condition
;
submodulename
: NAME
| NAME vector
;
likeexpr
: '<' '>'
| '<' expression '>'
| '<' DEFAULT '(' expression ')' '>'
;
opt_condition
: condition
|
;
opt_connblock
: connblock
|
;
connblock
: CONNECTIONS ALLOWUNCONNECTED ':'
opt_connections
| CONNECTIONS ':'
opt_connections
;
opt_connections
: connections
|
;
connections
: connections connectionsitem
| connectionsitem
;
connectionsitem
: connectiongroup
| connection opt_loops_and_conditions ';'
;
connectiongroup
```

```
: opt_loops_and_conditions '{'
connections '}' opt_semicolon
;
opt_loops_and_conditions
: loops_and_conditions
|
;
loops_and_conditions
: loops_and_conditions ',' loop_or_condition
| loop_or_condition
;
loop_or_condition
: loop
| condition
;
loop
: FOR NAME '=' expression '..' expression
;
connection
: leftgatespec '-->' rightgatespec
| leftgatespec '-->' channelspec '-->' rightgatespec
| leftgatespec '<--' rightgatespec
| leftgatespec '<--' channelspec '<--' rightgatespec
| leftgatespec '<-->' rightgatespec
| leftgatespec '<-->' channelspec '<-->' rightgatespec
;
leftgatespec
: leftmod '.' leftgate
| parentleftgate
;
leftmod
: NAME vector
| NAME
;
leftgate
: NAME opt_subgate
| NAME opt_subgate vector
| NAME opt_subgate '++'
;
parentleftgate
: NAME opt_subgate
| NAME opt_subgate vector
| NAME opt_subgate '++'
;
rightgatespec
: rightmod '.' rightgate
| parentrightgate
;
rightmod
: NAME
```

```
| NAME vector
;
rightgate
: NAME opt_subgate
| NAME opt_subgate vector
| NAME opt_subgate '++'
;
parentrightgate
: NAME opt_subgate
| NAME opt_subgate vector
| NAME opt_subgate '++'
;
opt_subgate
: '$' NAME
|
;
channelspec
: channelspec_header
| channelspec_header '{'
opt_paramblock
'}'
;
channelspec_header
: opt_channelname
| opt_channelname dottedname
| opt_channelname likeexpr LIKE dottedname
;
opt_channelname
:
| NAME ':'
;
condition
: IF expression
;
vector
: '[' expression ']'
;
expression
:
expr
;
expr
: simple_expr
| '(' expr ')'
| CONST '(' expr ')'
| expr '+' expr
| expr '-' expr
| expr '*' expr
| expr '/' expr
| expr '%' expr
```

```
| expr '^' expr
| '-' expr
| expr '==' expr
| expr '!=' expr
| expr '>' expr
| expr '>=' expr
| expr '<' expr
| expr '<=' expr
| expr '&&' expr
| expr '||' expr
| expr '##' expr
| '!' expr
| expr '&' expr
| expr '|' expr
| expr '#' expr
| '~' expr
| expr '<<' expr
| expr '>>' expr
| expr '?' expr ':' expr
| INT '(' expr ')'
| DOUBLE '(' expr ')'
| STRING '(' expr ')'
| funcname '(' ')'
| funcname '(' expr ')'
| funcname '(' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ',' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ',' expr ',' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr ')'
| funcname '(' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr |
funcname '(' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr | funcname
'(' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr ',' expr ;
simple_expr
: identifier
| special_expr
| literal
;
funcname
: NAME
| XMLDOC
| XML
;
identifier
: NAME
| THIS '.' NAME
| NAME '.' NAME
| NAME '[' expr ']' '.' NAME
;
special_expr
```

```
: INDEX
| INDEX ’(’ ’)’
| SIZEOF ’(’ identifier ’)’
;
literal
: stringliteral
| boolliteral
| numliteral
;
stringliteral
: STRINGCONSTANT
;
boolliteral
: TRUE
| FALSE
;
numliteral
: INTCONSTANT
| REALCONSTANT
| quantity
;
quantity
: quantity INTCONSTANT NAME
| quantity REALCONSTANT NAME
| INTCONSTANT NAME
| REALCONSTANT NAME
;
opt_semicolon
: ’;’
|
;
```