État de l'art - Sécurité dans les réseaux de capteurs sans fil

David Martins, Hervé Guyennet

Etat de l'art
Sécurité dans les réseaux de capteurs sans fil

David MARTINS (martins@lifc.univ-fcomte.fr)*
Hervé GUYENNET (guyennet@lifc.univ-fcomte.fr) *

Abstract: Les réseaux de capteurs sans fil sont des réseaux ad-hoc particuliers qui se caractérisent par leurs contraintes d'énergie et leur puissance limitée. Ce papier propose un état de l'art sur la sécurité dans ce type de réseau. Nous montrons quelles sont les spécificités des réseaux de capteurs sans fil et les vulnérabilités qui en découlent. Nous présentons ensuite une liste des attaques que l'on peut trouver dans ces réseaux particuliers et les solutions apportées par la communauté scientifique pour les sécuriser.

Keywords: Réseaux de capteurs sans fil, sécurité, vulnérabilité

1 Introduction

Les facilités de déploiement des capteurs sans fil et la baisse de leur coût ont permis de généraliser l'utilisation de réseaux de capteurs sans fil. Aujourd'hui on retrouve ce type de réseau aussi bien dans la surveillance industrielle, que dans la mesure de données environnementales [KPC+06] [Wel06], la domotique, la détection d'incendie [TFdGEB06], le milieu médical [MFJWM04] ou bien encore dans le domaine militaire.
La plupart de ces applications ont pour mission de surveiller une zone et d'obtenir une réaction quand elles détectent une donnée critique.
La divulgation de ces données critiques peut ne pas avoir une grande incidence dans des domaines tels que la domotique ou bien la capture d'événement environnemental. Sa confidentialité peut par contre être indispensable dans d'autres applications, comme pour le secret médical d'un patient à l'hôpital ou pour la sécurité du territoire dans le domaine militaire.

Un exemple de ces applications critiques est décrit dans le projet CodeBlue[MFJWM04], où des capteurs recueillent des informations d'un patient. D'autres exemples existent aussi dans les applications militaires, comme par exemple la surveillance d'une zone de guerre ou l'enregistrement de l'état de santé ou de la position des troupes.

Dans ces deux cas, la confidentialité de l'information est primordiale, d'un point de vue juridique dans le premier cas, et d'un point de vue sécuritaire dans le second.
Cette sécurité est bien sûr mise en danger par le médium utilisé, à savoir les ondes, mais également par les vulnérabilités spécifiques aux réseaux de capteurs sans fil.

Les solutions utilisées dans les réseaux ad hoc classiques, ne peuvent pas s'appliquer stricto sensu aux réseaux de capteurs sans fil, car ces dispositifs sont limités par leur batterie et leur puissance de calcul.

* LIFC, Équipe SDR, 16 route de gray - 25030 BESANCON Cedex - FRANCE
Tel : +33 (0)3 81 66 64 55 - Fax : +33 (0)3 81 66 64 50

Concrètement les solutions de cryptographies utilisées actuellement, comme les clés asymétriques, sont des solutions trop lourdes pour être calculées par les processeurs des capteurs actuels. Les protocoles de sécurisation doivent aussi limiter le nombre de messages nécessaires à leur bon fonctionnement, car la communication entre capteurs est la principale source de consommation d'énergie.

Ces contraintes [CKM00] nous obligent actuellement à repenser des solutions efficaces en terme de rapidité de calcul et de consommation énergétique, pour pouvoir sécuriser les réseaux de capteurs sans fil sans consommer leur énergie.

Dans ce papier nous présentons les spécificités des réseaux de capteurs sans fil et leurs vulnérabilités. Nous détaillons ensuite les solutions actuelles les plus courantes proposées par la communauté scientifique.

Ce papier est organisé de la manière suivante. Dans la section 2, nous discutons des spécificités des réseaux de capteurs sans fil, en insistant sur leurs vulnérabilités et leur architecture. Dans la section 3 nous listons les attaques qui menacent les réseaux de capteurs sans fil. Dans la section 4 nous présentons les solutions existantes pour contrer ces attaques et les mécanismes utilisés. Enfin dans la section 5 nous concluons sur les avancées futures.

2 Spécificités des réseaux de capteurs sans fil

Les réseaux de capteurs sans fil sont des réseaux ad-hoc spécifiques [ASSC02] avec un nombre de noeuds plus conséquents, une énergie limitée et une puissance de calcul plus faible que les réseaux ad-hoc classiques. Ce sont ces particularités que nous introduisons dans la partie suivante.

2.1 Topologie

La topologie que l'on retrouve classiquement au sein des réseaux de capteurs sans fil est un ensemble de noeuds (chaque noeud représentant un capteur) qui sont déposés de manière hétérogène sur une zone ou des objets voir des individus mouvants. Tous ces noeuds communiquent entre eux, chaque noeud peut communiquer avec les autres noeuds qui sont situés dans sa zone de couverture.

Les réseaux de capteurs sans fil sont le plus souvent reliés à une ou plusieurs bases. Ces bases ont pour mission de récupérer les informations circulant sur le réseau, et de les stocker ou bien de les envoyer directement via une liaison internet ou une liaison GSM. Ces bases peuvent être par exemple un ordinateur portable ou un capteur de puissance plus importante que les autres noeuds classiques. Elles peuvent avoir un rôle de contrôleur du réseau et elles font souvent le lien entre l'utilisateur et le réseau.

2.2 Routage

Pour limiter le nombre de communications coûteuses en énergie, les réseaux de capteurs sans fil utilisent des protocoles de routage efficaces [AKK04]. Une solution souvent utilisée est la clusterisation, qui divise le réseau en plusieurs clusters. Dans chacun de ces clusters, un noeud maître (cluster-head) est élu et aura pour mission de récupérer les informations

des noeuds du cluster dont il a la charge pour les transmettre aux autres clusters et inversement. Le choix du noeud maître sera fait en désignant par exemple le noeud avec l'énergie la plus importante, pour augmenter la vie du réseau.
D'autres problèmes de routage doivent aussi être pris en compte pour limiter le nombre de communications comme les problèmes d'implosion ou de chevauchement qui sont expliqués dans [HKB99].

2.3 La tolérance aux fautes

Dans les réseaux de capteurs sans fil, un ou plusieurs capteurs peuvent ne pas fonctionner correctement. En effet les capteurs sont des entités sensibles aux altérations d'états comme des phénomènes climatiques (humidité, chaleur, électromagnétisme) ou du fait d'une batterie faible.
Dans ce cas de figure, le réseau doit être capable de détecter ce type d'erreur est d'y remédier, en cherchant par exemple à modifier ses tables de routage pour trouver un autre chemin permettant de transmettre l'information et de maintenir le réseau toujours opérationnel. De la même manière, les capteurs doivent pouvoir détecter des capteurs défaillants qui envoient des informations erronées du fait de leur état.

2.4 Mise à l'échelle

Le nombre de capteurs utilisés dans les réseaux de capteurs sans fil peut varier de quelques entités à plusieurs dizaines de milliers. C'est d'ailleurs la principale utilité des réseaux de capteurs qui doivent pouvoir s'auto organiser à une grande échelle et être efficace quelque soit le nombre. Pour cela les protocoles des réseaux de capteurs sans fil doivent être capables de fonctionner et de s'adapter selon le nombre de noeuds.

2.5 Une énergie limitée

Les capteurs sont équipés de batteries avec une énergie limitée (plusieurs jours à quelques années). De plus, les réseaux de capteurs sans fil quand ils sont déployés, le sont souvent dans des zones difficiles d'accès pour l'homme. Il est donc difficile de pouvoir changer les batteries des capteurs. Si le nombre des capteurs dépasse la centaine d'entités, il est encore plus difficile d'intervenir pour trouver le capteur défaillant et changer sa batterie. Les capteurs sont en général déployés pour ne plus être modifiés.
La consommation de l'énergie des réseaux de capteurs sans fil doit être la plus préservée possible. Dans ce but, les capteurs actuels ont des périodes de veille durant leur temps d'inactivité pour préserver leur batterie.
Les communications sont les actions les plus coûteuses en terme d'énergie. Les calculs le sont, mais dans une moindre importance. Il est donc fortement nécessaire de limiter le nombre de communications entre capteurs et si possible le nombre de calculs.

2.6 Faible puissance de calcul

Malgré les progrès récents dans la fabrication de capteurs de plus en plus puissants, les capteurs actuels souffrent d'un manque de puissance de calcul (par exemple seulement 16 Mhz de puissance et 128Koctets de mémoire programmable pour un capteur MicaZ). Cette faible puissance ne permet pas d'utiliser des algorithmes complexes dans les réseaux

de capteurs sans fil, et particulièrement dans la cryptographie poussée.

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

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

3 Présentation des attaques

Les différentes spécificités des réseaux de capteurs sans fil (énergie limité, faible puissance de calcul, utilisation des ondes radio, etc..) les exposent à de nombreuses menaces.
Si certaines de ces menaces peuvent se retrouver dans les réseaux ad-hoc d'autres sont spécifiques aux réseaux de capteurs sans fil et s'attaquent plus particulièrement à l'énergie limitée des capteurs.

On parlera d'attaque active si un attaquant modifie l'état du réseau, et d'attaque passive dans le cas où il ne cherchera qu'à l'écouter.

3.1 Destruction ou vol

Les plus élémentaires des attaques actives dans les réseaux de capteurs sans fil sont le vol ou la destruction des capteurs. Les capteurs sont déployés dans des zones qui ne peuvent être toujours surveillées. Ainsi une personne physique seule peut subtiliser un ou plusieurs capteurs, voire peut les détruire. Si un capteur est détruit, le réseau doit être capable de s'adapter à la nouvelle situation et éviter d'être divisé en plusieurs sous-réseaux incapables de communiquer entre eux.

De plus, un noeud volé, peut divulguer certaines informations à un attaquant. Il peut tout aussi bien être reprogrammé et être réinséré dans le réseau et ainsi devenir un noeud malicieux, fonctionnant en tant que noeud espion comme expliqué dans [PPG05], [WGS+05] et [HBH04].

3.2 Attaque spécifique au type de capteur

Ce type d'attaque dépend du type de capteur utilisé sur le réseau.
Un attaquant va modifier de manière physique le comportement du capteur. Il peut par exemple allumer une flamme devant un capteur thermique ou bien allumer une lampe devant un capteur de luminosité. Le but est de tromper le capteur, et ainsi d'envoyer ou d'enregistrer de fausses informations sur le réseau, ou bien tout simplement de faire réagir assez longtemps un noeud ou le réseau pour qu'ils consomment leur énergie.

3.3 L'écoute passive

Cette attaque consiste à écouter le réseau et à intercepter les informations circulant sur le médium. Cette attaque est facilement réalisable si les messages circulant sur le réseau sont en clair. Par ailleurs cette attaque est difficile à détecter, car comme elle est passive, elle ne modifie pas l'activité du réseau.

3.4 Brouillage radio

Un attaquant va envoyer des ondes sur la même fréquence que le réseau de capteurs sans fil [WS02]. Ainsi les noeuds ne pourront plus communiquer car le médium est saturé par la brouillage radio.

3.5 L'injection de messages

L'attaquant va chercher par divers moyens à injecter des messages dans le réseau. Le but peut être de faire circuler de fausses informations ou tout simplement de saturer le réseau.

3.6 Flooding

Un attaquant va utiliser un ou plusieurs noeuds malicieux ou un dispositif particulier avec une puissance d'émission forte, pour envoyer régulièrement des messages sur le réseau pour le saturer.
On est en présence d'une attaque active qui est de même type que les attaques de type déni de service dans les réseaux classiques [WS02].

3.7 Hello Flooding

Les protocoles de découvertes sur les réseaux ad-hoc utilisent ce qu'on appelle des messages de type HELLO pour s'insérer dans un réseau et pour découvrir ses noeuds voisins.
Dans une attaque dite de HELLO Flooding, un attaquant va utiliser ce mécanisme pour saturer le réseau et consommer son énergie.

Dans [KW03], on trouve un exemple, représenté par la figure 1, d'un noeud malicieux X avec une connexion puissante qui lui permet d'envoyer à un grand nombre de noeuds des messages de type HELLO, de manière continue. Les noeuds voisins V vont alors essayer de lui répondre, même s'ils sont situés à des distances qui ne permettent pas d'atteindre le noeud malicieux. A force de tenter de répondre à ces messages ils vont petit à petit consommer l'intégralité de leur énergie.

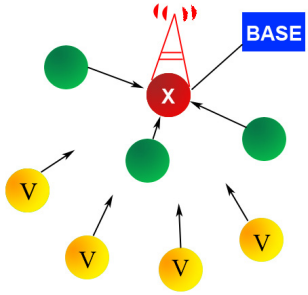

Fig. 1: *Attaque de type HELLO Flooding*

3.8 La privation de mise en veille

Cette attaque active a pour but de priver un capteur de se mettre en veille par différents moyens [SA99]. Le capteur s'il ne peut plus se mettre en veille va consommer très rapidement sa batterie, jusqu'à se retrouver hors service.

3.9 Insertions de boucles infinies

Un attaquant va modifier le routage du réseau avec un ou plusieurs noeuds malicieux, dans le but d'envoyer des messages qui vont être routés en boucles infinies et vont donc consommer l'énergie du réseau.

3.10 L'altération de message

Un noeud malicieux va récupérer un message et l'altérer, en lui ajoutant des fausses informations (sur le destinataire, l'émetteur ou les données), en le modifiant ou bien en détruisant des paquets pour rendre incompréhensible le message.

3.11 Ralentissement

Un attaquant peut programmer des noeuds malicieux qui seront comme des agents dormant et qui n'auront que pour but de ralentir l'information (par exemple avec une attaque de type trou gris).

3.12 Attaque du trou noir (black hole attack)

L'attaque du trou noir consiste tout d'abord à insérer un noeud malicieux dans le réseau [KW03].
Ce noeud, par divers moyens, va modifier les tables de routage pour obliger le maximum de noeuds voisins à faire passer l'information par lui. Ensuite comme un trou noir dans l'espace, toutes les informations qui vont passer en son sein ne seront jamais retransmises. La figure 2 représente un trou noir mis en place par un noeud malicieux X qui a modifié le routage pour que les clusters 1, 2, 3 et 4 fassent passer l'information par lui pour communiquer entre clusters. Dans ce cas de figure, le trou noir X ne retransmettra aucune information, empêchant toute communication entre les différents clusters.

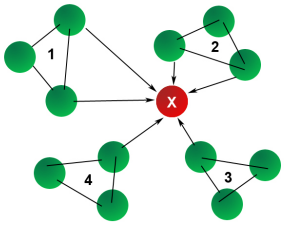

Fig. 2: *Exemple de trou noir dans un réseau clusterisé*

3.13 Attaque du trou gris (grey hole attack)

L'attaque du trou gris est une variante améliorée de l'attaque du trou noir [KW03]. Contrairement au trou noir, le trou gris relaye certaines informations. Par exemple, le trou gris va relayer toutes les informations concernant le routage, sauf pour des informations critiques. Ce type d'attaque est ainsi plus difficile à détecter que l'attaque du trou noir, le capteur malicieux tant qu'il se comporte de manière normale ne peut être détecté.

3.14 Sybil attack

Une attaque de type "Sybil attack" [NSSP04] consiste à ce qu'un capteur malicieux se fasse passer pour plusieurs capteurs. Il va ainsi pourvoir modifier la table de routage qui deviendra caduque. Un noeud malicieux qui peut se faire passer pour plusieurs noeuds peut gagner un avantage important pour une élection de noeud maître par exemple.

3.15 L'attaque du trou de ver (wormhole attack)

L'attaque du trou de ver nécessite l'insertion d'au moins deux noeuds malicieux [HPJ06]. Ces deux noeuds sont reliés entre eux par une connexion puissante comme par exemple une liaison filaire.

Le but de cette attaque est de tromper les noeuds voisins sur les distances. Généralement le protocole de routage cherche le chemin le plus court en nombre de sauts (hop). Dans le cas d'une attaque du trou de ver, les deux noeuds malicieux permettent d'atteindre un lieu éloigné avec un saut unique. Cette possibilité va tromper les autres noeuds sur les distances réelles qui séparent les deux noeuds, mais va surtout obliger les noeuds voisins à passer par les noeuds malicieux pour faire circuler les informations. Ainsi les noeuds malicieux qui forment le trou de ver vont se trouver dans une position privilégiée qui va leur permettre d'avoir une priorité sur l'information circulant à travers leurs noeuds proches. Cette attaque est représentée par la figure 3 où deux noeuds malicieux X1 et X2, reliés par une connexion puissante, forment un trou de ver. Les noeuds A et B vont alors privilégier la route la plus rapide formée par le trou de ver, et donc l'information pourra être récupérée par l'attaquant.

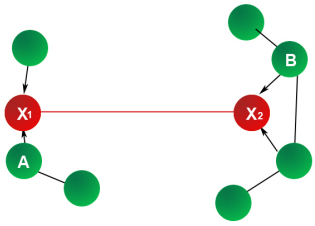

Fig. 3: *Exemple d'une attaque de type trou de ver*

3.16 L'attaque du trou de la base (sinkhole attack)

Dans cette attaque un noeud malicieux va s'attaquer directement à l'information circulant par la base, qui est le plus souvent le point qui recueille le plus d'informations de l'intégralité du réseau [KW03]. Pour cela, le noeud malicieux va proposer aux noeuds le chemin le plus rapide pour atteindre la base, en utilisant une connexion plus puissante.

Ainsi l'ensemble de ces noeuds va s'adresser en particulier à ce noeud malicieux pour transmettre l'information à la base. Toutes les informations qui transitent de ces noeuds vers la base pourront être récupérées par l'attaquant.

Pour générer une attaque encore plus puissante, un attaquant peut utiliser des stratégies de type trou de ver associées à une attaque de type trou de la base. Le but sera avec ces trous de ver de couvrir tous les noeuds du réseau. Cette situation est représentée dans

la figure 4, où les noeuds malicieux X1, X2 et X3 sont reliés par des connexions puissantes et forment des trous de ver. X3 est lui relié à la base par une connexion puissante pour réaliser une attaque du trou de la base. On parle alors d'une sphère d'influence exercée par l'attaquant sur le réseau, car il est ainsi capable de récupérer l'intégralité des informations qui circulent dans le réseau de capteurs sans fil.

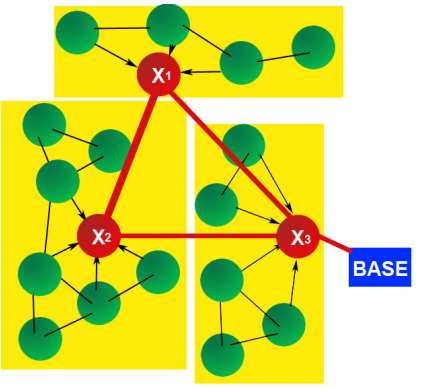

Fig. 4: *Exemple d'utilisation d'attaques de type trou de ver pour réaliser une attaque de type trou de la base*

4 Mécanismes de sécurité

Pour contrer les attaques qui menacent les réseaux de capteurs sans fil, plusieurs équipes de recherche tentent de trouver des solutions appropriées. Ces solutions doivent bien sûr prendre en compte les spécificités des réseaux de capteurs sans fil. Il faut donc trouver des solutions simples qui permettent de sécuriser le réseau tout en consommant le moins d'énergie possible et adapter ces solutions à une puissance de calcul faible.

Dans l'éventail de ces solutions, on trouve des mécanismes tels que le partitionnement de données, l'utilisation de méthodes cryptographiques adaptées, la détection d'intrus par localisation ou bien encore l'indice de confiance.

4.1 Le partitionnement des données

[TCV07] et [DHM05] offrent une solution pour empêcher la récupération d'information dans les réseaux de capteurs sans fil par le partitionnement des données. Comme son nom l'indique le but est de découper l'information en plusieurs parties.

Si un capteur cherche à envoyer une information, celui-ci va la découper en plusieurs paquets de taille fixe. Chaque paquet sera ensuite envoyé sur des chemins différents, c'est à dire qu'elles ne passeront pas par la même route et donc les mêmes noeuds. Ces paquets seront finalement reçus par la base, qui pourra ensuite les rassembler pour pouvoir reproduire l'information. Ce mécanisme oblige un attaquant à récupérer l'ensemble des paquets s'il veut pouvoir lire l'information. Il doit aussi être capable d'écouter l'ensemble du réseau, pour récupérer les différentes paquets qui circulent sur des chemins différents. Un exemple de cette solution est représentée par la figure 5, où un capteur A divise un message en 3 paquets qui vont suivre respectivement 3 chemins différents.

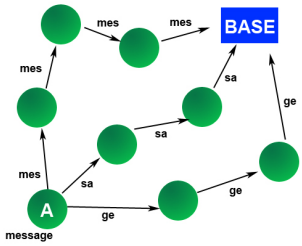

Fig. 5: *Exemple de partitionnement*

Cette solution oblige un agresseur à écouter l'ensemble du réseau et à récuperer l'ensemble des messages pour parvenir à récupérer l'information. Cependant cette solution augmente considérablement la consommation d'énergie (avec un risque de surchage de traitement), car elle solicite un nombre de noeuds plus importants.

4.2 La cryptographie

Comme nous l'avons expliqué auparavant, il n'est pas possible dans les réseaux de capteurs sans fil d'utiliser des méthodes de cryptographie complexes. La faible puissance des capteurs ne le permet pas, et quand elle le permet, le temps de calcul est trop long.

Cependant, il est possible d'utiliser des techniques de cryptographie simple avec des clés symétriques comme montré dans [ZSJ03].

Quatre types de cryptographie sont ainsi utilisés:

- Clé globale: une clé est partagée par l'ensemble du réseau. Pour envoyer un message, l'information est chiffrée avec cette clé. Une fois le message reçu, le message peut être déchiffré avec cette même clé (principe de la clé symétrique). C'est la solution la moins coûteuse en terme d'énergie, mais avec la sécurité la moins importante. Si un agresseur récupère la clé, il peut déchiffrer tout le réseau.

- Clé partagée par paire de noeuds: chaque noeud possède une clé différente pour communiquer avec un noeud voisin qui partage cette clé. Ainsi si un noeud possède "n" voisins, il aura "n" clés à stocker pour pouvoir communiquer avec ses voisins. Dans cette solution, un noeud qui cherche à envoyer un message, doit l'encrypter avec la clé du voisin qui recevra l'information. Le noeud voisin devra déchiffrer l'information pour la chiffrer à nouveau avec la clé qui correspond au destinataire suivant. C'est la solution cryptographique la plus sécurisée (l'agresseur doit récupérer chaque clé par paire de noeuds pour avoir accès à toute l'information), mais aussi la plus coûteuse en terme d'énergie et de latence. Chaque noeud intermédiaire doit déchiffrer le message du prédécesseur, puis le chiffrer avant de l'envoyer au noeud suivant.

- Clé partagée par groupe de noeuds: dans ce cas de figure, chaque groupe ou cluster partage une clé en commun qui lui permet de communiquer à l'intérieur du groupe. Les noeuds maîtres communiquent entre eux avec, soit une clé commune à tous les clusters heads, soit une clé commune par paire de cluster head. Cette solution est une solution hybride des deux premières techniques de chiffrement et apporte un compromis entre sécurité et consommation d'énergie.

- Clé individuelle: dans cette solution chaque noeud possède une clé personnelle pour chiffrer son information. Cette clé n'est connue que de la base. Ainsi un message envoyé par ce noeud circulera de manière cachée sur le réseau jusqu'à atteindre la base. Si cette solution est intéressante en terme de sécurité, elle n'apporte qu'une possibilité de communication sécurisé entre un noeud et la base, mais pas entre noeuds.

4.3 Génération

Une solution proposée par [BLM07] consiste à utiliser une clé de génération.
A chaque période ou génération, la base envoie une nouvelle clé à l'ensemble du réseau. Cette clé sert de certificat à chacun des noeuds, pour prouver son appartenance au réseau. Si un noeud non identifié tente de rentrer dans le réseau de capteurs sans fil et qu'il ne possède pas cette clé de génération, il ne pourra être accepté en son sein.

Un autre intérêt de cette technique est qu'elle permet de limiter les attaques de substitution d'un capteur et de sa reprogrammation pour être réinjecté dans le réseau.
Si ce noeud est subtilisé à l'instant 0 avec la clé de génération K(0), le temps qu'un attaquant le reprogramme pour le remettre dans le réseau il se sera écoulé un temps "x". Quand le capteur sera repositionné dans le réseau, la nouvelle clé de génération sera alors K(x). Le noeud malicieux demandera à ses noeuds voisins de rentrer dans le réseau avec la clé K(0) et non pas K(x), car il n'a pas pu recevoir la nouvelle clé. Comme K(0)!=K(x), les noeuds voisins n'accepterons pas sa requête et le noeud malicieux ne pourra pas rentrer dans le réseau.

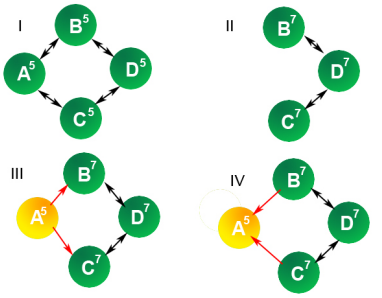

Fig. 6: *Détection de noeud malicieux par clé de génération*

Un exemple est donné par la figure 6, où quatre capteurs A, B, C, D font partie d'un réseau de capteurs qui communiquent par clés symétriques par paire de noeuds. A l'étape I, les capteurs ont pour clé de génération 5. A l'étape II, le noeud A est subtilisé par un attaquant, et pendant son absence sur le réseau, la base transmet une nouvelle clé de génération 7. A l'étape III, le capteur A reprogrammé et réinséré dans le réseau fait une demande d'insertion dans le réseau à B et C. A l'étape IV, les noeuds B et C refusent la demande de A, car en comparant leur clé de génération, ils se sont aperçus qu'elles ne correspondaient plus.
Cette technique est peu coûteuse en terme d'énergie et facile à déployer. Cependant elle ne s'adresse qu'à des réseaux fermés, qui ne peuvent pas accepter de nouveaux noeuds.

De plus, se pose le problème d'un noeud sain qui n'aurait pas pu recevoir une clé au cours du temps.

4.4 Localisation

Un mécanisme utilisé pour détecter les noeuds malicieux et particulièrement des attaques de type trou de ver, consiste à utiliser une technique de localisation géographique, comme proposé par [GSJ+03] et [LND05].
Pour cette solution, le réseau de capteurs sans fil doit être équipé de capteurs balises (beacon node), qui sont des capteurs qui connaissent leur position géographique, par exemple au moyen d'un équipement GPS.

Avec la localisation, si un capteur demande à entrer dans le réseau, les capteurs balises qui vont recevoir cette demande vont pouvoir estimer sa localisation par rapport à son domaine d'écoute. Les capteurs balises vont ensuite quadriller leur zone d'écoute respective, et chaque noeud qui a reçu la demande d'insertion dans le réseau va voter pour une zone du quadrillage qu'il est capable d'entendre. La zone qui obtiendra le plus grand nombre de voix sera considérée comme la zone où est censé se trouver le nouveau capteur.

La figure 7 montre un exemple de vote entre 4 capteurs balises A, B, C et D qui ont quadrillé leur zone d'écoute respective et qui ont chacun voté pour chaque zone de quadrillage. A la fin du vote, ils peuvent estimer la position du capteur recherché. Ce dernier doit potentiellement se trouver dans la zone avec le maximum de votes, c'est à dire dans l'exemple, la zone avec 3 votes.

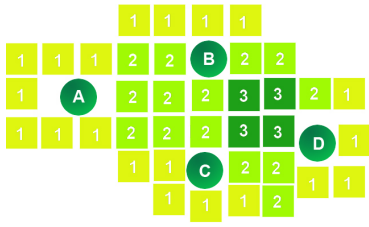

Fig. 7: *Exemple de localisation avec des capteurs de type beacon*

Dans le cas d'une attaque dite du trou de ver, les deux noeuds malicieux qui tentent une attaque vont être géo-localisés par les noeuds balises qui seront donc capables de déterminer que la distance entre ces deux noeuds est plus grande que la distance normale pour une communication en un seul saut, et ainsi détecter l'attaque. Le défaut de cette solution réside dans la nécessité du déploiement de capteurs balises équipés d'un dispositif GPS (et donc plus onéreux) ou préalablement calibrés sur le terrain.

4.5 L'indice de confiance et la réputation

Une solution proposée par [YZV03], [ZBDK04], [NV07], [RLW+04], [GS04] et [OZ07] consiste à utiliser les mécanismes de confiance et de réputation que l'on peut trouver dans les réseaux pair à pair [LS05], les réseaux de communauté ou bien encore dans les sites

marchands comme Ebay.

Dans ce type de réseau tout comme dans les réseaux de capteurs sans fil, il est difficile de savoir, au vu du nombre de noeuds, quel noeud peut être un noeud malicieux. Pour le détecter et conserver l'intégrité du réseau, chaque noeud du réseau va surveiller ses noeuds voisins et leurs actions au cours du temps. En fonction des actions réalisées par ses noeuds voisins, un noeud va augmenter une note de l'indice de confiance de ces noeuds, basée sur sa réputation. Si un noeud ne répond jamais à une requête, son indice de confiance va diminuer, de la même manière que si ce noeud retransmet toujours correctement l'information qu'on lui a demandé de transmettre, son indice de confiance va augmenter.

A l'aide de ces indices de confiance, un noeud va alors choisir le routage le plus adapté pour transmettre son information. Contrairement à des protocoles classiques de routage où le noeud chercherait le chemin le plus rapide en nombre de sauts ou de distance géographique, il va choisir ici de transmettre son information via les noeuds avec les indices de confiance les plus élévés, en d'autre terme, la route qui lui semble la plus sûre.
Ces techniques permettent d'éliminer du routage traditionnel les noeuds qui sont potentiellement dangereux, et empêcher ainsi l'information de passer par ces noeuds.

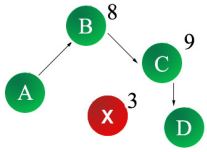

Fig. 8: *Choix de routage par réputation*

Ce mécanisme est représenté par la figure 8, où un noeud A doit transmettre une information à un noeud D. Au lieu de passer par le chemin le plus court qui passe par X, qui est un noeud avec un indice de confiance faible de 3 (sur une note de 10), et donc est potentiellement un noeud à risque, le noeud A va transmettre l'information par les noeuds B et C qui avec des indices de confiance de 8 et 9 proposent le chemin le plus sûr.

Cette solution peut être jumelée avec un méchanisme de surveillance entre voisins proches nommé méchanisme du chien de garde (watchdog) [RR06], où pour chaque communication entre deux noeuds A et B, un noeud intermédiaire C, situé dans la zone de communication, est chargé de surveiller que cette communication a bien été effectuée, comme représentée dans la figure 9.
Les solutions basées sur l'indice de confiance sont peu coûteuses en terme d'énergie et permettent, selon le type de sécurité voulu, de ne pas avoir recours à la cryptographie. Cependant pour des réseaux qui demandent une sécurité maximale, elles ne sont pas toujours adaptées. Ainsi un noeud malicieux qui enregistrerait des informations sur le réseau et, par ailleurs, se comporterait de manière normale, est difficilement détectable.

5 Conclusion

Les dernières avancées technologiques dans les réseaux de capteurs sans fil ont permis de généraliser l'utilisation de ce type de réseau.
Mais l'information est encore vulnérable à de nombreuses menaces, qui sont souvent spécifiques aux réseaux ad-hoc, voire exclusives aux réseaux de capteurs sans fil.

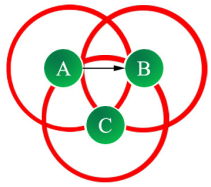

Fig. 9: *Exemple de chien de garde*

Les solutions apportées par la communauté scientifique pour contrer ces menaces ne garantissent pas toujours une sécurité maximale. La faible puissance des capteurs et surtout leur énergie limitée freinent le déploiement de techniques plus avancées, et il nous faut encore chercher des solutions qui puissent concilier sécurité, durée de vie et rapidité d'exécution des capteurs.

References

[AKK04] J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. In *IEEE Wireless Comm.*, volume 11, pages 6–28, 2004.

[ASSC02] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Comput. Netw.*, 38(4):393–422, 2002.

[BLM07] Chakib Bekara and Maryline Laurent-Maknavicius. A new resilient key management protocol for wireless sensor networks. In Damien Sauveron, Constantinos Markantonakis, Angelos Bilas, and Jean-Jacques Quisquater, editors, *WISTP*, volume 4462 of *Lecture Notes in Computer Science*, pages 14–26. Springer, 2007.

[CKM00] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. In *Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD*, 2000.

[DHM05] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. In *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 113–126, Washington, DC, USA, 2005. IEEE Computer Society.

[GS04] Saurabh Ganeriwal and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. In Sanjeev Setia and Vipin Swarup, editors, *SASN*, pages 66–77. ACM, 2004.

[GSJ+03] Marco Gruteser, Graham Schelle, Ashish Jain, Richard Han, and Dirk Grunwald. Privacy-aware location sensor networks. In Michael B. Jones, editor, *HotOS*, pages 163–168. USENIX, 2003.

[HBH04] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks: The need for secure systems. *Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder*, 2004.

[HKB99] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan. Adaptive protocols for information dissemination in wireless sensor networks. In *MOBICOM*, pages 174–185, 1999.

[HPJ06] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.

[KPC+06] Sukun Kim, Shamim Pakzad, David E. Culler, James Demmel, Gregory Fenves, Steve Glaser, and Martin Turon. Wireless sensor networks for structural health monitoring. In Andrew T. Campbell, Philippe Bonnet, and John S. Heidemann, editors, *SenSys*, pages 427–428. ACM, 2006.

[KW03] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, 2003.

[LND05] Donggang Liu, Peng Ning, and Wenliang Du. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *ICDCS*, pages 609–619. IEEE Computer Society, 2005.

[LS05] Zhengqiang Liang and Weisong Shi. Pet: A personalized trust model with reputation and risk evaluation for p2p resource sharing. In *HICSS*. IEEE Computer Society, 2005.

[MFJWM04] David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In *International Workshop on Wearable and Implantable Body Sensor Networks*, april 2004.

[NSSP04] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, pages 259–268, 2004.

[NV07] Pissinou Niki and Crosby Garth V. Cluster-based reputation and trust for wireless sensor networks. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, pages 604–608, January 2007.

[OZ07] Vladimir Oleshchuk and Vladimir Zadorozhny. Trust-aware query processing in data intensive sensor networks. In *SENSORCOMM '07: Proceedings of the 2007 International Conference on Sensor Technologies and Applications*, pages 176–180, Washington, DC, USA, 2007. IEEE Computer Society.

[PPG05] Bryan Parno, Adrian Perrig, and Virgil D. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, pages 49–63. IEEE Computer Society, 2005.

[RLW+04] Kui Ren, Tieyan Li, Zhiguo Wan, Feng Bao, Robert H. Deng, and Kwangjo Kim. Highly reliable trust establishment scheme in ad hoc networks. *Computer Networks*, 45(6):687–699, 2004.

[RR06] Lopez J. Roman R., Jianying Zhou. Applying intrusion detection systems to wireless sensor networks. In *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, pages 640–644, January 2006.

[SA99] Frank Stajano and Ross J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols Workshop*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194. Springer, 1999.

[TCV07] Michel Abdalla Thomas Claveirole, Marcelo Dias De Amorim and Yannis Viniotis. Résistance contre les attaques par capture dans les réseaux de capteurs. In *JDIR*, 2007.

[TFdGEB06] Antoine-Santoni Thierry, Santucci Jean Francois, de Gentili Emmanuelle, and Costa Bernadette. Using wireless sensor network for wildfire detection. a discrete event approach of environmental monitoring tool. In *Environment Identities and Mediterranean Area, 2006. ISEIMA '06. First international Symposium on*, 2006.

[Wel06] Matt Welsh. Deploying a sensor network on an active volcano. In *USENIX Annual Technical Conference, General Track*. USENIX, 2006.

[WGS+05] Xun Wang, Wenjun Gu, Kurt Schosek, Sriram Chellappan, and Dong Xuan. Sensor network configuration under physical attacks. In Xicheng Lu and Wei Zhao, editors, *ICCNMC*, volume 3619 of *Lecture Notes in Computer Science*, pages 23–32. Springer, 2005.

[WS02] A.D. Wood and J.A. Stankovic. Denial of services in sensor networks. *IEEE Computer*, October 2002.

[YZV03] Z. Yan, P. Zhang, and T. Virtanen. Trust evaluation based security solution in ad hoc networks. In *NordSec 2003, Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, 2003.

[ZBDK04] H. Zhu, F. Bao, R. H. Deng, and K. Kim. Computing of trust in wireless networks. In *Proceedings of 60th IEEE Vehicular Technology Conference, Los Angles, California*, September 2004.

[ZSJ03] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia. Leap - efficient security mechanisms for large-scale distributed sensor networks. In Ian F. Akyildiz, Deborah Estrin, David E. Culler, and Mani B. Srivastava, editors, *SenSys*, pages 308–309. ACM, 2003.