La sécurité dans les réseaux de capteurs sans fils

Manel Boujelben[1], Ahmed Boujelben[1], Habib Youssef [2], Mohamed Abid[1]

[1] Unité de recherche CES, Ecole Nationale d'Ingénieurs de Sfax, BPW 3038, Sfax, Tunisie
boujelben_manel@yahoo.fr, ahmed_boujelben@yahoo.fr, mohamed.abid@enis.rnu.tn
[2] Unité de recherche PRINCE, ISITC, BPW 4011, Hammam Sousse, Tunisie
habib.youssef@fsm.rnu.tn

Abstract. Le marché des réseaux sans fil s'est considérablement développé ces dernières années. De ce constat, une nouvelle branche s'est créée pour offrir des solutions économiquement intéressantes pour la surveillance à distance et le traitement des données dans les environnements complexes et distribués : les Réseaux de Capteurs Sans Fil « RCSF ». Ces réseaux sont formés par des composants minuscules appelés « noeuds de capteurs ». Ces noeuds communiquent à l'aide d'un réseau Adhoc sans fil. L'alimentation électrique de chaque capteur est assurée par une batterie individuelle dont la consommation doit être optimisée. Plusieurs travaux de recherche et de développement étudient différents aspects liés à cette nouvelle technologie. Cet article présente une synthèse sur quelques points clés en cours d'étude sur les réseaux de capteurs d'une façon générale d'une part, et la sécurité dans ces réseaux d'autre part.

1 Introduction

Les RCSF présentent une technologie très innovante pouvant assurer plusieurs fonctionnalités selon le domaine d'application où ils sont déployés. Les nœuds de capteurs présentent le composant de base des RCSF. Ces noeuds sont peu coûteux, de basse puissance et de petites tailles [1]. Ils sont capables de détecter un phénomène et de traiter l'information au niveau local ou de l'envoyer à un ou plusieurs points de collecte, à l'aide d'une connexion sans fil.
Etant donné que les RCSF peuvent circuler des données sensibles et fonctionner dans les environnements hostiles sans surveillance, il est impératif que ces soucis de sécurité soient adressés dès le début de la conception. Le but de ce travail est d'étudier les caractéristiques des RCSF en se focalisant surtout sur le problème de sécurité. Cette étude représente une base de départ pour pouvoir discerner les différentes solutions de sécurité proposées quitte à les adapter aux contraintes des RCSF. Ce papier est composé de deux sections. La première expose une présentation des RCSF. La deuxième détaille les différentes attaques qui mettent en échec ces réseaux et les mesures défensives adéquates.

2 Généralités sur les réseaux de capteurs sans fil

Les RCSF sont des réseaux Adhoc qui se distinguent par un certain nombre de différences et de défis spécifiques [1] [2]. Le nombre de noeuds dans un RCSF est plus grand que celui dans un réseau Adhoc. En plus, ces noeuds présentent des limites d'énergie, de ressources de calcul et de mémoire. La taille espérée d'un nœud serait quelques millimètres cubiques, la gamme de prix indicatif moins d'un 1$ [2].

Dans ce qui suit, on va présenter les diverses applications de ces réseaux, leur architecture ainsi que les différents composants d'un nœud de capteur.

2.1 Applications des réseaux de capteurs sans fil

Les RCSF sont actuellement déployés dans un éventail d'applications, on peut citer :
- *Le militaire* : détecter les ennemis, suivre leurs mouvements, etc.
- *Le transport* : gestion du trafic, déformation de structure, etc.
- *L'environnement* : détection des feux dans les forêts, détection de polluants dans l'air ou le sol, suivi des mouvements des oiseaux et insectes, etc.
- *Le médical* : aide à la médication, suivi des patients à distance, etc.
- *Le bâtiment* : gestion de la température et de la lumière dans un immeuble, automatisation et contrôle des applications domotiques, etc.

2.2 Architecture d'un réseau de capteurs

Les noeuds de capteur sont habituellement dispersés dans un champ de capteurs comme montré dans la figure Fig. 1. Chacun de ces noeuds a la possibilité de rassembler des données et de les router à un nœud médiateur "sink" à travers une architecture sans fil. Le sink peut communiquer avec le noeud de gestion de taches « task manager » par Internet ou satellite [1].

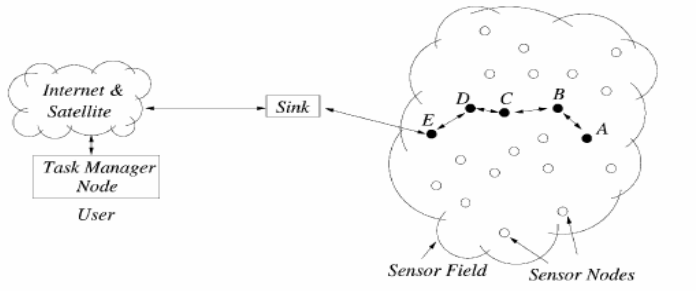

Fig. 1. Architecture d'un réseau de capteurs sans fil

2.3 Composants d'un nœuds de capteurs

Chaque nœud de capteur est formé de quatre composants de base (voir Fig. 2) :
- L'unité de détection « Sensing Unit »: se compose de deux sous unités : le capteur et le convertisseur analogique numérique (ADC).
- L'unité de traitement « Processing Unit »: elle est associée à une petite unité de stockage. Elle contrôle les procédures qui permettent au noeud de capteur de collaborer avec les autres noeuds afin d'effectuer les tâches assignées.
- L'unité de transmission « Transmission Unit »: relie le noeud au réseau.
- L'unité de puissance « Power Unit »: c'est la source d'énergie dans un nœud.

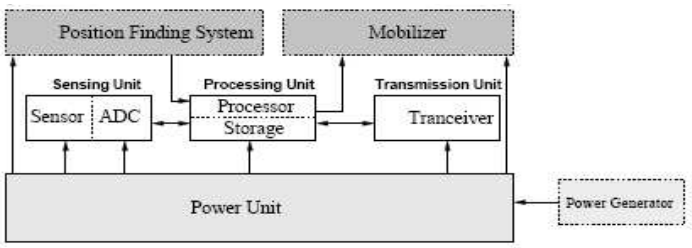

Fig. 2. Les composants d'un nœud de capteur

Un nœud de capteur peut avoir également des composants additionnels tels qu'un système de localisation « Position Finding System », un générateur de puissance « Power Generator » et un mobilisateur « Mobilizer ».

3 Sécurité dans les réseaux de capteurs sans fil

Plusieurs applications utilisant les RCSF nécessitent d'établir des mécanismes de sécurité efficaces. Cependant, en raison des contraintes de ressources, la sécurité dans ces réseaux pose des défis différents. On présentera alors dans cette section les besoins de sécurité, les attaques et les mesures défensives dans un RCSF.

3.1 Les besoins de sécurité dans un réseau de capteurs sans fil

Les RCSF doivent assurer les défis suivants [5] :

- *Confidentialité de données:* elle consiste à préserver le secret des messages échangées et ne pas les révéler à un nœud non autorisé. L'approche standard pour assurer la confidentialité est de chiffrer les données.
- *Intégrité des données* : l'intégrité des données assure qu'aucune donnée reçue n'a été changée en transit. L'intégrité est assurée en utilisant les fonctions de hachage.
- *Fraîcheur des données :* la fraîcheur de données suggère que les données soient récentes, en s'assurant qu'aucun vieux message n'a été rejoué. Pour résoudre ce problème, un compteur de temps, peut être ajouté dans le paquet.
- *Authentification* : l'authentification de données permet à un récepteur de vérifier que les données sont vraiment envoyées par l'expéditeur réclamé. Elle peut être réalisée en calculant le code d'authentification de message (MAC) des données communiquées.

3.2 Attaques

Les RCSF sont particulièrement vulnérables à plusieurs types d'attaques. Par exemple :

- Attaques de déni de service "Denial of Service attacks » : Wood and Stankovic définissent une attaque de déni de service en tant que "n'importe quel événement qui diminue ou élimine la capacité d'un réseau d'exécuter sa fonction prévue" [6]. Les attaques de DoS sont classées selon leurs occurrences dans chaque couche du modèle OSI :

  - *Au niveau de la couche physique* : une attaque peut simplement bloquer un noeud en transmettant un signal radio qui interfère avec les fréquences radio employées.

- *Au niveau de la couche liaison* : un attaquant peut simplement violer le protocole de transmission en transmettant des messages afin de produire des collisions.
- *Au niveau de la couche réseau* : un noeud peut tirer profit de la nature multi sauts du réseau en refusant simplement de router les messages.
- *Au niveau de la couche transport* : la couche transport est susceptible aux attaques, tel que l'envoie de plusieurs requêtes de demandes de connexion à un noeud.

- Attaques sur les protocoles de routage : Plusieurs attaques peuvent menacer les protocoles de routage pendant le processus d'établissement de la table de routage. On peut citer [7] :
  - *Acheminement sélectif « Selective forwarding »:* un noeud malicieux peut refuser d'acheminer certains messages en les détruisant par exemple. Une variante de cette attaque est l'attaque du trou noir « Black Hole » dans laquelle un nœud refuse de router n'importe quel message qu'il voit.
  - *« Sybil Attack » :* cette attaque est décrite comme "un dispositif malveillant prenant d'une manière illégitime des identités multiples". Cette attaque se base sur un noeud malveillant prenant l'identité de noeuds multiples, et conduisant de ce fait les multiples chemins de routage par un noeud malveillant.
  - *Attaque de trou de ver « wormholes »* : est une attaque dans laquelle un noeud malveillant écoute un paquet ou des séries de paquets, les perce dans un tunnel par le réseau de capteurs à un autre noeud malveillant, et puis réplique les paquets.
- Les attaques physiques : Les attaques physiques détruisent les capteurs de manière permanente. Par exemple, les attaquants peuvent extraire des secrets cryptographiques des noeuds, trifouiller les circuits associés « tampering », ou les remplacer avec des capteurs malveillants sous la commande de l'attaquant [8].

3.3 Mesures défensives

Plusieurs mesures défensives peuvent être employées pour satisfaire les besoins de sécurité des RCSF et pour les protéger contre les attaques [5].

- Etablissement de clef

Traditionnellement, l'établissement de clef est fait en utilisant un parmi plusieurs protocoles publics d'échange de clefs. Un des plus commun est le protocole de Diffie-Hellman. La plupart des techniques traditionnelles, cependant, sont peu convenables dans les dispositifs de basses puissances tels que les noeuds de capteur. C'est dû en grande partie au fait que les techniques typiques d'échange de clef emploient la cryptographie asymétrique.

La cryptographie asymétrique ou cryptographie à clef publique : dans ce cas-ci, il est nécessaire de maintenir deux clefs mathématiquement reliées, dont une est publique tandis que l'autre est maintenue privée. Ce type de cryptographie suppose l'utilisation de certificats d'autorité (CA) établis par une autorité centrale qui garantie qu'une clé publique appartient bien à son propriétaire et non à un usurpateur. Deux techniques principales employées pour mettre en application des crypto systèmes à clef publique : RSA et la cryptographie à courbe elliptique (ECC). Le problème de la cryptographie asymétrique, dans un RCSF, est le fait qu'elle peut rapidement épuiser les ressources énergétiques des noeuds.

La cryptographie symétrique ou cryptographie à clef secrète : Elle utilise une simple clef partagée connue seulement entre les deux hôtes communicants. Cette clef partagée est employée pour le chiffrage et le déchiffrage. L'exemple traditionnel de la cryptographie symétrique est DES (Data Encryption Standard). On peut citer aussi 3DES (triple DES), RC5, AES, etc. Le problème principal de la cryptographie symétrique est le mécanisme d'échange

de clef. Ainsi comment s'assurer que la clef est partagée seulement entre les deux hôtes qui souhaitent communiquer.

Protocoles d'établissement de clefs : plusieurs protocoles ont été proposés tels que :

- Le protocole "LEAP" décrit par Zhu et al [9] adopte un mécanisme à multiples clefs "multiple keying mechanisms". Quatre clefs différentes sont employées selon avec qui le noeud de capteur communique. Des capteurs sont préchargés avec une première clef de laquelle d'autres clefs peuvent être établies.
- Dans le PIKE [10], Chan et Perrig décrivent un mécanisme d'établissement de clef entre deux noeuds qui est basée sur la confiance commune à un troisième noeud dans le réseau.

▪ Défendre contre les attaques de DoS

Pour remédier à l'attaque de déni de service au niveau de la couche physique, on étend le spectre de communication (spread-spectrum). Pour manipuler le blocage à la couche MAC, les noeuds pourraient utiliser un contrôle d'admission de MAC qui est une limitation de taux. Ceci permettrait au réseau d'ignorer ces demandes conçues pour épuiser les réserves de puissance d'un noeud. Au niveau de la couche réseau, les noeuds le long du périmètre de la région bloquée rapportent leur statut à leurs voisins qui définissent alors en collaboration la région bloquée et conduisent simplement autour d'elle. Pour surmonter le déni de service au niveau de la couche transport le serveur doit forcer le client à utiliser ses propres ressources au début [6].

▪ Défendre contre les attaques sur les protocoles de routage

Puisque les nœuds de capteurs sans fil sont conçus de façon à avoir des contraintes de ressources, de puissance et de distributivité, des protocoles efficaces de routage doivent être employés afin de maximiser la durée de vie de la batterie de chaque nœud tout en assurant une sécurité optimale. Il y a une variété de protocoles de routage en service dans les RCSF, ainsi il n'est pas possible de fournir un protocole simple de sécurité qui pourra sécuriser chaque type de protocole de routage.

Deng, Han, et Mishra décrivent un protocole de routage tolérant aux intrusion, INSENS, qui est conçu pour limiter la portée de la destruction de l'intrus et de router loin de l'intrusion sans devoir identifier l'intrus [11].

Tanachaiwiwat, et al présentent une nouvelle technique appelée TRANS (Trust Routing for Location Aware Sensor Networks) [12]. En utilisant le µ-TESLA [13], TRANS peut s'assurer qu'un message est envoyé le long d'un chemin établi par des noeuds de confiance en utilisant le routage à base de localisation « location aware routing ».

Un problème relatif est le concept des « wormholes » dans un réseau de capteurs. Du matériel additionnel, tel qu'une antenne directionnelle [14], est utilisée pour défendre contre des attaques de trou de ver. Ceci, cependant, peut être très coûteux quand il sera déployé à grande échelle de réseau.

Pour défendre contre le « Sybil attack », le réseau a besoin d'un certain mécanisme pour valider qu'un identifiant particulier est la seule identité tenue par un noeud physique donné. Newsome et autres décrivent dans [15] deux méthodes pour valider les identités.

▪ Défendre contre les attaques physiques

Les noeuds de capteur peuvent être équipés de matériel physique pour augmenter la protection contre diverses attaques. Par exemple, pour se protéger contre le "tampering" dans les capteurs, l'une des défenses implique « tamper-proofing » le package physique du nœud [8]. Une autre approche possible pour protéger les capteurs contre des attaques physiques est « self-termination ». L'idée fondamentale est que le capteur se tue, y compris détruire toutes les données et les clefs, quand il sent une attaque.

4 Conclusion

Le déploiement des RCSF présente un grand intérêt dans plusieurs domaines étant donné la forte demande. Les nœuds de capteurs sont dynamiques, souvent alimentés par une source d'énergie autonome (batterie) et utilisent des ondes radio pour la communication. Toutes ces contraintes rendent l'application de mécanismes de sécurité efficaces et performants plus difficile.

Cet article a rappelé les différents points clés des RCSF. Un état de l'art des problèmes et des solutions de sécurité proposées pour accommoder les contraintes spécifiques de ce type de réseau a été proposé. Cependant, les différents travaux restent dans la plupart des cas théoriques et difficiles à appliquer à cause des contraintes d'énergie et de mémoire dans les RCSF, laissant ouvert l'aspect recherche dans ce domaine.

Références

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci: Wireless sensor networks: a survey. Computer networks, Volume 38, Issue 4 , 15 March 2002, Pages 393-422

[2] Holger Karl, Andreas Willig: A short survey of wireless sensor networks. Technical Report TKN-03-018, Berlin, October 2003

[3] I. Khemapech, I. Duncan & A. Miller: A Survey of Wireless Sensor Networks Technology. In PGNET, Proc. of the 6th Annual PostGraduate Symp. on the Convergence of Telecommunications, (Liverpool, UK), pp. xx-xx, EPSRC, June 2005.

[4] A. Bharathidasan, Vijay Anand Sai Ponduru: Sensor Networks: An Overview. Technical report, University of California, Davis.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary: Wireless Sensor Network Security: A Survey. Security in Distributed, Grid, and Pervasive Computing, Editor: Yang Xiao, Chapter 17, Auerbach Publications, CRC Press, 2006.

[6] A. D. Wood & J. A. Stankovic. Denial of service in sensor networks. Comp, 35(10):54–62, 2002.

[7] Chris Karlof David Wagner: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In Proc of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[8] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii. Search-based physical attacks in sensor networks: Modeling and defense. Technical report, Dept. of Computer Science and Engineering, The Ohio-State University, February 2005.

[9] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pages 62–72, New York, NY, USA, 2003.

[10] H. Chan and A. Perrig. Pike: Peer intermediaries for key establishment in sensor networks. In IEEE Infocom 2005

[11] J. Deng, R. Han, and S. Mishra. INSENS: intrusion-tolerant routing in wireless sensor networks. In Technical Report CU-CS-939-02, University of Colorado, 2002.

[12] S. Tanachaiwiwat, P. Dave, R. Bhindwale: Poster abstract secure locations: routing on trust and isolating compromised sensors in location aware sensor networks. In Proc of the 1st international conference on Embedded networked sensor systems, pages 324–325.ACM Press, 2003.

[13] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. Wireless Networking, 8(5):521–534, 2002.

[14] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In 11th Annual Network and Distributed System Security Symposium, February 2004.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press, 2004.