EasyChair Preprint

№ 4773

Security Issues in Wireless Sensor Networks (RCSFs)

Amado Illy and Tiguiane Yélémou

December 23, 2020

Problématiques de Sécurité dans les Réseaux de Capteurs Sans Fil

Amado Illy [1] et Tiguiane Yélémou[2]

[1]Université Nazi BONI, Burkina Faso
Email : (amedilly65, tyelemou)@gmail.com

Résume. Les réseaux de capteurs sans fil (RCSF) sont devenus très courants ces dernières années et leurs applications se multiplient considérablement. Ces réseaux sont composés de dispositifs sans fil miniatures qui ont une puissance de calcul et une capacité de stockage limitées. Aussi, souvent, ils embarquent une batterie comme seule source d'énergie. De plus, ces réseaux peuvent être déployés dans de milieux hostiles sans surveillance. Cette situation pose de défis sécuritaires. Les ressources matérielles limitées rendent impossible l'application des mécanismes de sécurité traditionnels au paradigme du RCSF. Par conséquent, il est nécessaire d'analyser et de mieux comprendre les exigences de sécurité de ces réseaux afin de mieux adapter les solutions existantes. Dans ce papier, nous présentons différents types d'attaques qui menacent la sécurité de communication avec les réseaux de capteurs sans fil. Nous analysons également des solutions existantes pour faire face à ces attaques et les mécanismes utilisés. Nous présentons comme perspective l'utilisation de la technologie SDN pour la sécurisation des communications dans ces réseaux.

Mots-clés : réseaux de capteurs sans fil (RCSF), ressources matérielles limitées, sécurité, vulnérabilité.

1 Introduction

Un Réseau de capteurs Sans Fil (RCSF) est un type spécial de réseau auto-organisé dédié à des applications spécifiques. Il constitue un nouveau champ de recherche visant à fournir des solutions économiquement intéressantes et faciles à mettre en œuvre pour la télésurveillance et la récolte de données dans des environnements complexes. Les RCSF se composent d'un grand nombre de nœuds déployés, qui collectent les données environnementales de manière automatisée et les transmettent vers un ou plusieurs points de collecte. Ces réseaux présentent un intérêt particulier pour les applications militaires, environnementales, domotiques, médicales et, bien entendu, les applications liées à la surveillance des infrastructures critiques.

Dans de nombreuses applications de réseau de capteurs, les données peuvent être menacées par des événements externes qui empêchent le bon fonctionnement du réseau. Dans l'article [1], l'auteur fait ressortir un état de l'art sur la sécurité dans ce type de réseau. La confidentialité, l'intégrité et la disponibilité des données sont des fonctions importantes que le réseau doit fournir. En raison des caractéristiques spécifiques de ces réseaux, notamment le manque d'infrastructure dédiée de commutation, les limitations de puissance, la topologie dynamique, le nombre important de capteurs, une sécurité physique limitée et un volume d'énergie embarquée limitée, garantir une communication sécurisée et efficace est une tâche difficile [2]. Ces capteurs sans fil sont souvent déployés dans des environnements ouverts et hostiles et sont donc soumis à différents types de menaces et d'attaques, telle que l'interception de données envoyées / reçues par le support sans fil et donc la possibilité de modifier et de répéter les données, la captation physique du capteur afin de lire les codes secrets le contenant par des moyens plus évolués. Les intrus peuvent également injecter, saturer ou endommager les équipements réseau. Dans les applications critiques, ces attaques peuvent être malveillantes et entraîner d'importantes pertes économiques et de sécurité. Malheureusement, malgré la variété des applications de réseau de capteurs, leur succès dépend de ces problématiques de leur sécurisation.

L'Objectif de notre étude est de mener une revue de la littérature sur la sécurité des réseaux de capteur enfin de bien cerner ces différents défis.

Cet article est structuré comme suit. Dans la section 2, nous discutons des spécifications des réseaux de capteurs sans fil, en mettant l'accent sur ses vulnérabilités et son architecture. Dans la section 3, nous présentons quelques attaques qui menacent la sécurité de communication avec les réseaux de capteurs sans fil. Dans la section 4, nous faisons ressortir des solutions existantes pour contrer ces attaques et les mécanismes utilisés. Enfin, dans la section 5, nous résumons et présentons des perspectives des travaux futurs.

2 Spécificités des réseaux de capteur sans fil

Un RCSF est un réseau ad hoc particulier. Les nœuds du RCSF peuvent communiquer entre eux sans passer par une infrastructure. Comparé aux réseaux ad-hoc classiques, les nœuds de capteurs composant les RCSF ont une puissance de calcul plus faible, une énergie limitée et avec un nombre nœuds plus conséquents. Ce sont ces particularités que nous présentons dans cette partie suivante.

2.1 Limitation en énergie

C'est la contrainte la plus stricte, car les capteurs sont généralement déployés dans des endroits difficiles d'accès ou inaccessibles, nous ne pouvons donc pas remplacer ou charger les batteries [3]. Si le nombre de capteurs dépasse cent entités, il est plus difficile d'intervenir pour trouver le capteur défectueux et remplacer sa batterie. La consommation d'énergie des réseaux de capteurs sans fil doit être économisée autant que possible. En termes d'énergie, la communication est l'opération la plus coûteuse. Par conséquent, il est très nécessaire de limiter le nombre de communications entre capteurs et, si possible, le nombre de calculs.

2.2 Routage

Afin de limiter le nombre de communications à forte consommation d'énergie, les RCSF utilisent des protocoles de routage efficaces. La clusterisation est une solution courante qui divise le réseau en plusieurs clusters [4]. Dans chacun de ces clusters, un nœud maître sera élu et sera chargé de récupérer les informations des nœuds du cluster,

dont il a la charge de les transmettre aux autres clusters et vice versa. La sélection du nœud maître se fera en désignant, par exemple, le nœud ayant la plus grande énergie pour augmenter la durée de vie du réseau.

2.3 Agrégation de données

La réduction de la quantité d'informations redondantes transmises par les capteurs peut prolonger la durée de vie du réseau, et la méthode utilisée est l'agrégation de données. Pour effectuer des opérations d'agrégation, un nœud intermédiaire doit avoir accès aux données transmises par ses paires pour calculer l'information utile en utilisant une fonction d'agrégation comme : la moyenne, le maximum, le minimum.

2.4 Topologie

La topologie généralement rencontrée dans les RCSFs est un ensemble de nœuds déposés de manière hétérogène sur la zone. Chaque nœud peut communiquer avec d'autres nœuds situés dans sa zone de couverture. Les nœuds de capteurs sans fil sont généralement connectés à une ou plusieurs stations de base. La tâche de ces bases est de récupérer les informations circulant sur le réseau et de les stocker, ou de les envoyer directement via des liaisons longues distances. Ces bases peuvent être, par exemple, des ordinateurs portables ou des capteurs plus puissants que d'autres nœuds conventionnels. Ils peuvent agir en tant que contrôleurs de réseau et servir généralement de lien entre l'utilisateur et le réseau.

2.5 La tolérance aux fautes

Dans un réseau de capteurs sans fil, un ou plusieurs capteurs peuvent ne pas fonctionner correctement. En fait, les capteurs sont des entités sensibles aux changements d'état. Dans ce cas, le réseau doit être capable de détecter ce type d'erreur et de la corriger. Par exemple en cherchant à modifier sa table de routage pour trouver un autre chemin permettant de transmettre des informations à la station de base. De même, le capteur doit être capable de détecter un capteur défectueux qui envoie de fausses informations en raison de son état [5].

2.6 Faible puissance de calcul

Malgré les dernières avancées dans la fabrication de capteurs de plus en plus puissants, les capacités de ces capteurs ne permettent toujours pas d'utiliser des algorithmes complexes.

2.7 Mise en échelle

Le nombre de capteurs utilisés dans les réseaux de capteurs sans fil peut aller de quelques entités à des dizaines de milliers. C'est également l'objectif principal du réseau de capteurs, il doit pouvoir s'organiser à grande échelle et être efficace quel qu'en soit le nombre. Pour cette raison, le protocole de réseau de capteurs sans fil doit pouvoir fonctionner et s'adapter en fonction du nombre de nœuds.

3 Différents types d'attaques

Les différentes caractéristiques des RCSFs (énergie limitée, faible puissance de calcul, utilisation des ondes radio, etc.) font qu'ils sont face à de nombreuses menaces [1]. Bien que certaines de ces menaces puissent être trouvées dans des réseaux ad hoc, d'autres sont spécifiques aux RCSFs.

3.1 Les attaques ciblant la couche physique et liaison

Les protocoles de couche physique sont responsables de la sélection de la fréquence porteuse, de la détection et de la modulation du signal. Les attaques de brouillage sont les plus courantes dans la couche physique d'un RCSF. Le but de ceci est de provoquer des interférences pour occuper le canal et empêcher le capteur de communiquer normalement. En ce qui concerne la couche liaison de données, elle fournit des fonctions et des moyens de traitement pour transmettre des données entre deux entités de réseau. Elle permet aussi, le plus souvent, de détecter et éventuellement corriger certaines erreurs qui se produisent sur la couche physique (en cas d'interférence ou d'atténuation des signaux électromagnétiques).

3.2 Les attaques ciblant la couche réseau

Cette couche est responsable de l'acheminement des données fournies par la couche transport tout en optimisant la consommation d'énergie. Les types d'attaques intervenant dans cette couche sont :

Attaque du trou noir

Une attaque de trou noir consiste d'abord à insérer un nœud malveillant dans le réseau. Ce nœud modifiera la table de routage de différentes manières pour forcer les nœuds voisins à faire passer leurs données par lui [6]. Comme un trou noir dans l'espace, toutes les informations qui passeront ne seront jamais transmises.

Attaque du trou de ver

Une attaque du trou de ver nécessite l'insertion d'au moins deux nœuds malveillants. Ces deux nœuds sont liés l'un à l'autre via une connexion forte. Le but de cette attaque est de tromper les nœuds voisins en termes de distance. Très souvent, les protocoles de routage recherchent le chemin le plus court en fonction du nombre de sauts.

L'attaque du trou de la base

Dans cette attaque, le nœud malveillant convaincra ses voisins qu'il est le nœud le plus proche de la station de base en utilisant une puissance de transmission élevé [4]. Par conséquent, tous les paquets reçus seront falsifiés et envoyés à la station de base.

3.3 Les attaques ciblant la couche transport

Les protocoles de couche de transport ne sont pas toujours mis en œuvre dans les réseaux de capteurs sans fil, mais lorsqu'ils existent, les attaques peuvent profiter de leurs spécifications.

Déluge de paquets SYN

Les attaques par déni de service qui existent sur le réseau classique au niveau de la couche transport peuvent également s'appliquer aux réseaux de capteurs : par exemple, si le protocole TCP est utilisé dans le réseau, un attaquant peut inonder le réseau de paquets SYN utilisés pour initier des connexions entre deux nœuds [5]. Cette attaque nécessite une machine plus puissante que le capteur (et surtout, une meilleure alimentation), mais permet à la fois de créer des congestions dans le réseau, et de saturer les capacités des capteurs en ouvrant un nombre trop grand de sessions TCP.

3.4 Les attaques ciblant la couche application

La couche application implémente éventuellement les applications utilisées par le réseau de capteurs au plus haut niveau pour fournir des services spécifiques. Les protocoles utilisés sur cette couche dépendent donc totalement de l'objectif final du réseau. Si le protocole utilisé sur la couche application induit la création de sessions en mode connexion (par exemple, TCP sur la couche transport), l'attaquant peut effectuer une attaque de désynchronisation pour détruire ces sessions. Il est également possible d'effectuer une désynchronisation sur les horloges des nœuds pour les empêcher d'établir le même référentiel temporel, ce qui peut affecter le fonctionnement normal de certaines applications.

4 Mécanismes de sécurité

En réponse aux attaques qui menacent les RCSFs, des équipes de recherche tentent de trouver des solutions appropriées. Bien entendu, ces solutions doivent tenir compte de la particularité des réseaux de capteurs sans fil. Il faut donc trouver des solutions simples pour consommer le moins d'énergie possible tout en assurant la sécurité du réseau et adapter ces solutions à une faible puissance de calcul.

4.1 La cryptographie

Il a été récemment prouvé qu'il était possible d'utiliser la cryptographie à clé publique dans les RCSF. Comme montré dans [7], l'auteur propose l'utilisation d'une technique hybride des systèmes symétriques et asymétriques. Le réseau a été initialement déployé en utilisant la pré-distribution de paires de clés asymétriques ECC (Elliptic Curve Cryptography) pour chaque nœud. Ces clés sont stockées dans le nœud avant le déploiement et sont utilisées pour établir un lien sécurisé. Ces liens fournissent l'authentification de la source et l'intégrité des données, et permettent aux nœuds d'échanger des clés symétriques en toute sécurité. La cryptographie symétrique entre les nœuds du réseau permet de garantir la confidentialité des données échangées. Toutefois, ces solutions de sécurisation (confidentialité) par le chiffrement consomment encore beaucoup d'énergie, de temps de calcul et de capacité de stockage. Et ne sont donc pas bien appropriées aux RCSF. À cette fin, des primitives cryptographiques légères ont été introduites.

Cryptographie légère

La cryptographie légère est un membre de la famille de la cryptographie, qui vise à développer un mécanisme cryptographique efficace désigné pour les appareils aux ressources limitées en termes d'espace mémoire et de puissance. Elle est considérée comme une forme plus légère de cryptographie traditionnelle.

Dans l'article [8], les auteurs ont proposé un nouvel algorithme de cryptographie léger basé sur une structure hybride robuste par fusion des techniques de chiffrement RECTANGLE, LED et SPECK. Avec l'aide de la conception hybride, ils ont réussi à améliorer les aspects de planification clés des LED et des attaques de clés associées qui étaient négligées dans le chiffrement LED.

Dans l'article [9], les auteurs proposent un algorithme de chiffrement léger appelé SIT. Il s'agit d'un chiffrement par bloc de 64 bits et nécessite une clé de 64 bits pour crypter les données. L'architecture de cet algorithme est un hybride de Feistel et un réseau de remplacement unifié. Il augmente le nombre de tours pour assurer une meilleure sécurité, mais conduit finalement à une consommation accrue d'énergie.

Dans [10], l'auteur propose un mécanisme de cryptographie léger logiciel basé sur la redondance, appelée IRC. La redondance permet d'éviter la plupart des attaques par perturbation. Il propose de réduire le coût de la redondance sur l'architecture 32 bits en utilisant le parallélisme par découpage de bits au lieu de l'implémentation 32 bits classique. En effet l'auteur utilise une implémentation efficace de 8 bits pour un schéma de chiffrement qui exploite simultanément 4 octets dans un mot de 32 bits.

4.2 Système de détection d'intrusion (IDS)

Dans l'article [4], l'auteur propose de développer et d'implémenter un ensemble de modèles de détection d'intrusion pour le réseau de capteurs sans fil à base de cluster (RCSFC), qui prend en compte les contraintes d'énergie et de mémoire des nœuds. Ces

systèmes ont la capacité de détecter les attaques de l'intérieur ou de l'extérieur du réseau, ce qui est différent des autres solutions de sécurité (telles que les techniques de chiffrement qui empêchent uniquement les attaques externes de pénétrer sur le réseau). L'auteur propose dans son modèle l'utilisation d'un algorithme d'apprentissage basé sur la SVM (Machines à vecteurs de support) en intégrant la technologie de détection basée sur les signatures d'attaques. Cet algorithme permet de minimiser la quantité d'informations échangées dans le RCSF. La réduction de la consommation est due au fait que chaque nœud échange avec ses voisins un ensemble de vecteurs clés appelé vecteur de support, contrairement au réseau de neurones où toutes les données d'entrées sont échangées entre les capteurs. Ils présentent une faible charge de communication. Les techniques de détection d'intrusion peuvent êtres divisées en deux catégories : détection basée sur les signatures d'attaques et détection d'anomalie. En effet, la combinaison de ces deux technologies permet d'obtenir un système de détection d'intrusion ayant un taux élevé de détection.

Dans [11], l'auteur s'est intéressé aux problèmes de sécurité liés aux systèmes de confiance et de réputation dans les réseaux de capteurs sans fil pour faire face aux attaques internes. Il a à cet effet proposé deux nouvelles approches nommées Bee-Trust Scheme et B-Smart. Sa première approche nommée Bee-Trust Scheme permet de résoudre le problème des recommandations malhonnêtes sous un nouvel angle en s'inspirant du modèle naturel du comportement des abeilles lors de la recherche de leur nourriture. Dans sa seconde contribution l'auteur propose un nouveau mécanisme de confiance et de réputation nommé B-Smart permettant une gestion intelligente des valeurs de réputation grâce à l'utilisation conjointe des notions de smart contract et de blockchain. L'association de ces deux concepts offre à ce protocole une grande résistance à un grand nombre d'attaques internes.

4.3 Authentification robuste

Les solutions d'authentification actuelles reposent principalement sur une forme de cryptographie. Bien que particulièrement efficaces, ces méthodes n'empêchent pas tou-

jours les attaques internes. En effet, dans le cas d'un réseau à clé partagée unique, n'importe quel nœud du réseau peut se faire passer pour un autre. Dans l'article [12], l'auteur propose une solution qui améliore la sécurité par l'intégration d'un mécanisme de vérification de mot de passe et de chiffrement des estampilles basés sur les fonctions de hachage et l'opérateur OU-exclusif. Cette méthode vise à pallier les insuffisances des solutions d'authentification qui ont été proposées au paravent. L'une de ces solutions était basée sur quatre phases : une phase d'enregistrement, une phase de login, une phase d'authentification et une phase de changement de mot de passe, ne tenant pas en compte les problèmes d'attaques par Dos. Cette solution prend en compte les attaques par Dos. Peres et al. [13] montre qu'il est possible de valider l'origine d'une trame en se focalisant sur une caractéristique physique des réseaux de capteurs sans fil, leur sédentarité. Il est en effet possible d'utiliser la puissance reçue de la trame pour évaluer la probabilité que la trame provienne effectivement d'une source hypothétique.

4.4 Localisation

En raison de l'hostilité ou de l'immensité de la zone à surveiller, la plupart de ces applications (militaires, environnementales, domotiques…) utilisent un grand nombre de capteurs déployés aléatoirement. Par conséquent, la phase de localisation est non seulement nécessaire au fonctionnement du réseau, mais également nécessaire à l'utilisation des données collectées. Dans l'article [2], l'auteur présente une proposition nommée WFDV : Wormhole-Free DV-hop pour sécuriser l'algorithme de localisation DV-Hop contre l'attaque du trou de ver. L'idée principale de l'auteur est de mettre en place une contremesure proactive à l'algorithme de base DV-Hop, nommée prévention d'infection. Il comprend deux étapes pour détecter les attaques du trou de ver. La première phase, utilise deux techniques peu coûteuses sur la base d'informations locales disponibles pendant le fonctionnement normal des nœuds capteurs. Quant à la deuxième étape, une technique plus avancée est appliquée uniquement si une attaque wormhole a été suspectée pour ignorer les messages délivrés par un lien wormhole. Cependant, s'il n'y a pas d'attaque de trou de ver, le capteur n'a pas besoin de gaspiller ses ressources inutilement.

5 Conclusion et perspectives

Les dernières avancées technologiques dans les réseaux de capteurs sans fil ont rendu possible l'utilisation généralisée de ce type de réseau. Mais les informations restent vulnérables à de nombreuses menaces, qui sont souvent spécifiques aux réseaux ad-hoc, voire exclusives aux RCSFs. Les solutions apportées par la communauté scientifique à ces menaces ne garantissent pas toujours une sécurité maximale. La faible puissance des capteurs et surtout leur énergie limitée entravent le déploiement de techniques plus avancées. Nous devons encore trouver des solutions capables d'équilibrer la sécurité, la durée de vie et la vitesse d'exécution des capteurs.

Au regard de la faible capacité de calcul et la faible quantité d'énergie embarquée des nœuds de capteurs, nous voudrons dans un futur proche investiguer une gestion centralisée de la sécurisé dans les RCSF. Dans cette approche, un contrôleur serait utilisé pour supporter les calculs complexes gourmands en temps de calcul et en consommation d'énergie. Les nœuds de capteurs se référeraient à ce contrôleur pour les différentes opérations d'authentification, de chiffrement, de contrôle d'intégrité et de traçabilité.

Références

[1] D. Martins, H. Guyennet, D. Martins, H. Guyennet, and É. De, "État de l ' art - Sécurité dans les réseaux de capteurs sans fil To cite this version : HAL Id : hal-00661898 Etat de l ' art Sécurité dans les réseaux de capteurs sans fil," 2012.

[2] F. D. E. S. Sciences and F. I. L. A. D. Hoc, "La sécurité dans les réseaux sans fil ad hoc," 2012.

[3] W. Drira, C. Bekara, M. Laurent, W. Drira, C. Bekara, and M. Laurent, "Sécurité dans les réseaux de capteurs sans fil : conception et implémentation To cite this version : HAL Id : hal-01373430 S ´ ecurit ´ e dans les r ´ eseaux de capteurs sans fil Conception et impl ´ ementation," 2016.

[4] F. D. E. Technologie, "A l'universite de tlemcen," 2013.

[5] Y. Yousef, "Routage pour la gestion de l ' énergie dans les réseaux de capteurs sans fil Yaser Yousef To cite this version : HAL Id : tel-00590407 Faculté des Sciences et Techniques Thèse de Doctorat Spécialité INFORMATIQUE présentée Par : YOUSEF Yaser Routage pour l," 2011.

[6] D. U. Paris-est, "Université Paris-Est Thèse de Doctorat Quentin Monnet contre les attaques par déni de service," 2015.

[7] I. Mansour, G. Chalhoub, and M. Misson, "Sécurité des communications dans les réseaux de capteurs sans fil (RCSF)," no. May 2000, p. 2011, 2011.

[8] A. Patil, G. Bansod, and N. Pisharoty, “Hybrid lightweight and robust encryption design for security in IoT,” *Int. J. Secur. its Appl.*, vol. 9, no. 12, pp. 85–98, 2015.

[9] M. Usman, I. Ahmed, M. Imran, S. Khan, and U. Ali, “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, 2017.

[10] B. Lac, “Cryptographie légère intrinsèquement résistante aux attaques physiques pour l ’ Internet des objets . To cite this version : HAL Id : tel-02884873 Cryptographie légère intrinsèquement résistante aux attaques physiques pour l ’ Internet des Objets,” 2020.

[11] U. Aboubakr and B. Tlemcen, “Détection des attaques internes dans les réseaux de capteurs sans fil,” 2019.

[12] Y. Faye, I. Niang, and H. Guyennet, “Authentification Robuste par Mot de Passe Basée sur une Analyse Probabiliste de Risque d ’ Attaque par Déni de Service Dans les Réseaux de Capteurs Sans Fil.”

[13] M. Peres and F. Krief, “La couche physique comme source de confiance dans les r ´ eseaux de capteurs sans fil,” pp. 2–3.