Culture Sciences de l'Ingénieur

La Revue 3E.I

école normale supérieure paris—saclay

Sécurité de ZigBee

Maxime SECHEHAYE[1]

Édité le 10/06/2024

[1] *ENS Paris-Saclay – DER Nikola tesla*

Cette ressource fait partie du N°112 de La Revue 3EI de mai 2024.

Cette ressource présente les mécanismes de sécurité présents dans le protocole de communication sans fil ZigBee. On y rappelle brièvement la structure d'un réseau ZigBee avec les différents éléments le composant avant de détailler les différents éléments qui permettent d'établir des communications sécurisées. Ces éléments mis à disposition par le protocole ne sont toutefois pas obligatoirement utilisés par des fournisseurs de solution ZigBee. On s'attachera donc à proposer des exemples de choix judicieux pour améliorer la sécurité d'un réseau ZigBee.

1 - Introduction

ZigBee est un protocole de communication qui permet à différents équipements géographiquement proches de communiquer sans fil. Il s'agit d'un protocole d'utilisation simple et peu chère, particulièrement adapté pour des réseaux sans fil personnels (*Wireless Personal Area Network*, *WPAN*) avec des applications de domotiques par exemple.

1.1 - Rappels sur l'architecture d'un réseau ZigBee

Pour pouvoir aborder sereinement le reste de cette ressource, voici un bref rappel sur l'architecture d'un réseau ZigBee avec ses différents composants.

Un réseau ZigBee est composé de trois types d'appareils :

- Coordinateur : c'est le premier membre d'un réseau ZigBee. C'est donc lui qui va le configurer. Il attribue les adresses des nouveaux membres du réseau, surveille l'état du réseau et participe au routage des messages.
- Routeur : appareil permettant de transmettre les messages en choisissant le chemin optimal pour atteindre le terminal de destination.
- Terminal : dispositif émetteur et/ou récepteur qui échange des informations avec d'autres nœuds du réseau ZigBee.

Un réseau ZigBee peut être réalisé suivant une des trois topologies suivantes : en étoile, maillée ou en arbre.

Dans la topologie en étoile (voir la figure 1), il y a un coordinateur qui se charge de l'ensemble du routage. Tous les autres nœuds du réseau sont des terminaux. C'est une topologie simple et facile à mettre en place mais dont le bon fonctionnement repose uniquement sur un nœud, le coordinateur.

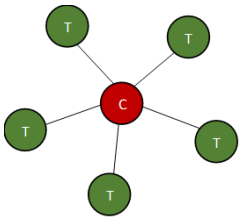

Figure 1 : Topologie en étoile d'un réseau ZigBee (C : Coordinateur, T : Terminal)

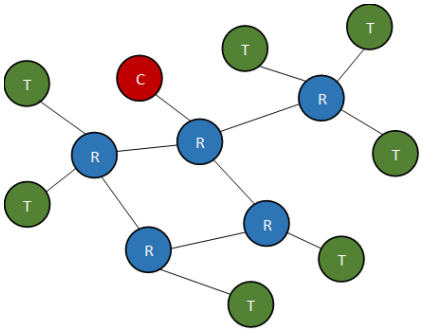

Figure 2 : Topologie maillée d'un réseau ZigBee (C : Coordinateur, R : Routeur, T : Terminal)

Dans les topologies maillée (*mesh*) et en arbre (voir les figures 2 et 3), le réseau composte des routeurs. La topologie maillée offre plus de redondance en cas de panne d'un routeur.

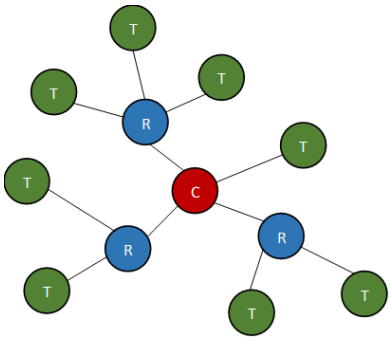

Figure 3 : Topologie en arbre d'un réseau ZigBee (C : Coordinateur, R : Routeur, T : Terminal)

1.2 - Structure d'une trame ZigBee

Voici la structure d'une trame ZigBee qui nous sera utile pour comprendre certains éléments de sécurité par la suite :

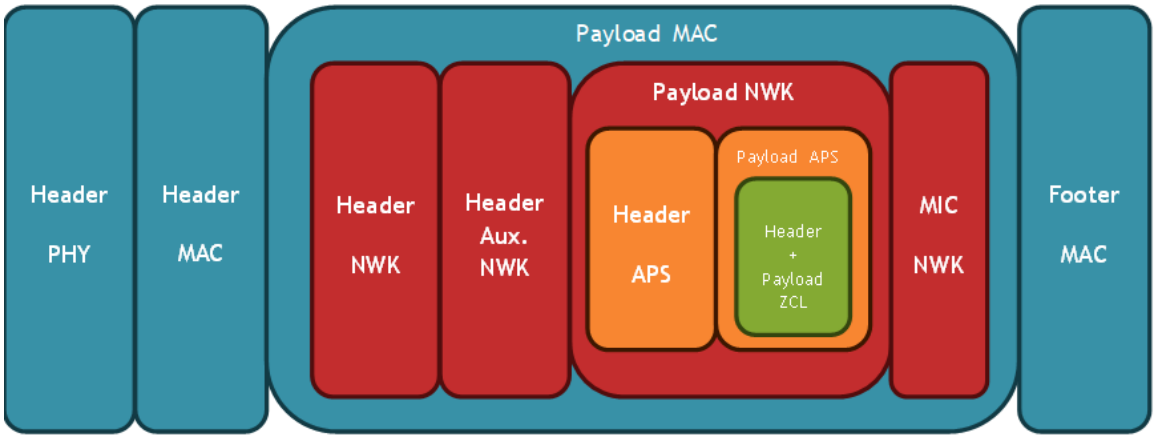

Figure 4 : Structure d'une trame ZigBee

Où PHY correspond à la couche physique, MAC signifie *Medium Access Control*, NWK représente la couche réseau, APS la couche d'application et ZCL la *Zigbee Cluster Library* (fonctionnalités courantes standardisées pour un développement plus rapide).

2 - Éléments de sécurité du protocole ZigBee

Le protocole de communication ZigBee prévoit un certain nombre d'éléments qui, si mis en place et utilisés correctement comme nous le verrons dans la suite de cet article, permettent d'améliorer la sécurité du réseau. On va ici détailler chacun de ces éléments.

2.1 - Compteur de trames

Lorsqu'un nœud du réseau ZigBee envoie un message, la trame comporte un champ correspond à son compteur de trames. Ce compteur permet d'éviter les attaques par rejeu.

Chaque nœud maintient une liste des compteurs de trames de ses voisins et de ses enfants (dans le cas d'un routeur). Ainsi, lorsqu'il reçoit un message d'un de ses voisins, il peut facilement vérifier si le compteur de trames présent dans ce message est supérieur au dernier dont il a eu connaissance. Si ce n'est pas le cas, le message est ignoré.

2.2 - Centre de confiance centralité (*Centralized Trust Center*)

Le centre de confiance centralisé est le nœud du réseau ZigBee où est centralisée la gestion de la sécurité de ce réseau. Ce nœud :

- Authentifie les nouveaux arrivants sur le réseau.
- Autorise ou non l'accès au réseau.
- Distribue les clés de sécurité.

Le choix du centre de confiance ainsi que sa politique de fonctionnement sont des choix cruciaux lors de la création d'un réseau ZigBee

Le plus souvent, le centre de confiance centralisé est confondu avec le coordinateur.

2.3 - Liste d'accès contrôlé (*Access Control List*)

Cette liste permet au centre de confiance de définir des règles d'accès au réseau ZigBee pour les nouveaux nœuds. On peut y renseigner une liste d'appareils autorisés (*white list*) ou bien une liste d'appareils interdits (*black list*). On peut également y définir des permissions accordées ou non à certains nœuds. L'implémentation de cette liste varie d'une solution ZigBee à l'autre suivant la politique de sécurité désirée.

2.4 - Clés de sécurité

Clé de sécurité du réseau (*Network Key*)

Il s'agit d'une clé de chiffrement sur 128 bits commune à tous les nœuds du réseau ZigBee et transmise lors de la procédure d'intégration au réseau. Cette clé sert à chiffrer les messages de maintenance du protocole ZigBee au sein du réseau mais aussi à chiffrer les informations réseau contenues dans les messages envoyés. C'est généralement cette clé qui est utilisée lors du calcul du code d'intégrité (*Message Integrity Code*, *MIC*) de chaque message (voir *MIC NWK* sur la figure 4).

Quand elle est transmise à un nouveau nœud, cette clé est elle-même chiffrée avec une clé préconfigurée déjà connue du centre de confiance et du nouveau nœud.

Clé de sécurité de la liaison (*Link Key*)

Cette clé de chiffrement est créée pour chiffrer les données échangées entre deux nœuds spécifiques. Les messages entre ces deux nœuds sont donc chiffrés à la fois avec la clé de liaison et la clé de réseau.

C'est le centre de confiance qui se charge de générer aléatoirement cette clé et de la transmettre aux deux nœuds concernés. Pour ce faire, une clé préconfigurée peut être partagée entre le nœud et le centre de confiance. C'est avec cette clé que le centre de confiance partagera de manière sécurisée la clé de réseau et pourra aussi générer une clé de liaison spécifique à cette session entre lui et le nouveau nœud. Ainsi, lorsque le nœud demande une clé de liaison pour chiffrer ses communications avec un autre nœud, le centre de confiance lui transmettra une clé aléatoire chiffrée avec la clé de liaison qu'il partage avec ce nœud.

Provisionnement de clé par vérification de certificat (*Certificate-Based Key Establishment*)

Il est possible d'utiliser des certificats numériques fournis par des organisations reconnues pour identifier de manière sécurisée un nouveau nœud sur le réseau ZigBee. Ce certificat permet aussi de procéder à un échange sécurisé d'une clé de liaison entre le centre de confiance et le nouveau nœud.

Politique de sécurité décentralisée (*Distributed Security*)

Depuis ZigBee 3.0, il est possible de décentraliser la sécurité du réseau. Lorsque cette politique de sécurité est choisie, ce sont les routeurs par lesquels les nouveaux nœuds entrent sur le réseau ZigBee qui sont en charge d'authentifier ces nouveaux arrivants et de distribuer les clés de sécurité. Il n'y a alors plus de nœud central qui a connaissance de tous les nœuds authentifiés du réseau.

La documentation officielle de ZigBee n'impose pas une politique de sécurité en particulier. Le choix est laissé aux fournisseurs de solutions ZigBee.

La seule obligation donnée par le protocole ZigBee est l'utilisation d'un chiffrement par bloc AES avec une clé sur 128 bits.

Sécurité « saut par saut »

Dans le protocole ZigBee, la sécurité est effectuée en mode « saut par saut » (*hop-by-hop*). Cela signifie que chaque fois qu'un paquet ZigBee passe par un routeur, ce dernier vérifie l'intégrité du paquet avec le MIC et empêche toute attaque par rejeu en vérifiant le compteur de trames.

Une fois ces vérifications effectuées, s'il n'y a aucun problème, le routeur va rechiffrer la trame avec la clé de réseau et modifier les champs du header *Aux. NWK* de la trame (voir figure 4), notamment l'adresse source ainsi que le compteur de trames. Ainsi, lorsqu'un autre routeur ou le terminal de destination recevra la trame, il pourra vérifier à nouveau qu'elle n'a pas été altérée ou rejouée.

Cette politique de sécurité permet de ne pas encombrer le réseau avec des messages corrompus ou rejoués car ils seront rapidement identifiés et ignorés. Cependant, les routeurs sont davantage

sollicités par rapport à du simple routage. C'est une des raisons pour lesquelles le protocole ZigBee n'est pas adapté pour des réseaux de grande échelle.

3 - Sécurisation de l'intégration d'un nouveau nœud au réseau

On va décrire ici les principaux éléments qui ont une influence sur la sécurité du réseau lorsqu'un nouveau nœud le rejoint.

3.1 - Protection de la clé de réseau lors de son transfert

Il est crucial de sécuriser le transfert de la clé de réseau au nouveau nœud. Le choix de la clé préconfigurée en est grandement responsable. Il existe différents choix que nous allons détailler.

Clé par défaut - « *Well-known* »

Il s'agit d'une clé préconfigurée par défaut et qui est donc connue de tous, sur tous les réseaux ZigBee. Cette clé a pour valeur hexadécimale 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39, ce qui donne après décodage ASCII « ZigBeeAlliance09 ».

Il est évident qu'il faut absolument éviter ce choix de clé préconfigurée car il n'apporte aucune sécurité au transfert de la clé réseau.

Clé préconfigurée spécifique au réseau

On peut configurer une clé qui sera choisie comme clé de lien préconfigurée pour tous les nouveaux nœuds sur le réseau.

Le déploiement de cette solution est facile car la clé est commune à tous les nœuds sur le réseau. La sécurité du transfert de la clé de réseau est alors améliorée par rapport à la clé par défaut qui est connue même à l'extérieur du réseau ZigBee concerné.

Clé de liaison dérivée à partir d'un code d'installation

Depuis ZigBee 3.0, un code d'installation (*install code*) peut être utilisé par le nœud entrant et le centre de confiance pour générer une même clé permettant de chiffrer la clé de réseau. Ce code est généré aléatoirement lors de la conception du nœud et doit être communiqué au centre de confiance du réseau avant l'arrivée du nœud dans ce réseau.

Ce même code d'installation peut ensuite être utilisé pour générer une clé de liaison entre le centre de confiance et le nouveau nœud.

Il est vivement recommandé de transmettre hors-réseau le code d'installation au centre de confiance (par QR code par exemple).

Le code d'installation permet l'authentification du nouveau nœud et garantit l'unicité de la clé au sein du réseau. C'est donc le choix apportant le plus de sécurité au transfert de la clé de réseau.

3.2 - Mise en service hors-réseau

Il est possible de transférer hors-réseau toutes les informations nécessaires à l'intégration au réseau. On évite donc de passer par le réseau où ces informations sensibles pourraient être interceptées. Différentes solutions sont envisageables :

Pré configuration lors de la conception de l'appareil

Lorsqu'on fait ce choix, la clé de réseau est présente en permanence sur l'appareil. Il n'y a alors pas le droit à l'erreur sinon l'appareil sera inutilisable. De plus, un piratage d'un tel appareil rendrait la clé de réseau accessible depuis l'extérieur, ce qui compromettrait le réseau concerné.

NFC / QR code

On peut utiliser une communication NFC ou encore un QR code pour transmettre la clé de réseau. Ces mécanismes de communication sont très faciles d'utilisation mais il ne suffit sur place que d'un lecteur pour obtenir les informations sensibles.

Site internet

On peut enfin stocker toutes les informations de sécurité dans une base de données qui est reliée à un site internet. Si on utilise les codes d'installation pour le transport de la clé de réseau, cela peut nécessiter une base de données conséquente. De plus, on ne fait que transmettre la responsabilité de la sécurité au site internet.

4 - Sécurisation après l'intégration d'un nouveau nœud au réseau

4.1 - Empêcher les attaques par reconnexion

Si la clé préconfigurée peut être réutilisée à chaque reconnexion, il est possible de simuler une tentative de reconnexion en usurpant l'identité de l'appareil et en utilisant cette clé préconfigurée. On peut alors obtenir la clé de réseau et donc compromettre l'ensemble du réseau ZigBee.

Pour empêcher ce type d'attaque, ZigBee 3.0 propose un mécanisme de négociation de clé de liaison avec le centre de confiance. Lors de la première connexion de l'appareil au réseau ZigBee avec la clé préconfigurée, le centre de confiance génère une nouvelle clé de liaison qui sera utilisée lors des reconnexions futures.

Il est recommandé de désactiver la reconnexion avec la clé préconfigurée dans la politique du centre de confiance. Si un appareil tente de se reconnecter avec la clé préconfigurée, il faudrait mettre en place une intervention manuelle au centre de confiance pour autoriser ou non cette reconnexion.

4.2 - Changer régulièrement la clé de réseau

Puisque la clé de réseau est l'élément de sécurité majeur du réseau ZigBee, il est souhaitable de la changer régulièrement afin de s'assurer qu'aucun piratage d'un ancien appareil du réseau ne vienne compromettre ce réseau. On procède ainsi :

- Le centre de confiance diffuse la nouvelle clé de réseau à tous les nœuds en la chiffrant avec la clé actuelle qui est sur le point de de devenir obsolète

- Le centre de confiance diffuse un message *Switch Key* comprenant le numéro permettant d'identifier la nouvelle clé de réseau. C'est dorénavant cette clé qui sera utilisée sur le réseau.

Pour ne pas surcharger le réseau ZigBee de messages de diffusion, il faut trouver un juste intervalle de temps au bout duquel on change la clé de réseau. C'est un compromis entre sécurité et performance du réseau ZigBee. On pourrait le faire à chaque fois qu'un appareil quitte le réseau pour s'assurer qu'un piratage de cet appareil ne compromette pas la sécurité du réseau.

5 - Conclusion

Nous avons ici observé les éléments de sécurité présents dans le protocole de communication ZigBee. Ce protocole propose différents mécanismes de sécurité et laisse beaucoup de liberté sur son implémentation. Il revient donc à l'utilisateur de ce protocole de faire les bons choix pour assurer la sécurité de son réseau. Cette sécurité repose principalement sur celle de la clé de réseau.

Nous avons pu constater que les choix sont nombreux et qu'il faut donc être conscient de leur importance, de leurs enjeux et des conséquences que tel ou tel choix peut avoir.

Cette ressource ne se veut pas exhaustive sur les politiques de sécurité possible et sur les vulnérabilités de ce protocole. Le lecteur souhaitant approfondir ces connaissances à ce propos pourra se référer au papier de NXP sur la sécurité de ZigBee [2] ainsi qu'à la présentation lors de la conférence BlackHat des failles de sécurité possibles de ZigBee et leur exploitation [5].

Références :

[1]: *ZigBee Specification*, ZigBee Alliance, 2015
https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

[2]: *Maximizing security in ZigBee networks*, NXP Laboratories UK, 2017
https://www.nxp.com/docs/en/supporting-information/MAXSECZBNETART.pdf

[3]: *ZigBee 3.0 Security*, Digi, 2018
https://www.digi.com/support/knowledge-base/zigbee-3-0-security

[4]: *AN1233 : ZigBee Security*, Silicon Laboratories, 2022

[5]: *ZigBee exploited – The good, the bad and the ugly*, Tobias Zillner, Sebastian Strobl, black hat USA 2015
https://www.youtube.com/watch?v=9xzXp-zPkjU&ab_channel=BlackHat
https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf