communications avec les concentrateurs, voire de les modifier, elle sera capable d'influencer fortement le système intelligent et connecté.

1.3 L'ÉTAT DE LA SÉCURITÉ DES DONNÉES DANS LE MONDE DES OBJETS CONNECTÉS

Nous venons d'observer que le but de ces systèmes intelligents est de récupérer un maximum de données afin de nous offrir différents services. Par exemple, une maison intelligente va récupérer des données de température, d'humidité, d'éclairage, de qualité de l'air, afin de fournir un confort à l'utilisateur. La maison va pouvoir agir sur ces variables en allumant le chauffage ou la climatisation, en allumant ou éteignant des lumières etc.

Il en est de même pour tous les objets connectés : ils mesurent une variable physique, soit pour nous transmettre l'information, soit pour la modifier via un système intelligent. Ainsi, par nature les systèmes connectés intelligents sont amenés à collecter et utiliser de nombreuses données personnelles. De ce fait, il nous paraît nécessaire de s'intéresser à la sécurité de ces données personnelles afin qu'elles ne soient pas utilisées de manière préjudiciable à l'utilisateur final.

L'ensemble de ces données peut être détourné de son utilisation de base et une personne mal intentionnée peut provoquer de lourds dommages en prenant le contrôle d'un tel système. Nous allons maintenant analyser quelques-uns des protocoles de communications utilisés dans le domaine des objets connectés. Pour ce faire, nous étudierons les spécifications des protocoles ainsi que des articles faisant une analyse détaillée pour l'un ou l'autre des protocoles. Notre but ici est d'analyser ce que peuvent apporter ces différentes solutions en matière de sécurité générale et de protection des données personnelles.

Les protocoles que nous analysons permettent principalement la communication entre capteurs, effecteurs et concentrateurs. Ainsi, des failles de sécurité dans ces protocoles permettraient

d'attaquer un système connecté de l'intérieur ou en étant proche du système (quelques dizaines de mètres tout au plus).

Deux des protocoles les plus connus et les plus utilisés, gérant la couche physique, sont ZigBee, et Z-Wave (Salman et Jain, 2015). Ces derniers ont tous subi diverses modifications depuis leur première version, permettant d'améliorer leur efficacité et leur sécurité.

Cependant, comme le montrent certaines études, des vulnérabilités subsistent. Celebucki *et al.* (2018) ont effectué une analyse de sécurité de ces trois protocoles. Ils démontrent que des vulnérabilités subsistent, notamment durant les périodes d'échanges des clés. Ils mettent aussi en évidence que certaines de ces failles sont exploitables et peuvent mener à des pertes de confidentialité ou à des attaques de déni de service.

D'après leur étude, il serait possible de s'interposer dans une communication utilisant le protocole ZigBee, en récupérant les clés au moment de l'échange. Pour Z-Wave, le problème majeur vient de la rétrocompatibilité. Si un appareil des générations précédentes se trouve sur le réseau, alors toutes les communications se feront avec le protocole de la génération la plus ancienne. Or, les anciennes générations de ce protocole sont très mal sécurisées.

En plus des problèmes précédemment décrits, d'autres interviennent indépendamment des protocoles utilisés. En effet, afin d'avoir des coûts de production les plus faibles possible, les constructeurs d'objets connectés ont bien souvent fait des coupures au niveau de la sécurité des données.

On pourra citer par exemple l'ampoule Philips Hue pour laquelle une équipe de chercheurs a réussi à récupérer la clé de signature des mises à jour de micrologiciels. Le protocole de signature utilisé est un dérivé de l'AES. Ainsi, l'équipe de Ronen *et al.* (2017) a récupéré la clé et s'en est servi pour signer des versions malveillantes de micrologiciels qu'ils ont pu installer à distance sur des ampoules.

1.3.1 CRITÈRES D'ANALYSE

Pour cette analyse, nous allons définir trois niveaux de sécurité : -1, 0 et 1. Un niveau -1 correspond à une absence de méthode ou à l'utilisation d'une méthode obscure, inconnue ou non vérifiée. En effet, la sécurité par l'obscurité contredit les principes de Kerkhoffs (Kerckhoffs, 1883), notamment celui de la conception ouverte. La sécurité par l'obscurité est déconseillée par de nombreux experts tels que Schneier (1995). Un niveau 0 correspond à l'utilisation d'une méthode dépréciée par un organisme de standardisation ou de sécurité, tel que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ou le « National Institute of Standards and Technology » (NIST). L'utilisation d'une méthode pour laquelle il existe une attaque permettant de la briser sera aussi considérée comme un niveau 0. Enfin, l'utilisation d'une méthode recommandée, mais avec un ensemble de paramètres non recommandés correspond aussi à un niveau 0. Enfin, l'attribution d'un niveau 1 de sécurité correspond à l'utilisation d'une méthode recommandée ou jugée comme acceptable par un organisme, tout en utilisant les bons paramètres. Ici, nous étudierons les propriété suivantes :

1. intégrité des communications
2. authentification des messages
3. authentification des appareils
4. impact de la rétrocompatibilité

Pour chacune des trois premières propriétés, nous utiliserons la méthode de classification en trois niveaux, comme indiqué précédemment. Pour l'impact sur la rétro compatibilité, nous ne utiliserons deux niveaux : impact fort et impact faible. Ces derniers seront décrits dans la sous-section correspondante.

Chaque propriété aura ainsi sa propre note. Cette hiérarchie en plusieurs niveaux permet de rendre compte des risques qu'engendrent les diverses méthodes utilisées. En effet, l'absence de

méthodes permettant d'assurer une des propriétés choisies rend particulièrement vulnérable un objet. Il est plus facile de l'attaquer et de le compromettre si aucun mécanisme de défense n'est mis en place.

Ici, nous voyons la sécurité des données comme un jeu, dont l'objectif serait de protéger un trésor. Si nous enterrons le trésor dans une forêt et que personne ne le surveille, alors dès qu'une personne fouillera un peu la forêt, elle trouvera notre trésor. Si maintenant, nous construisons un coffre avec une serrure et que nous faisons garder le coffre par des gardes, il sera plus difficile de trouver et de voler notre trésor. Enfin, si nous construisons un château fort, en haut d'une montagne, avec des douves, des canons et une armée pour surveiller la salle du trésor et défendre le château, il sera extrêmement difficile de dérober le trésor.

Notre analogie montre aussi qu'il faut mettre plus de moyens pour mieux sécuriser le trésor. En effet, plus l'on ajoute de couches de sécurité complémentaires, et plus il devient difficile pour un attaquant de venir dérober notre précieux trésor. On comprend donc pourquoi un objectif strict de baisse des coûts de production n'est pas compatible avec un système sécurisé. Cette analogie décrit le principe de défense en profondeur, là aussi vivement recommandé par les experts comme Schneier. "Cependant, nous pouvons aussi remarquer que le système de sécurité doit être en adéquation avec le trésor à protéger. En effet, si le système de sécurité coûte plus cher à mettre en place et à entretenir que notre trésor, alors ce système de sécurité ne sera pas viable.

Confidentialité des communications

Nous avons vu précédemment qu'un des impacts néfastes des attaques contre les objets connectés est le vol de données sensibles de l'utilisateur. Afin de réduire ce problème, il faut que les systèmes assurent une propriété de confidentialité des données. Cela se traduit par la mise en

place de méthodes afin de rendre incompréhensibles et inexploitables les données de l'utilisateur pour toute personne non autorisée. Le constructeur doit donc définir et implémenter la ou les méthodes assurant la confidentialité des données. Ainsi, si un attaquant capture les ondes émises par les objets connectés, via une technique de radio logicielle [1] par exemple (Tuttlebee, 2003), il ne pourra ni les comprendre ni les exploiter.

Intégrité des communications

Afin d'éviter qu'un attaquant puisse modifier les messages transmis par les objets connectés, il nous faut une propriété d'intégrité. Une méthode assurant l'intégrité des communications permet de détecter l'altération d'un message lors de son transport et ainsi de ne pas le prendre en compte. Cela permet d'éviter qu'un attaquant puisse modifier les messages d'un objet et ainsi donner de fausses informations au système.

Le non-respect de cette propriété pourrait, par exemple, amener un attaquant à intercepter les messages d'une serrure connectée, puis à les modifier afin que la centrale reçoive en permanence le message "la porte est fermée". Ce faisant, il pourra alors rentrer dans la maison sans déclencher l'alarme d'ouverture de porte. Ici aussi, les techniques cryptographiques sont très efficaces pour assurer cette propriété.

Authentification des messages

Afin d'éviter qu'un attaquant puisse envoyer toute sorte de messages sur le réseau, il faut implémenter une méthode d'authentification des messages. Elle permet au système de toujours savoir de quel objet provient le message, de supprimer les messages frauduleux et d'éviter

1. Technique permettant de programmer et d'utiliser n'importe quels types récepteurs et émetteurs logiciels sur un matériel générique. Ici le matériel ne fait que numériser des ondes radio, c'est le logiciel à part entière qui les interprète.

certaines injections de messages dans le réseau. L'utilisation d'un protocole ne présentant pas cette caractéristique permettra à un attaquant donner des ordres à des objets, en se faisant passer pour la centrale.

Par exemple, dans un tel cas de figure, on pourrait avoir une porte de garage connectée, s'ouvrant à la réception d'un signal particulier, que seul l'utilisateur devrait pouvoir envoyer. Dans ce cas de figure, si l'attaquant se poste à quelques mètres de distance avec une radio logicielle, il pourra alors capturer le signal et le rejouer, lui permettant ainsi d'ouvrir la porte.

Authentification des appareils

Un autre point important est la manière dont sont identifiés les appareils qui ont le droit de se connecter au réseau. En effet, il existe plusieurs méthodes et, dans le cas où il n'y aurait aucune authentification, tout appareil effectuant une requête de connexion se verrait accepté. Cela peut poser problème, car un attaquant pourrait alors connecter ses propres appareils malveillants sur le réseau de l'utilisateur. Il pourrait alors lancer d'autres attaques plus facilement et, selon les configurations du réseau outrepasser certaines méthodes de protection comme le chiffrement du réseau. C'est possible si l'ensemble du réseau utilise la même clé de chiffrement pour l'ensemble des communications. Pouvant se joindre au réseau sans approbation de l'utilisateur, l'objet de l'attaquant recevra la clé du réseau et il pourra alors s'en servir pour déchiffrer toutes les communications.

Impact de la rétrocompatibilité

Notre dernier critère d'analyse concerne la rétrocompatibilité. Cette fonctionnalité est souvent obligatoire ou fortement recommandée. Elle permet à des utilisateurs de pouvoir acheter de nouveaux équipements et de les installer chez eux, sans pour autant avoir à changer tous leurs

équipements d'origine. Cependant, la présence d'une telle fonctionnalité peut engendrer de lourds problèmes de sécurité. En effet, pour beaucoup de protocoles, les premières versions n'utilisaient aucune méthode de protection. Ainsi, il n'y avait aucune confidentialité, aucune authentification.

De ce fait, si nous avons un réseau contenant uniquement des objets neufs, utilisant les versions sécurisées des protocoles et que nous décidons d'y ajouter un équipement plus ancien, ne possédant qu'une version non sécurisée du protocole, deux cas se présentent à nous. Dans le premier, le réseau va créer un canal de communication dédié à cet objet, permettant ainsi de l'utiliser sans mettre en péril la sécurité du réseau. On va considérer ce cas comme un impact faible de la rétrocompatibilité.

Dans le second cas, le système va décider d'utiliser la même version du protocole pour communiquer avec l'ensemble des objets. De ce fait, le système va utiliser la version non sécurisée du protocole, qui est la seule disponible et utilisable par tous les objets. On va ainsi voir une baisse du niveau de sécurité de l'ensemble du réseau. On qualifiera donc cela comme un impact fort de la rétrocompatibilité.

On voit ici qu'il vaut mieux que notre protocole ait un impact faible de rétrocompatibilité. Il permet d'introduire moins de vulnérabilités et donc d'augmenter la sécurité globale de notre système intelligent. Bien entendu, une meilleure sécurité permet d'augmenter la difficulté d'une attaque contre ce système et donc de réduire les possibilités de compromission de la totalité du système. Nous allons donc attribuer un niveau -1 pour les protocoles qui ont un impact fort et un niveau 1 pour ceux ayant un impact faible.

1.3.2 ZIGBEE

Nous allons étudier dans cette section le protocole ZigBee. À l'aide des deux articles choisis (Xueqi *et al.*, 2017), (Morgner *et al.*, 2017), ainsi que des spécifications techniques (Alliance, 2014), nous avons été capables de rapidement analyser le protocole selon les critères précédemment définis. Nous ferons dans un premier temps un bref historique du protocole puis nous effectuerons l'analyse de la sécurité de ce protocole.

Historique du protocole

D'après le site officiel de ZigBee [2], le protocole ZigBee a été développé par la ZigBee Alliance, regroupant plusieurs centaines d'entreprises. Cette alliance a été fondée en 2002. Les premières spécifications du protocole ZigBee 1.0 ont été ratifiées en décembre 2004. Le protocole a été créé pour permettre la communication de petits équipements personnels, tout en utilisant le moins d'énergie possible. Le second but était de bâtir un protocole et des puces l'implémentant, au tarif le plus bas. Le protocole se base sur la norme IEEE 802.15.4 (Molisch *et al.*, 2004). ZigBee permet la mise en place de réseaux maillés, c'est-à-dire que les nœuds peuvent dialoguer entre eux, sans forcément passer par une centrale. La version que nous étudions ici est la version 3.0, déployée en 2015.

Fonctionnement général du protocole

Le protocole ZigBee est organisé en couches, un peu à la manière du modèle OSI (ISO, 1978). Ainsi, on se retrouve avec un protocole en quatre couches : physique (PHY), accès médian (MAC), réseau (NWK) et application (APL). Une représentation est donnée dans la figure 1.4

2. https ://www.zigbee.org

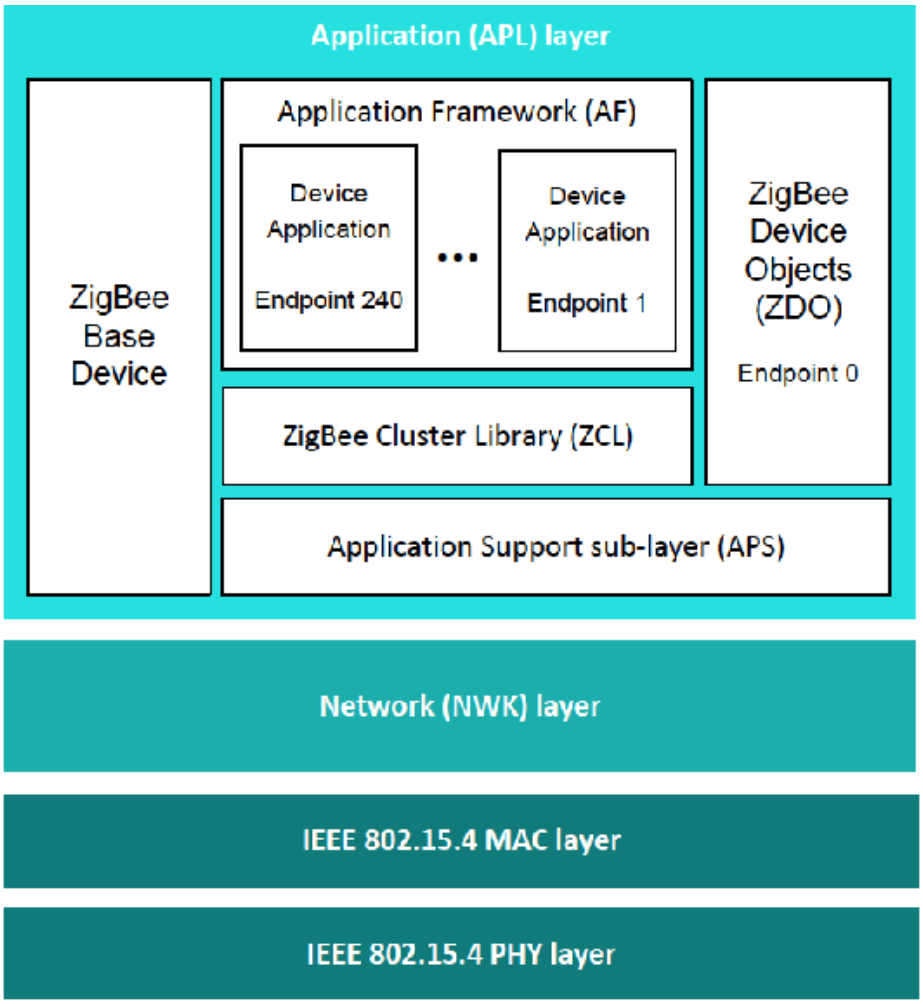

Figure 1.4 – Les couches du protocole ZigBee, tiré de Xueqi *et al.* (2017)

Ainsi, chaque couche est responsable de gérer une partie bien précise de la communication. La couche PHY est responsable de la traduction des messages en ondes physiques qui seront ensuite émises par l'appareil, puis captées et retransformées en données numériques par un autre appareil. Nous ne nous intéresserons pas à cette couche dans la suite de ce travail. Pour son fonctionnement général, ZigBee propose deux modes différents. Le premier est un mode centralisé et le second est un mode distribué. Les deux présentent des différences dans leur manière d'ajouter de nouveaux appareils dans le réseau ainsi que dans leur méthode de protection des messages. Nous voyons donc que deux de nos critères sont impactés par le mode de fonctionnement. Nous

reviendrons plus tard sur ces détails.

Analyse de sécurité

Pour commencer, il faut savoir que le protocole ZigBee assume une confiance totale entre les couches. En conséquence, les mécanismes de protection sont partagés entre les couches. D'après Fan et al. (Xueqi *et al.*, 2017), ainsi que Morgner (Morgner *et al.*, 2017), la couche MAC est définie par le protocole IEEE 802.15.4 et permet donc l'utilisation d'un algorithme de chiffrement appelé AES-CCM* (prononcé AES CCM star), utilisant une version améliorée de l'algorithme CBC-MAC faisant partie des algorithmes de code d'authentification normés par l' « International Organisation for Standardization » (ISO) ISO (2019). Il est utilisé ici avec la version AES 128, algorithme de chiffrement standard, recommandé par les grandes agences de sécurité informatique telles que l'ANSSI (ANSSI, 2014). Cet algorithme permet d'assurer les propriétés de confidentialité, d'intégrité et d'authentification des messages (Dworkin, 2004).

Cependant, il faut noter que la clé de chiffrement est partagée par tous les appareils du réseau et correspond à "la clé du réseau". Ainsi, on peut voir que si un attaquant peut connecter un équipement malveillant dans un réseau ZigBee, il obtiendra la clé de chiffrement et pourra alors compromettre les propriétés de confidentialité, d'intégrité et d'authentification des messages.

Pour la couche NWK, le principe est le même, un algorithme CCM* est utilisé, mais en utilisant les mêmes clés que pour la couche MAC. Cependant, la nouveauté de la version 3.0 de ZigBee est de pouvoir mettre en place une dernière utilisation d'un chiffrement AES-128 dans la couche APL. Dans cette dernière couche, on pourra utiliser des clés différentes de la clé de réseau afin de créer des canaux de communications sécurisés entre deux appareils. Cela peut se traduire par la mise en place d'un canal dédié entre une centrale de commande et une serrure connectée afin d'augmenter la sécurité de cette dernière (Aliance, 2017).

Maintenant que nous connaissons les mécanismes disponibles pour chaque couche, étudions les deux modes de fonctionnement du protocole afin de déterminer si ces méthodes sont correctement utilisées. D'après les équipes de recherches qui ont analysé ce protocole (Xueqi *et al.*, 2017), (Morgner *et al.*, 2017) le mode centralisé procure un plus haut niveau de sécurité. En effet, dans le mode distribué, tous les appareils doivent utiliser une clé de lien prédéfinie, pour obtenir la clé du réseau. Cette première clé, utilisée pour transmettre de manière chiffrée la clé du réseau lors de l'ajout d'un nouvel équipement, est pré-configurée par les constructeurs et devient donc la même pour tous les appareils.

Ensuite, tous les nœuds utilisent la même clé de réseau pour communiquer. Nous voyons ici une faille importante. Lors de l'appareillage, la clé du réseau est transmise à un nouvel appareil en étant chiffrée. Or comme la clé de chiffrement utilisée est connue de tous, elle devient inutile puisque tout le monde peut l'utiliser pour déchiffrer le message contenant la clé du réseau. Ainsi, dans leurs travaux, les chercheurs ont réussi à obtenir la clé du chiffrement d'un réseau ZigBee en capturant les paquets lors de l'ajout d'un nouvel appareil au réseau (Xueqi *et al.*, 2017). À partir de là, plus aucune des mesures de protection utilisées par le protocole ZigBee n'est efficace.

Concernant le mode de communication centralisé, nous pouvons observer une sécurité accrue. En effet, ce mode de communication fait intervenir un équipement particulier, appelé le centre de confiance (« Trust Center » ou TC en anglais). Cette nouvelle entité permet de centraliser la sécurité du réseau. Elle possède plusieurs fonctionnalités comme la gestion des clés et l'autorisation d'ajout de nouveaux nœuds dans le réseau. Ce dernier peut ajouter un appareil sur le réseau en utilisant une clé préconfigurée globale (la même que pour le mode décentralisé) ou une clé unique pour chaque paire d'entités. Le TC supporte aussi la mise en place de listes de contrôle d'accès (ACL) afin de déterminer à l'avance les appareils pouvant se joindre au réseau. Cette méthode d'authentification des appareils avec la méthode des clés uniques préconfigurées

est recommandée par des organismes de sécurité. On voit donc ici un plus grand niveau de sécurité, car le TC va pouvoir utiliser des clés différentes pour communiquer avec chaque nœud, permettant ainsi de conserver les propriétés de confidentialité, d'intégrité et d'authentification, même si certains appareils se sont fait corrompre. Cependant, il faut noter que cela n'est possible qu'avec des appareils compatibles dont le constructeur a correctement défini la clé unique, utilisable entre le TC et le nouveau nœud. Si cette clé n'existe pas, ce sera la clé globale, connue de tous, qui sera utilisée. C'est ce qui s'est passé dans l'expérience menée par Fan et al. (Xueqi *et al.*, 2017).

Pour finir, les spécifications de ZigBee indiquent que tous les appareils d'un même réseau doivent utiliser la même version du protocole et utiliser le même mode de communication. De plus, tous les appareils doivent être rétrocompatibles. Nous pouvons traduire cela par un impact fort de la rétrocompatibilité sur le protocole.

Outils et attaques disponibles

Afin de tester la sécurité d'un réseau ZigBee, plusieurs outils dont les sources sont libres ont été créés. Le principal est un cadriciel (ou «framework") appelé « KillerBee » [3]. Ce dernier permet d'implémenter facilement, à l'aide de composants matériels dédiés, quelques attaques simples contre les objets ZigBee. Il a d'ailleurs été utilisé par les équipes de recherches précédemment citées. Il existe aujourd'hui des surcouches pour ce logiciel, par exemple « SecBee » [4] et «Z3sec» [5]. Ces outils permettent de mettre en place diverses attaques, par exemple l'attaque « Touchlink » (Morgner *et al.*, 2017), la capture, l'analyse et le rejeu de paquets ou l'envoi massif de paquets afin de saturer le réseau (aussi appelé «flood"). L'attaque basée sur la fonctionnalité « Touchlink » permet à un attaquant d'ajouter un équipement frauduleux au sein d'un réseau

3. https ://github.com/riverloopsec/killerbee
4. https ://github.com/Cognosec/SecBee
5. https ://github.com/IoTsec/Z3sec

ZigBee. L'équipe de Morgner *et al.* (2017) montre que la présence d'un seul objet possédant cette fonctionnalité dans le réseau peut compromettre la totalité de la sécurité de ce dernier.

Enfin, certaines attaques de déni de service sont impossibles à contrer avec ZigBee. C'est le cas notamment de toutes les attaques sur le spectre ondulatoire. En effet, si un attaquant sature le spectre en utilisant une antenne de forte puissance, les objets ZigBee changeront sans cesse de canal de communication, sans jamais pouvoir se stabiliser.

Ainsi, nous pouvons conclure que la sécurité d'un réseau utilisant le protocole ZigBee dépend énormément de ses équipements et de sa configuration initiale. Un bon niveau de sécurité peut être atteint, si l'on utilise un mode de communication centralisé, avec uniquement des appareils en version 3.0 et disposant d'une clé préconfigurée unique. Il ne faut pas non plus que des objets ayant la fonctionnalité « TouchLink » soient présents sur le réseau. L'ajout d'une liste de contrôle d'accès permet aussi de mieux authentifier les appareils devant se joindre au réseau. Toute autre configuration est vulnérable.

1.3.3 Z-WAVE

Nous allons étudier dans cette section le protocole Z-Wave. À l'aide des trois articles choisis Yassein *et al.* (2018), (Badenhop *et al.*, 2017), (Rouch *et al.*, 2017) nous avons été capables de rapidement analyser le protocole selon les critères précédemment définis. Nous ferons dans un premier temps faire un bref historique du protocole puis nous effectuerons l'analyse de la sécurité de ce protocole.

Historique du protocole

Z-Wave est un protocole propriétaire, développé à partir de 2001 par la société Zensys (Ehrlich, 2008). À la base, le protocole se destinait à être principalement utilisé pour la création de

maisons intelligentes. L'entreprise fut rachetée à plusieurs reprises et la conception du protocole a mené à la création de la Z-Wave Alliance en 2005. La première version du protocole avait pour objectif de fournir de bonnes performances et ne proposait ainsi que peu de sécurité. De plus, les spécifications techniques et le code du protocole n'ont été dévoilés en partie, qu'en 2016. Avant, les études de code étaient très restreintes et les chercheurs et développeurs devaient signer des clauses de non-divulgation. Ainsi, l'étude de ce protocole fut ardue pour les équipes de chercheurs.

Fonctionnement du protocole

Tout comme le protocole ZigBee, Z-Wave est organisé en couches : la couche physique (PHY), la couche médiane (MAC), la couche adaptative contenant trois sous-couches (SAR, NWK, ENC), la couche LLC et enfin la couche applicative (APP). La couche physique sert (comme pour ZigBee) à transformer les données en signal radio. La couche MAC implémente les mécanismes d'approbation de frames, de validation de données et de retransmission. Cette couche est basée sur la norme IEEE 802.11 Yassein *et al.* (2018).

Contrairement à ZigBee, la couche MAC ne va pas fournir des méthodes pour sécuriser le protocole. La sécurité est ici faite majoritairement par la couche adaptative et notamment par la sous-couche ENC. La sous-couche réseau NWK permet de router les paquets à travers le réseau maillé, la sous-couche SAR permet de reformer les paquets qui ont été segmentés. La couche de chiffrement ENC permet de chiffrer les données avec un algorithme AES-128. Elle fournit aussi un algorithme CBC-MAC lui permettant d'assurer les propriétés de confidentialité, intégrité et authentification des communications. Nous pouvons observer que ce sont les mêmes méthodes utilisées pour assurer la sécurité du protocole ZigBee. La couche LLC permet de définir la manière dont doivent dialoguer les modules Z-Wave. Elle correspond à un jeu de commandes qui peut être envoyé et reçu. La couche application est développée par le programmeur afin de créer

un service tel que le changement de couleur d'une ampoule en fonction de la commande reçue. Ainsi, nous allons principalement analyser la couche adaptative, responsable de la sécurité du protocole.

Analyse de sécurité

Afin d'analyser la sécurité de ce protocole, les chercheurs ont dû développer diverses plateformes de radio logicielle afin de pouvoir capturer les paquets du réseau et les injecter. Cela permet aux chercheurs de se faire passer pour des utilisateurs légitimes, s'ils connaissent les clés du réseau. De plus, il faut noter que les réseaux Z-Wave sont composés de capteurs et effecteurs classiques, ainsi que d'un équipement particulier appelé «Gateway". Ce dernier permet de faire les liaisons entre les appareils, d'ajouter des nœuds dans le réseau et de lier les équipements au réseau internet. Nous apprend dans les articles (Yassein *et al.*, 2018; Badenhop *et al.*, 2017) que pour la version S2 de Z-Wave, le routeur va utiliser des clés uniques pour intégrer des équipements dans le réseau. Ces clés sont en général indiquées sur la boite de l'équipement que l'on veut intégrer. Il va ensuite y avoir un protocole d'échange de clé ECDH (Elliptic Curve Diffie Hellman), très robuste et recommandé par l'ANSSI. Cela change énormément par rapport à la précédente version qui utilisait une clé de chiffrement composée uniquement de "0" afin de chiffrer la clé du réseau. De plus, pour ajouter un nouvel élément dans le réseau il suffisait d'appuyer sur un bouton et la «gateway » ajoutait au réseau tous les équipements qui en faisaient la demande.

En fin d'année 2017, Rouch *et al.* (2017) ont réussi à créer un contrôleur universel Z-Wave, leur permettant de prendre le contrôle d'un de ces réseaux. Ici, les chercheurs capturent le «Home ID » du contrôleur originel en écoutant le réseau cible. Ensuite, ils fabriquent un faux fichier de sauvegarde et s'en servent pour forcer le contrôleur frauduleux à utiliser le «Home ID » du contrôleur sain. Ils utilisent cette méthode, car autrement il est absolument interdit

par les spécifications du protocole de choisir la valeur du «Home ID". Ensuite, les chercheurs éteignent un court moment le contrôleur sain et utilisent le contrôleur malicieux pour récupérer les connexions avec les noeuds du réseau.

Nous voyons ici une attaque intéressante, permettant aux attaquants de prendre la main sur n'importe quel réseau Z-Wave. Cependant, cette dernière requiert un accès proche du réseau cible, ainsi qu'un moyen pour redémarrer le contrôleur cible. Cela peut se faire physiquement ou en coupant la source d'énergie du bâtiment. Cette technique est donc difficile à mettre en place. De plus, dans un réseau utilisant complètement la dernière version du «secure mode", ce genre d'attaque devient impossible.

Pour finir, on apprend que les versions S0 et S2 ne sont pas compatibles et que très peu de produits possèdent la version S2 du protocole. De plus, bien que les spécifications Z-Wave S2 permettent l'utilisation de chiffrement AES et de ses dérivés, la certification n'oblige pas cette utilisation. En mai 2018, seule une quarantaine de produits étaient certifiés S2 sur le marché européen (Tierney, 2018).

En conséquence, si l'on veut utiliser un produit en version S0 dans le réseau il faut rétrograder l'ensemble de la sécurité du réseau. C'est d'ailleurs la base d'une attaque trouvée en 2018 par un laboratoire de chercheurs (Tierney, 2018). Cette dernière permet de rétrograder la sécurité d'un réseau Z-Wave S2 en une version S0. Pour ce faire, il suffit d'utiliser un objet frauduleux, faisant croire au réseau qu'il ne possède pas la version S2 du protocole. L'impact de la rétrocompatibilité est donc fort.

Contrairement au protocole ZigBee, il existe peu d'outils pour faciliter l'exploitation de réseaux Z-Wave. Seuls quelques «sniffers » physiques existent, mais ce sont les équipes d'experts qui développent leurs propres outils.

Tout comme pour le protocole ZigBee, la sécurité d'un réseau Z-Wave dépend principalement des

objets qui le composent et de la configuration mise en place par l'utilisateur. Il est possible d'avoir un réseau sécurisé à condition de n'avoir que des équipements S2, qui sont malheureusement peu nombreux. La faille nommée «Z-Shave", permettant de forcer l'ensemble du réseau Z-Wave à utiliser la version 0 (non sécurisée) reste tout de même préoccupante, car elle affecterait environ 100 millions d'appareils (cyberveille sante.gouv.fr, 2018).

1.3.4 SYNTHÈSE

Nous venons de voir que les deux protocoles analysés possèdent des configurations dans lesquelles les propriétés définies plus tôt sont respectées. Nous pouvons résumer cela dans la Table 4.1 :

Protocole	Confidentialité	Intégrité	Authentification des messages	Authentification des appareils	Impact de la rétro compatibilité
ZigBee 3.0	AES-128 Niveau 1	CCM* Niveau 1	CCM* Niveau 1	Clé pré-configurée Niveau 1	Impact Fort Niveau -1
Z-Wave S2	AES-128 Niveau 1	CBC-MAC Niveau 1	CBC-MAC Niveau 1	Clé pré-configurée Niveau 1	Impact Fort Niveau -1

Tableau 1.1 – Niveau de sécurité des protocoles ZigBee et Z-Wave

Nous pouvons donc observer que, dans les meilleures configurations, les protocoles sont globalement bien sécurisés. De plus, on observe que les deux protocoles utilisent les mêmes algorithmes pour garantir leur propriété de confidentialité et d'authentification des appareils. Leur seul point faible se trouvant au niveau de la rétrocompatibilité, qui oblige un abaissement général du niveau de sécurité si l'on souhaite utiliser d'anciens modèles. Les deux protocoles sont ainsi similaires et l'un ne surpasse pas l'autre selon nos critères.

Cependant, il faut noter que cette situation idéale n'est que peu réelle. En effet, ces dernières demandent des efforts à l'utilisateur qui se doit de paramétrer correctement le réseau. En effet, nous avons vu que la majorité des équipements Z-Wave ne possèdent pas la version sécurisée S2. De plus, le mode de communication par défaut des équipements ZigBee est le mode décentralisé pour plus de simplicité d'utilisation. Enfin, tous les articles que nous avons utilisés pour analyser ces deux protocoles mettaient en place des attaques contre ces protocoles.

Ainsi, des chercheurs ont réussi à capturer des clés de réseau ZigBee (Xueqi *et al.*, 2017) ce qui leur a ensuite permis d'espionner le réseau, de forger de faux paquets et de les injecter dans le réseau. D'autres chercheurs ont utilisé la fonctionnalité «Touchlink » de ce même protocole pour prendre le contrôle total d'un réseau ZigBee (Morgner *et al.*, 2017). Ils ont montré que la présence d'un seul équipement ayant cette fonctionnalité activée était suffisante pour mettre en péril toute la sécurité du réseau. Pour Z-Wave, les équipes ont réussi à attaquer le protocole de routage des paquets afin de créer une attaque "trou noir" (Badenhop *et al.*, 2017). Cette attaque leur permet de faire en sorte que les appareils ne puissent plus communiquer entre eux et ce sans qu'ils s'en rendent compte. Plus récemment, une équipe de chercheurs à réussi à exploiter une faille permettant de forcer un réseau Z-Wave à utiliser la version S0 du protocole, très peu sécurisé (Tierney, 2018).