Information Security

Zigbee 3.0 - Ein Neustart mit alten Schwächen

Eine Sicherheitsanalyse des ZigBee 3.0 Protokolls und Entwicklung eines Tools zur Ermittlung von Verbreitungsdaten

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Manuel Graindl

1610619511

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: Tobias Zillner, BSc MSc MSc

Betreuer/in: FH-Prof. Prof. (h.c.) Dipl.-Ing. (FH) Thomas Brandstetter, MBA

St. Pölten, 14. Januar 2019 _____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

*

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/-Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

ZigBee 3.0 ist die neueste Version des ZigBee Standards und basiert auf Revision 21 der ZigBee Spezifikation. Der ZigBee Standard legt ein standardisiertes Vorgehen bei der Kommunikation zwischen Internet of Things Geräten vor und ist einer der weitest verbreitetsten Standards im IoT Bereich.

ZigBee Geräte haben sich in der Vergangenheit immer wieder als verwundbar herausgestellt, wobei erfolgreich Angriffe gegen ZigBee Geräte und Netzwerke durchgeführt wurden. Daher wurde im Zuge dieser Diplomarbeit darauf eingegangen, welche Sicherheitsmechanismen ZigBee 3.0 bietet und wie diese implementiert sind. Im weiteren Verlauf wurde untersucht, ob sicherheitstechnische Schwachstellen von früheren ZigBee Protokollversionen mit ZigBee 3.0 behoben wurden.

Bei der Analyse des ZigBee Pro Standards hat sich herausgestellt, dass es in der Art und Weise wie Sicherheitsmaßnahmen bei ZigBee Netzwerken und Geräten implementiert sind, wenig Änderungen gegeben hat. Daher können viele Angriffe, welche auch bei älteren ZigBee Versionen funktioniert haben, auch bei ZigBee 3.0 noch durchgeführt werden. Eine Ausnahme waren hierbei Replay-Angriffe, welche unter ZigBee 3.0 nicht mehr durchführbar sind, da Frame Counter nicht mehr einfach zurückgesetzt werden können.

Ein weiterer Hauptfokus dieser Diplomarbeit lag auf der Ermittlung der Verbreitung von ZigBee 3.0 Geräten und deren tatsächlich eingesetzten Sicherheitsmaßnahmen. Hierzu wurde via „Warwalking“ Daten von ZigBee Netzwerken in Industrie- und Wohngebieten gesammelt. Hierzu wurde ein Warwalking Tool entwickelt, mit welchem man durch die Verwendung von „CC2531 Dongles“ ZigBee Netzwerke aufspüren und Kommunikationen mitlesen kann. Bei der Auswertung der Daten hat sich herausgestellt, dass die Durchdringung von ZigBee Geräten in industriellen Gebieten deutlich höher ist als in Wohngebieten, wobei ein Großteil der gefundenen Systeme Beleuchtungssysteme sind. Das allgemeine Sicherheitsniveau von Netzwerken, sowie die Tatsache ob es sich um ZigBee 3.0 Geräte handelt, konnte nicht ermittelt werden da diese Art von Informationen nicht im Header der ZigBee Nachrichten mitgesendet werden.

Inhaltsverzeichnis

1. Einführung

ZigBee Pro ist ein 2015 veröffentlichter offener Standard, welcher die kabellose Kommunikation zwischen IoT Geräten regelt. ZigBee Geräte, welche sich an die ZigBee Pro 2015 Spezifikation halten, werden auch ZigBee 3.0 Geräte genannt. Der Zigbee Standard wird von der Non-Profit Organisation ZigBee Alliance entwickelt, welche 2002 gegründet wurde. Die ZigBee Alliance hat es sich zum Ziel gesetzt, flexible, zuverlässige und einfach anzuwendende Standards für die immer smarter werdende Welt zu entwickeln. ZigBee 3.0 wurde mit dem Hintergrund entwickelt, eine Lösung für alle Märkte bereitzustellen. Beispiele hierfür sind Heimautomatisierung, Industrie, Baugewerbe, Einzelhandel, Gesundheitssektor, und viele mehr. Zusätzlich wird auch die Kompatibilität mit älteren Zigbee Geräten und Services gewährleistet. Der ZigBee 3.0 Standard soll somit alle ZigBee Alliance Entwicklungen unter einen Hut bringen. [1][2]

1.1. Was ist ZigBee 3.0?

ZigBee 3.0 ist die neueste Version des ZigBee Standards und basiert auf Revision 21 der ZigBee Spezifikation. [3] Bei ZigBee 3.0 handelt es sich um einen globalen Standard, welcher die Funk-Kommunikation zwischen Internet of Things (IoT) Geräten regelt, die auf niedrigen Stromverbrauch ausgelegt sind. Weiters gibt der ZigBee Standard das Standardverhalten von Geräten vor. Dies soll dazu dienen, dass unterschiedliche Hersteller sich darauf verlassen können, dass spezifische Geräte wie beispielsweise Glühbirnen immer auf dieselbe Art und Weise auf bestimmte Befehle reagieren. ZigBee ist neben Z-Wave [4] und Thread [5] eines der vielversprechendsten IoT Protokolle der letzten Jahre. Das ZigBee Protokoll wurde in der Vergangenheit mehreren Sicherheitsanalysen unterzogen und es wurden immer wieder Schwachstellen entdeckt, welche von Angreifern erfolgreich ausgenutzt werden konnten.

1.2. Problemstellung

Smart Homes und das Internet of Things (IoT) gewinnen immer mehr an Bedeutung. Angefangen von der Glühbirne, welche je nach Uhrzeit und Lichtverhältnissen die Beleuchtung anpasst, bis hin zum Kühl-

schrank, der automatisch Lebensmittel nachbestellt, sollten diese zu Ende gehen. Viele private Haushalte, aber auch Firmen, bauen immer mehr auf IoT Geräte um Abläufe zu automatisieren oder Strom- und Heizkosten zu sparen. ZigBee ist einer der am weitest verbreitetsten Standards im IoT Bereich und wird von Firmen wie Philips, Amazon, Qualcomm, und vielen mehr eingesetzt. Durch die steigende Anzahl an IoT Geräten steigt auch die Gefahr von Angriffen gegen IoT Netzwerke, da diese ein immer lukrativer werdendes Angriffsziel darstellen. Folgend werden Problemstellungen vorgestellt, welche in dieser Diplomarbeit behandelt werden.

1.2.1. Sicherheit

ZigBee Geräte haben sich in der Vergangenheit immer wieder als verwundbar herausgestellt und es konnten erfolgreiche Angriffe gegen ZigBee Geräte und Netzwerke durchgeführt werden. [6][7] In dieser Diplomarbeit wird ZigBee 3.0, die neueste Version des ZigBee Standards, einer Sicherheitsanalyse unterzogen und die implementierten Sicherheitsmechanismen evaluiert. Weiters wird ein Vergleich zu vorherigen ZigBee Version gezogen um heraus zu finden, was sich in Bezug auf die Sicherheit verändert hat und ob bekannte Angriffsvektoren nach wie vor ausnutzbar sind.

1.2.2. Verbreitung

Ein weiterer Teil dieser Diplomarbeit ist die Ermittlung der Verbreitung von ZigBee Geräten. Zu diesem Thema gibt es kaum Informationen, daher wird im Rahmen dieser Diplomarbeit ein Warwalking / -driving Tool entwickelt, um ZigBee Geräte und Netzwerke zu lokalisieren. Dadurch sollen zuverlässig Daten zur Verbreitung geliefert werden.

1.3. Forschungsstand

Im Bereich ZigBee Security wurden über die Jahre mehrere Sicherheitsanalysen und auch erfolgreiche Angriffe gegen ZigBee Netzwerke durchgeführt. Folgend sind Beispiele für bisherige Sicherheitsanalysen angeführt.

T. Zillner hat in seiner Forschungsarbeit „ZIGBEE EXPLOITED The good, the bad and the ugly“ (2015) beschrieben, dass das Sicherheitslevel der ZigBee Sicherheitsarchitektur darauf beruht, dass die symmetrischen Schlüssel sicher gespeichert sind beziehungsweise bei der Auslieferung der Geräte bereits auf diesen vorhanden sind. Auf diese Art müssen die symmetrischen Schlüssel, welche für die verschlüsselte Kommunikation verwendet werden, nie im Klartext übermittelt werden. Wird jedoch ein

nicht-vorkonfiguriertes Gerät dem Netzwerk hinzugefügt, wird ein mit dem sogenannten Default Trust Center Link-Key verschlüsselter Network-Key gesendet, um eine verschlüsselte Kommunikation zu ermöglichen. Diese einmalige Übertragung kann von einem Angreifer mitgelesen werden, wodurch die Sicherheit des Netzwerkes in Gefahr ist. [6, S. 3]
Des Weiteren wurde festgestellt, dass es bei den getesteten Heimautomatisierungssystemen keine Möglichkeit gab den Schlüssel zurückzusetzen oder zu ändern. In elf Monaten Testzeit wurde außerdem keine Rotation des Schlüssels festgestellt. [6, S. 5]
Smart Lighting Lösungen wie beispielsweise Glühbirnen konnten übernommen werden, indem ein „reset to factory default“ Befehl geschickt wurde. Dies hat dazu geführt, dass die Glühbirne erneut nach verfügbaren Netzwerken sucht und sich ohne das Eingreifen einer Person mit diesem verbindet. [6, S. 5]

Fan et al. haben in ihrer Forschungsarbeit „Security Analysis of Zigbee“ (2017) mögliche Angriffe gegen mehrere ZigBee Geräte durchgeführt. Hier war es möglich den Network-Key zur Verschlüsselung der Verbindung, bei der Initialen Übertragung mitzulesen und mit Hilfe des öffentlich bekannten „Default Trust Center Link-Key“ (DTCLK) zu entschlüsseln. [7, S. 13]

Cao et al. haben in ihrem Paper „Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks“ einen Angriff namens Ghost vorgestellt. Dieser nutzt eine Schwachstelle des IEEE 802.15.4 MAC Layers des ZigBee Standards aus, welche zur Folge hat, dass einem ZigBee Gerät durch aufwändige Berechnungen Energie entzogen werden kann. Der Angriff baut auf der Tatsache auf, dass der Framecounter, welcher Replay-Angriffe verhindern soll, im Klartext mit den verschlüsselten Nachrichten gesendet wird. Indem ein Angreifer die Kommunikation in einem ZigBee Netzwerk mithört, kann dieser gefälschte Pakete an ZigBee Geräte mit einem inkrementierten Framecounter senden. Dadurch wird das Paket akzeptiert und berechnet, was zur Verschwendung von Energie der Batterie des Gerätes führt. Weiter hat dies zur Folge, dass legitime Pakete verworfen werden, da stets nur Pakete mit dem höchsten Framecounter akzeptiert werden. Dieser Angriff kann ohne Wissen über den Network-Key oder Netzwerkinformationen durchgeführt werden. Durch diesen Angriff kann ein Denial of Service (DoS) Angriff durchgeführt werden. Sollte der Angriff erfolgreich und die Energie des Gerätes aufgebraucht sein, muss dieses neu gestartet werden. Dies hat zur Folge, solange keine Gegenmaßnahmen implementiert sind, dass die Access Control List (ACL) leer ist und der Framecounter auf 0 gesetzt wird. Dadurch können früher aufgezeichnete Nachrichten erneut gesendet werden, was einen Replay-Angriff ermöglicht. [8]

Die Firma Praetorian Group, Inc. beschäftigt sich mit dem Thema der Verbreitung von ZigBee Geräten

und hat in einem Projekt die Internet of Things Map ins Leben gerufen. Auf dieser Karte werden IoT Geräte aufgezeichnet, die ZigBee zur Kommunikation verwenden. Um dies zu erreichen wurde ein tragbares Gerät entwickelt, welches nach ZigBee Netzwerken sucht und gefundene Netzwerke auf der Karte vermerkt. Das Projekt wurde 2015 durchgeführt, über den weiteren Verbleib des Projekts sind jedoch keine Informationen verfügbar. [9] Es ist anzumerken, dass im Gegensatz zu diesem Projekt, im Rahmen dieser Diplomarbeit explizit nach ZigBee 3.0 Netzwerken gesucht wird.

1.4. Forschungsfrage

Aus der Problemstellung und der Analyse des momentanen Forschungsstandes ergeben sich folgende Forschungsfragen:

- Welche Sicherheitsmechanismen bietet ZigBee 3.0 und wie sind diese implementiert?
- Wurden sicherheitstechnische Schwachstellen von früheren ZigBee Protokollversionen in ZigBee 3.0 behoben?
- Wie ist die Verbreitung von ZigBee 3.0 Geräten und welche Sicherheitsmechanismen werden tatsächliche eingesetzt?

1.5. Methodik

Nachfolgend wird die Methodik zur Lösung der Forschungsfragen beschrieben. Zu Beginn wird das ZigBee 3.0 Protokoll allgemein beleuchtet. Hierbei wird der ZigBee 3.0 Protokoll Stack und dessen einzelnen Schichten beschrieben, sowie deren Funktion erklärt. Nachfolgend wird ein Vergleich zu früheren ZigBee Protokoll Versionen gezogen, um herauszufinden, wie sich dieses zu Version 3.0 verändert hat. Letztlich wird das geplante Vorgehen bei der Erhebung der Verbreitungsdaten von ZigBee 3.0 Geräten erläutert.

1.5.1. Sicherheitsanalyse

Der erste Schritt zur Beantwortung der Forschungsfragen ist das Durchführen einer Sicherheitsanalyse des ZigBee 3.0 Protokolls. Hierbei soll herausgefunden werden, welche Sicherheitsmechanismen ZigBee 3.0 zur Verfügung stellt, um Angriffe auf Geräte abzuwehren oder zu vermeiden. Es werden vergangene, erfolgreiche Angriffe analysiert und mit den Sicherheitsmechanismen von ZigBee 3.0 verglichen um herauszufinden, ob diese Angriffe bei ZigBee 3.0 Geräten nach wie vor möglich sind.

1.5.2. ZigBee Netzwerkscanner

Da kaum Informationen zur Verbreitung von ZigBee 3.0 Geräten vorhanden sind, wird im Zuge dieser Diplomarbeit ein Proof of Concept Programm eines Warwalking-Tools entwickelt. Unter Warwalking versteht man das Auffinden und Lokalisieren von Funknetzwerken, indem vorhandene Funkkommunikation aufgezeichnet wird. Mittels des entwickelten Tools sollen Daten zur Tatsächlichen Verbreitung erhoben werden können.

Folgende Informationen über gefundenen ZigBee 3.0 Netzwerke sollen erhoben werden:

- Prozentanteil an ZigBee 3.0 Netzwerken im Vergleich zu früheren Zigbee Versionen
- Geografische Aufteilung von ZigBee 3.0 Netzwerken
- Aufteilung von ZigBee 3.0 Netzwerken in Bezug auf Wohn- und Industriegebiete
- Häufigkeit von ZigBee Geräten nach Hersteller
- Häufigkeit von ZigBee Geräten nach Gerätetyp
- Implementierte Sicherheitsmaßnahmen der Netzwerke und Geräte

Durch die Ermittlung der geographische Lage des Netzwerks soll vermieden werden, dass Geräte mehrmals erfasst werden und so die gesammelten Informationen über die Verbreitung von ZigBee 3.0 Geräten verfälscht werden. Die Ermittlung der verwendeten ZigBee Version hat den Hintergrund, dass zum einen die Verbreitung von ZigBee 3.0 Geräten festgestellt werden soll und zum anderen kann damit ein Vergleich gezogen werden, wie viele ZigBee 3.0 Geräte im Verhältnis zu älteren ZigBee Geräten betrieben werden. Neben dem Vorhandensein des ZigBee 3.0 Netzwerks an sich, sollen auch Informationen über die darin betriebenen Geräte beziehungsweise Gerätetypen gesammelt werden. Fokus liegt hierbei zunächst auf dem Hersteller des Gerätes. Wenn möglich, sollen aber auch spezifische Gerätetype identifiziert werden. Weiters soll auch ein Überblick über die implementierten Sicherheitsmaßnahmen geliefert werden, welche in ZigBee Netzwerken und Geräten genutzt werden.

Die für die Entwicklung des Tools verwendeten Testgeräte müssen von der ZigBee Alliance zertifizierte ZigBee 3.0 Geräte sein. Diese Zertifizierung bestätigt, dass das Gerät den ZigBee Standard verwendet und diesen korrekt, beziehungsweise vollständig implementiert hat.

1.5.3. Erhebung und Auswertung der Daten

Hauptfokus dieser Diplomarbeit ist die Entwicklung eines Tools zur Sammlung von Verbreitungs- und Sicherheitsdaten von ZigBee Geräten. Um die Funktionalität des Tools in realen Umgebungen zu testen, werden im Rahmen dieser Diplomarbeit in Wien Daten erhoben.

An folgenden Orten findet die Datensammlung statt:

- Baden bei Wien, Fußgängerzone Wassergasse / Neustiftgasse
- Vösendorf, Shopping City Süd
- Wien, Kärntnerstraße
- Wien, Mariahilferstraße
- Wien, Stadioncenter
- Wien, Wohngebiet abseits der Mariahilferstraße
- Wien, Innere Stadt

Bei den Gebieten Mariahilferstraße und Kärntnerstraße handelt es sich um Einkaufsstraßen. Daher ist in diesen Gebieten eine dichte Verteilung an Geschäften vorzufinden. Hier werden Verbreitungsdaten im Zusammenhang mit industriellen Gebieten erhoben. Die Wohngebiete abseits der Mariahilferstraße, sowie die Innere Stadt Wien, sollen Daten zur Verteilung von ZigBee Netzwerken in Wohngebieten liefern. Die Problematik dahinter ist, dass es keine Garantie dafür gibt in den ausgewählten Gebieten tatsächlich ZigBee Netzwerke vorzufinden. Voraussetzung für die erfolgreiche Erhebung von Daten ist das fertiggestellte Warwalking Tool.

2. ZigBee 3.0 - Überblick

ZigBee 3.0 ist ein von der ZigBee Alliance entwickelter Standard für die kabellose Kommunikation zwischen IoT Geräten. Dieser wurde mit dem Hintergrund entwickelt, einen kabellosen Zweiwegkommunikationsstandard, welcher auf niedrigen Kosten und Stromkonsum basiert, zur Verfügung zu stellen. Dieses Kapitel liefert einen Überblick über den ZigBee Standard, die Funktionsweise des ZigBee 3.0 Protokolls, sowie das Zusammenspiel der einzelnen Schichten des ZigBee 3.0 Stacks. Weiters wird ein Überblick geliefert, wie ZigBee Netzwerke aufgebaut sind und funktionieren und welche Gerätetypen es in einem solchen Netzwerk gibt.

2.1. Verwendete Standards

ZigBee Alliance hat mehrere Standards veröffentlicht, welche neben dem Aufbau und Zweck des ZigBee Protokolls auch das Standardverhalten von diversen ZigBee Geräten festlegen. Dazu gehören: [10]

- ZigBee PRO 2015 (Revision 21)
- Base Device Behavior (BDB)
  - BDB Commissioning
  - Automatic ZCL attribute reporting
  - BDB security options
- Green Power Basic Proxy
- ZigBee Cluster Library (ZCL) Revision 6
- ZigBee Application Architecture
- ZigBee Lighting and Occupancy Device Specification

Die für diese Diplomarbeit relevanten Standards sind der IEEE 802.15.4-2011 Standard [11] und die ZigBee Pro 2015 Spezifikation [3].

2.1.1. IEEE 802.15.4-2011

Die Basis des ZigBee Stacks bildet der IEEE 802.15.4-2011 Standard. Dieser Standard regelt die drahtlose Datenübertragung zwischen Geräten, welche auf geringen Stromverbrauch in Personal Wireless Area Networks (Low-Rated wpans) ausgelegt sind. Im ZigBee Stack ist dieser Standard für den Physical und MAC Layer zuständig.

2.1.2. ZigBee Pro 2015 Spezifikation

Das in ZigBee 3.0 Netzwerken verwendete Netzwerkprotokoll wird ist der ZigBee Pro 2015 Spezifikation beschrieben und ist für den Network Layer und den Application Layer des ZigBee Stacks zuständig. ZigBee Pro regelt die Netzwerkstruktur sowie Routing und stellt weitere Sicherheitsmechanismen zur Verfügung.

2.2. Rollen und Zuständigkeiten

In einem ZigBee Netzwerk wird zwischen drei Arten von Geräten unterschieden, welche spezifische Funktionen übernehmen:

- Endgerät
- Router
- Coordinator bzw. Trust Center

2.2.1. Endgeräte

Endgeräte in einem ZigBee Netzwerk sind alle Geräte, welche nicht das Trust Center oder dedizierte Router sind. [3, S. 11] Endgeräte können nur Nachrichten empfangen oder Nachrichten an das Trust Center, Parent Gerät oder andere Endgeräte schicken, dürfen empfangene Nachrichten jedoch nicht weiterleiten oder routen.

Ein Parent Gerät ist jenes Gerät, über welches ein Endgerät oder Router dem Netzwerk beigetreten ist. Ein Parent kann das Trust Center oder ein Router im Netzwerk sein. Ein Gerät kann immer nur ein Parent Gerät haben.

2.2.2. Router

Router können entweder dediziert nur für Routing im Netzwerk zuständig sein, oder zusätzlich Endgerät-Funktionalität besitzen. [3, S. 2] Ein Beispiel hierfür wäre eine Glühbirne, welche Nachrichten im Netzwerk weiterleiten kann. Bei vermaschten Netzen haben solche Geräte den Vorteil, dass das Netz ausfallsicherer und stabiler wird, da mehrere Geräte mit Routing-Funktionalität eine größere Anzahl an Knotenpunkten im vermaschten Netz bedeuten. Dadurch gibt es mehrere Möglichkeiten wie eine Nachricht sein Ziel erreichen kann, sollte ein Gerät im Netzwerk ausfallen.

2.2.3. Coordinator oder Trust Center

Der Coordinator oder das Trust Center ist ein Gerät im ZigBee Netzwerk, welches von allen Geräten im Netzwerk vertraut wird. Das Trust Center ist für die Verteilung von Schlüssel und die Initialisierung und Verwaltung von Geräten im Netzwerk zuständig. Weiters ist das Trust Center dafür zuständig, Sicherheits-Policies für das Netzwerk vorzugeben und aktuell zu halten. Es darf in einem zentralisierten Netzwerk nur ein Trust Center geben. [3, S. 380]

In einem verteilten Netzwerk werden Sicherheitsschlüssel von den einzelnen Routern verteilt, wodurch sie die Rolle des Trust Centers einnehmen. Es wird jedoch nur der Network-Key und keine Trust Center Link-Keys verteilt, da es kein einzigartiges Trust Center im Netzwerk gibt. [3, S. 380]

Geräten ist es möglich vorkonfigurierte Trust Center Adressen und Link-Keys zu besitzen um einem Netzwerk beizutreten. Es ist weiters möglich für Geräte den bekannten Centralized Global Trust Center Link-Key für die erste Verbindung zu verwenden, was es potentiell ermöglicht, diese erste Verbindung zu entschlüsseln und den Network-Key des ZigBee Netzwerks zu stehlen. [3, S. 380]

Details zu den verwendeten Sicherheitsschlüssel und deren Anwendungsgebiete werden in Kapitel 3 genauer beleuchtet.

2.3. Netzwerktopologien

Wie in Abbildung 2.1 auf Seite 10 zu sehen ist, kann ein ZigBee Netzwerk in der Sterntopologie, Baumtopologie oder als vermaschtes Netz (Mesh Network) betrieben werden.

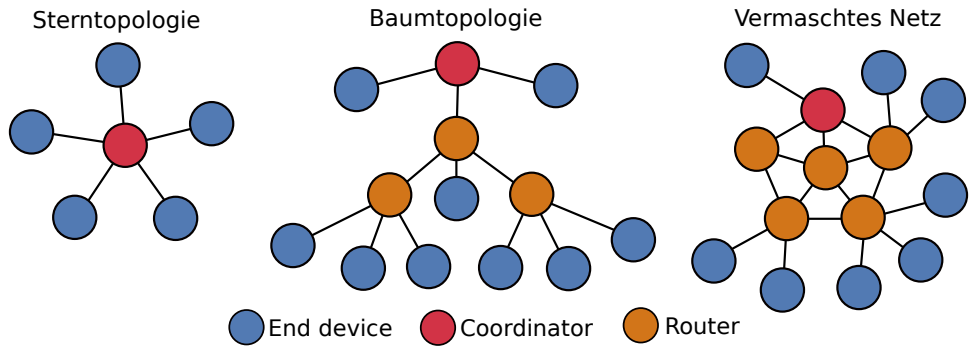

Abbildung 2.1.: ZigBee Netzwerktopologien

In der Sterntopologie wird das Netzwerk von einem einzigen Gerät, dem ZigBee Coordinator kontrolliert. Der ZigBee Coordinator ist dafür zuständig, Geräte im Netzwerk zu initiieren und diese aktuell zu halten. Alle anderen Endgeräte kommunizieren direkt mit dem ZigBee Coordinator beziehungsweise Trust Center.

In der Baumtopologie und bei vermaschten Netzen, ist der ZigBee Coordinator für die Initiierung des Netzes und die Auswahl von bestimmten Schlüssel-Netzwerkparametern zuständig. Das Netzwerk kann jedoch durch ZigBee Router erweitert werden. In einer Baumtopologie leiten die Router Nachrichten in einer hierarchischen Routing-Strategie weiter. In vermaschten Netzen ist Peer-to-Peer Kommunikation möglich. [3, S. 2] ZigBee ist auf die Verwendung von vermaschten Netzen ausgelegt. Dadurch sind dies in der Regel jene Netzwerktopologie, welche am ehesten anzutreffen ist.

Weiters wird in einem ZigBee Netzwerk zwischen verteilten und zentralisierten Netzwerken unterschieden. Diese Netze unterscheiden sich dahingehend, dass es in einem zentralisierten Netzwerk nur ein einzigartiges Trust Center geben darf. In einem verteilten Netzwerk gibt es kein einzigartiges Trust Center und die einzelnen Router können die Rolle des Trust Center einnehmen.

2.4. ZigBee Stack

In Abbildung 2.2 auf Seit 11 ist zu sehen, dass der ZigBee Stack in die vier Schichten „Application Layer“, „Network Layer“, „IEEE 802.15.4 MAC Layer“ und „IEEE 802.15.4 PHY Layer“ aufgeteilt ist. Der ZigBee 3.0 Stack wurde mit dem Hintergrund entwickelt, dass Geräte, welche eine ältere ZigBee Protokollversion implementiert haben, ZigBee 3.0 Netzwerken beitreten können. Weiters ist es auch für ZigBee 3.0 Geräte möglich Netzwerken beizutreten, in denen ältere Protokollversionen verwendet werden. Das bedeutet, dass das Protokoll rückwärtskompatibel entwickelt wurde. Nachfolgend werden

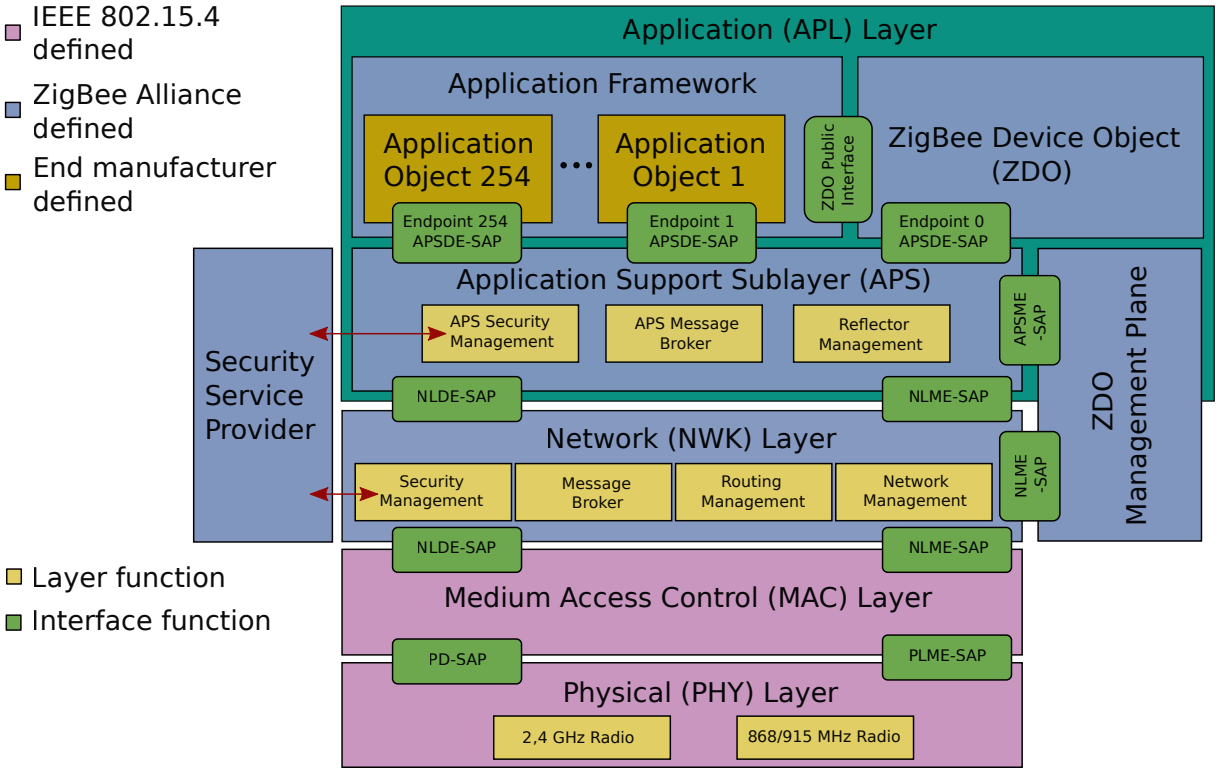

Abbildung 2.2.: Überblick der ZigBee Stack Architektur [3, S. 2]

die einzelnen Schichten des ZigBee 3.0 Stacks überblicksmäßig beschrieben. Technische Details der einzelnen Schichten sind in den Anhängen A - Physical (PHY) Layer, B - Medium Access Control (MAC) Layer, C - Network Layer und D - Application Layer ersichtlich.

2.4.1. Physical (PHY) Layer

Dies ist die unterste Schicht des ZigBee Stacks, welche für die physischen Übermittlungsmedien zuständig ist und den Austauscht von Datenbits regelt. [12, S. 34]
Der PHY Layer ist zuständig für:

- die verfügbaren Frequenzbänder
- die Modulation des Funksignales
- den Aufbau des Datenpaketes (Physical Protocol Data Unit - PPDU), welches vom PHY Layer generiert wird

Sicherheitstechnisch sind auf diesem Layer keine Maßnahmen vorhanden, da dieser lediglich ein standardisiertes Vorgehen beim Aufbau einer Funkverbindung festlegt.

2.4.2. Medium Access Control (MAC) Layer

Diese Schicht ist für die Adressierung zuständig. Es bestimmt wo ausgehende Pakete hingesendet werden und bei eingehenden Paketen bestimmt sie, wo diese Pakete hergekommen sind. [12, S. 34]

MAC Sicherheitsmaßnahmen

Der MAC Layer stellt diverse Sicherheitsservices zur Verfügung, welche von höheren Schichten im Stack verwendet werden können. Zu den Services gehören Datenintegrität, Datenvertraulichkeit und Schutz vor Replay-Angriffen.

Informationen zu den Sicherheitsservices befinden sich im sogenannten Auxiliary Security Header des MAC Layers. [11, S. 139-142] Da per Design, Sicherheitsmaßnahmen in ZigBee Netzwerken im Network und Application Layer implementiert sind, wird der Auxiliary Header im Frame nicht mitgesendet. Der Grund für das eliminieren der optionalen MAC Sicherheitsfeatures ist, dass eine volle Implementierung des MAC Layers zu hohe Speicherkosten auf den Geräten verursachen würde. [3, S. 486]

2.4.3. Network Layer (NWK)

Diese Schicht stellt die ZigBee PRO Funktionalität zur Verfügung und bietet Interfaces zu den IEEE 802.15.4 Schichten. Diese Schicht ist für die Netzwerkstruktur und Routing zuständig. [12, S. 34]

Wie in Abbildung 2.2 auf Seite 11 zu sehen ist, bietet die Network Layer Data Entity (NLDE) Datentransfer Services via dem dazugehörigen Service Access Point (SAP), dem NLDE-SAP an. Die Network Layer Management Entitiy (NLME) bietet Management Services via dem NLME-SAP an. Die NLME verwendet die NLDE um einige der Managementaufgaben zu erledigen. Weiters wird dort eine Datenbank von Managed Objects verwaltet, die Network Information Base (NIB). [3, S. 242]

Security Suites

Bei ZigBee Netzwerken gilt das Prinzip, dass jene Schicht, welche ein Datenpaket erzeugt, auch für dessen Schutz zuständig ist. Das Sicherheitsniveau wird hierbei via sogannte Security Suits (auch Security-Level genannt) bestimmt. Bei der in ZigBee Netzwerken verwendeten Security Suits handelt es sich um eine Abwandlung des AES-CCM, den CCM*. Im Gegensatz zum AES-CCM, erlaubt der CCM* die Verwendung von Authentication-Tags variabler Länge anstatt der fixen Längen beim AES-CCM. Die Spezifika des CCM* Security Suites werden in Kapitel 3.11 beschrieben. [3, S. 456]

Network Layer Data Entity (NLDE)

Die NLDE stellt einen Datenservice zur Verfügung, welche es Applikationen erlauben sogenannte Application Protocol Data Units (APDU) zwischen Geräten zu transportieren. APDUs können nur zwischen Geräten im selben Netzwerk transportiert werden.

Die NLDE stellt folgende Services zur Verfügung: [3, S. 219]

- **Erstellung von Network level PDU (NPDU):** Die NLDE muss in der Lage sein, ein NPDU von einem Application Support Sub-Layer PDU zu erzeugen, indem ein passender Protokoll-Header hinzugefügt wird.
- **Topologie-spezifisches Routing:** Die NLDE muss in der Lage sein, ein NPDU zu einem passendem Gerät zu senden, welches entweder die finale Destination oder der nächste Hop zur finalen Destination in der Kommunikationskette ist.
- **Sicherheit:** Die NLDE muss die Authentizität und Vertraulichkeit einer Nachricht gewährleisten können.

Network Layer Management Entity (NLME)

Die NLME stellt folgende Managementservices zur Verfügung, die es einer Applikation erlauben mit dem Stack zu interagieren.

Die NLME stellt folgende Services zur Verfügung: [3, S. 219-220]

- **Neue Geräte konfigurieren:** Dies beschreibt die Fähigkeit, den Stack so zu konfigurieren, dass für den Betrieb notwendige Operationen durchgeführt werden können. Konfigurationsoptionen beinhalten zum Beispiel als ZigBee Coordinator ein Netzwerk zu beginnen oder einem existierenden Netzwerk beizutreten.
- **Netzwerk starten:** Die Fähigkeit ein neues Netzwerk zu starten.
- **Einem Netzwerk (wieder) beitreten oder verlassen:** Neben der Fähigkeit einem Netzwerk beizutreten, wieder beizutreten oder ein Netzwerk zu verlassen, beschreibt dies ebenfalls die Fähigkeiten eines ZigBee Coordinators oder eines ZigBee Routers, das Verlassen des Netzwerkes von anderen Geräten veranlassen können.

- **Adressierung:** Dies beschreibt die Fähigkeit Geräten, welche dem Netzwerk beitreten, Adressen zu verleihen.
- **Neighbor discovery:** Dies ist die Fähigkeit direkte Nachbarn zu entdecken, aufzuzeichnen und Informationen über diese zu sammeln.
- **Route discovery:** Dies ist die Fähigkeit, Routen durch das Netzwerk aufzuzeichnen und zu entdecken um Nachrichten effizient weiterleiten zu können.
- **Reception control:** Dies ist die Fähigkeit zu kontrollieren, wann ein Empfänger aktiviert wird und für wie lange.
- **Routing:** Dies ist die Fähigkeit unterschiedliche Routing Mechanismen zu verwenden, wie Unicast, Broadcast, Multicast oder viele zu einem Routing, um effizient Daten austauschen zu können.

2.4.4. Application Layer (APL)

Diese Schicht enthält die Applikationen, welche auf dem Gerät zur Verfügung gestellt werden. Das bedeutet, sie gibt dem Gerät seine Funktionalität. Es können mehrere Applikationen auf einem Gerät betrieben werden. Ein Umgebungssensor kann zum Beispiel unterschiedliche Applikationen für das Messen der Temperatur, Luftfeuchtigkeit und Luftdruck haben. [12, S. 34]

In diesem Kapitel wird die Funktion des APS Sub-Layer, der ZDOs und der herstellerdefinierten Applikationsobjekten beschrieben, welche Teil des Application Layers sind.

Application Support (APS) Sub-Layer

Das APS Sub-Layer stellt ein Interface zwischen dem Network Layer (NWK) und dem Application Layer (APL) zur Verfügung. Hierbei bietet das APS Sub-Layer ein generelles Set an Services an, welche sowohl von ZigBee Device Objects (ZDO) als auch von Manufacturer-Defined Application Objects verwendet werden können. Die Services werden durch zwei Entities zur Verfügung gestellt, die APS Data Entity (APSDE) durch den APSDE Service Access Point (APSDE-SAP) und die APS Management Entity (APSME) durch den APSME Service Access Point (APSME-SAP) [13, S. 17]

Die APSDE stellt Services zur Datenübertragung zwischen zwei oder mehreren Application Entities im selben Netzwerk zu Verfügung.

Die APSME stellt eine Anzahl an Services für Application Objects zur Verfügung, wie Sicherheitsservices und das Binden von Geräten. Außerdem wird hier eine Datenbank von Managed Objects verwaltet, die APS Information Base (AIB).

Application Framework

Das Application Framework ist die Umgebung in ZigBee Geräten, in welchen Applikationen gehostet werden. Es können bis zu 254 unterschiedliche Application Objects definiert werden, wobei jedes dieser Objects mit einer Endpoint Adresse von 1 bis 254 identifizierbar ist. Adresse 0 und 255 sind reserviert für die APSDE-SAP Verwendung. Adresse 0 Stellt ein Interface zu ZDO dar und Adresse 255 ist für den Broadcast zu allen Application Objects reserviert. Die Endpunkte 241-254 sind von der ZigBee Alliance zugeordnet und dürfen nicht ohne Zustimmung verwendet werden. [13, S. 18]

Application Profiles: Um die Funktionalität von Applikationen zu gewährleisten, welche sich auf unterschiedlichen Geräten befinden, werden sogenannte Application Profiles eingesetzt. Diese Application Profiles sind Vereinbarungen über Nachrichten, Nachrichtenformate und Verarbeitungsaktionen, wodurch Applikationen Kommandos senden, Daten anfordern und dergleichen verarbeiten können.

Cluster: Einzelne Applikationen können in sogenannte Cluster zusammengefasst werden. Cluster werden durch „Cluster Identifier“ identifiziert und sind einzigartig innerhalb des Scopes eines Application Profiles.

ZigBee Device Objects

Die ZigBee Device Objects (ZDO), stellen eine Basisklasse an Funktionen und ein Interface zwischen den Application Objects, Device Profiles und dem APS zur Verfügung. Die ZDO befindet sich zwischen dem Application Framework und dem APS. Es ist dafür zuständig, allgemeine Anforderungen von Applikationen zu befriedigen und ist für folgendes zuständig: [13, S. 18-19]

- Initiierung des APS, Network Layer und Security Service Provider
- Zusammensetzung der Konfigurationsinformationen der Endapplikationen um Discovery, Security Management, Network Management und Binding Management festzulegen und zu implementieren.

Device Discovery: Device Discovery erlaubt es Geräten, andere Geräte zu entdecken. Es gibt zwei Arten von Discovery Requests, IEEE Address Request und Network Address Request. Der IEEE Address Re-

quest ist Unicast und setzt voraus, dass die Netzwerk Adresse bekannt ist. Der Network Address Request ist Broadcast, wobei die Nachricht die bekannte IEEE Adresse als Payload beinhaltet.

Service Discovery: Service Discovery erlaubt es Geräten, die Fähigkeiten von anderen Geräten im Netzwerk zu entdecken. Service Discovery kann durchgeführt werden, indem an jeden Endpoint eines Gerätes ein Request gesendet wird oder indem das sogenannte Match Service Feature verwendet wird.

3. ZigBee 3.0 - Sicherheit

Die von ZigBee angebotenen Sicherheitsservices beinhalten Methoden zum Austausch und Generierung der unterschiedlichen Sicherheitsschlüssel, zum Schutz des Netzwerkframes und für das Management von Geräten. [3, S. 375] In diesem Kapitel werden die Sicherheitsmechanismen beschrieben, welche in ZigBee Netzwerken und Geräten eingesetzt werden.

3.1. Sicherheitsannahmen

ZigBee verwendet ein Open Trust Modell welches darauf beruht, dass sich alle Schichten und Applikationen auf einem Gerät vertrauen. Jeder Hersteller von ZigBee Geräten ist dafür verantwortlich die notwendigen Sicherheitsservices korrekt und sicher zu implementiert. Das Sicherheitsniveau der ZigBee Sicherheitsarchitektur beruht auf:

- der Geheimhaltung des symmetrischen Schlüssels
- den implementieren Schutzmechanismen
- der korrekten Implementierung der kryptographischen Mechanismen und zugehörigen Sicherheits-Policies
- der ordnungsgemäßen Funktion von Zufallszahlengeneratoren

Beim initialen Schlüsselaustausch des Network-Keys, kann ein allgemein bekannter Schlüssel zur Verschlüsselung der Übertragung verwendet werden. Dies führt dazu, dass für den Moment des Schlüsselaustausches der Schlüssel von jedem Gerät erfasst werden kann. Alternativ kann für den initialen Schlüsselaustausch ein vorab geteilter Schlüssel verwendet werden, welcher außerhalb des ZigBee Netzwerkes geteilt wird. Als Beispiel kann hierfür ein Sticker mit einem QR-Code auf dem Gerät angebracht sein, welcher beim initialen Setup eingescannt werden muss.

Die zur Verfügung stehenden Sicherheitsservices bieten kryptographische Sicherheit nur zwischen den Interfaces verschiedener Geräte, also auf einer Geräte-zu-Geräte Basis. Die Trennung von Interfaces

zwischen den einzelnen Schichten des ZigBee Stacks erfolgt nicht kryptographisch und beruht auf dem korrekten Design der Security Service Access Points (SAP). [3, S. 375-376]

3.2. Sicherheitsdesign

Durch das Open Trust Modell, welches im Punkt 3.1 beschrieben wurde, ist die Wiederverwendung von Schlüsselmaterial zwischen den einzelnen Schichten eines Gerätes möglich. Dies führt weiters dazu, dass Ende-zu-Ende Sicherheit auf einer Gerät-zu-Gerät Basis statt zwischen einzelnen Schichten realisiert ist. [3, S. 376-377]
Dies führt zu folgenden Prinzipien der Sicherheitsarchitektur:

- Jene Schicht, welche einen Frame generiert und versendet, ist für den Schutz des Frames zuständig.
- Wenn Schutz vor beispielsweise bösartigen Netzwerkgeräten benötigt wird, muss Network Layer Sicherheit bei allen Frames verwendet werden. Dies führt dazu, dass nur jene Geräte, welche dem Netzwerk erfolgreich beigetreten sind und einen aktiven Network-Key besitzen, Frames mehr als einen Hop im Netzwerk senden können.
- Schlüssel können zwischen dem Network Layer und Application Layer wiederverwendet werden. Der aktive Network-Key soll beispielsweise für den Schutz von Application Layer Broadcast Frames oder Network Layer Frames verwendet werden. Die Wiederverwendung von Schlüssel hilft bei der Verringerung des erforderlichen Speicherplatzes.
- Ende-zu-Ende Sicherheit muss so implementiert sein, dass nur der Sender und Empfänger Zugriff auf die Nachricht erhalten, welche durch einen Shared-Key, beispielsweise Application Link-Key, geschützt sind.
- Um die Interoperabilität von Geräten zu vereinfachen, soll das Basis-Sicherheitsniveau von allen Geräten in einem Netzwerk dasselbe sein. Wenn mehr Sicherheit für einen Frame benötigt wird, als vom Netzwerk zur Verfügung gestellt wird, kann Sicherheit auf Basis des Application Layers zwischen Geräten hergestellt werden.

Es gibt mehrere Policies welche von ZigBee Geräten korrekt implementiert werden müssen. Zu diesen Policies gehören:

- Das Vorgehen bei Fehlern, welche beim Ver- und Entschlüsseln von Nachrichten auftreten. Beispielsweise das Erkennen von korrupten Nachrichten.

- Das Behandeln von Fehlern bei der Synchronisation von Frame Counter und Frame Counter Überläufe. Wenn beispielsweise der Frame Counter des Link- oder Network-Keys eines Gerätes überläuft, kann dieses keine Nachrichten mehr senden. Geräte müssen dies erkennen und behandeln können. Wie die gewährleistet werden kann, wird im Punkt 3.10 - Frame Counter Anforderungen auf Seite 26 genauer beleuchtet.
- Das Erkennen und Behandeln des Verlusts der Schlüsselsynchronisation. Endgeräte können in ZigBee Netzwerk schlafen. Wenn beispielsweise nun ein neuer Network-Key ausgestellt wird, bekommt dies das Endgerät eventuell nicht mit und besitzt noch immer den alten Network-Key. ZigBee Geräte müssen diesen Umstand erkennen und behandeln können. In diesem Fall durch einen sogenannten Trust Center Rejoin in das Netzwerk. Die Spezifika des Trust Center Rejoin werden im Punkt 3.7 - Key Switch auf Seite genauer beschrieben.
- Das periodische Aktualisieren der Schlüssel. Geräte müssen einen Mechanismus implementiert haben, welcher es erlaubt, Schlüssel zu aktualisieren und alte Schlüssel zu verwerfen.

3.3. Sicherheitsarchitektur

Sicherheitsmechanismen sind in zwei Schichten des Protokoll-Stacks eingebaut, dem Network (NWK) und dem Application Support (APS) Sublayer, welche für den sicheren Transport der von der jeweiligen Schicht generierten Frames verantwortlich sind. Der APS Sublayer stellt Services zum Aufbau und Erhalt von Sicherheitsbeziehungen bereit. Das ZigBee Device Object (ZDO) verwaltet die Sicherheits-Policies und ist für die sichere Konfiguration des Gerätes zuständig.

3.4. Sicherheitsschlüssel

Die Sicherheit in einem ZigBee Netzwerk basiert auf Link-Keys und dem Network-Key. Unicast Kommunikation zwischen Application Layer Entities wird mit einem 128-Bit Link-Key geschützt, welcher von beiden Geräten geteilt wird. Broadcast Kommunikation und alle anderen Network Layer Kommunikation werden mit einem 128-Bit Network-Key geschützt, welcher von allen Geräten im Netzwerk geteilt wird.

Es gibt pro ZigBee Netzwerk einen Network-Key, welcher im Distributed oder Centralized Security Mode verwendet werden kann. Der gewählte Security Mode gibt an, wie der Schlüssel im Netzwerk verteilt wird. Im Distributed Security Mode gibt es kein einzigartiges Trust Center im Netzwerk. Schlüssel

werden von den Routern im Netzwerk an beitretende Geräte via dem Transport Key Kommando weitergegeben. Im Centralized Security Mode verwaltet das Trust Center den Network-Key und eine Liste mit Link-Keys für alle Geräte im Netzwerk. Weiters ist das Trust Center für die Generierung und Verteilung der Sicherheitsschlüssel zuständig. [3, S. 428]

Es gibt unterschiedliche Arten von Link-Keys:

- Application Link-Key
- Unique Trust Center Link-Key
- Global Trust Center Link-Key
- Distributed Global Link-Key

Application Link-Keys werden zwischen zwei Geräten im Netzwerk geteilt und sind für die Sicherheit von Application Layer Kommunikation zuständig.

Ein Link-Key zwischen zwei Geräten, bei denen eines der Beiden das Trust Center ist, werden Trust Center Link-Keys genannt. Es gibt zwei Arten von Trust Center Link Keys, Unique und Global.

Ein Unique Trust Center Link Key wird zwischen dem Trust Center und einem Geräte im Netzwerk geteilt und ist für die Sicherheit von Unicast Kommunikation auf Application Layer Ebene zuständig. Dieser Schlüssel wird nur in zentralisierten Netzwerken eingesetzt, da es in einem verteilten Netzwerk kein einzigartiges Trust Center gibt.

Der Global Trust Center Link Key wird dazu verwendet, den Beitritt von Geräten in ein zentralisiertes Netzwerk mit einem einzigartigen Trust Center abzusichern. Der Standardwert des Global Trust Center Link-Keys ist 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39 (ZigBeeAlliance09).

Der Distributed Global Link-Key wird in verteilten Netzwerken, ohne einzigartiges Trust Center, zum Beitritt von Geräten eingesetzt. Dieser Schlüssel besitzt keinen Standardwert und muss auf den Geräten (Router und Endgeräte) bereits bei der Herstellung eingespielt werden.[7, S.]

Eine Zusammenfassung der verschiedenen Arten von Link-Keys ist in Tabelle 3.1 auf Seite 21 ersichtlich. [3, S. 377-378]

Schlüssel Name	Beschreibung
Global Trust Center Link-Key	Dieser Schlüssel wird verwendet um zentralisierten Netzwerken beizutreten
Distributed Global Link-Key	Dieser Schlüssel wird verwendet um verteilten Netzwerken beizutreten
Application Link-Key	Dieser Schlüssel wird zwischen zwei Geräten geteilt und zur Application Layer Verschlüsselung verwendet
Install Code Link-Key	Dieser Schlüssel wird von einem Installations-Code abgeleitet und im weiteren Verlauf ein Unique Trust Center Link-Key zum Beitritt in das Netzwerk erstellt.
Unique Trust Center Link-Key	Dieser Schlüssel wird zwischen dem Trust Center und einem Gerät im Netzwerk geteilt und wird für Trust Center Commands und Application Layer Verschlüsselung verwendet.

Tabelle 3.1.: Verwendete Link-Keys in ZigBee Netzwerken

3.5. Schlüsselableitungen

Um die Wiederverwendung von Sicherheitsschlüsseln zwischen unterschiedlichen Sicherheitsservices zu vermeiden, werden diese via einer Einweg-Funktion vom Link-Key abgeleitet. Ein auf diese Weise abgeleitete Schlüssel kann ein Key-Transport Key, ein Key-Load Key oder ein Data Key sein.

- Der Key-Load Key wird verwendet um die Übertragung von Link-Keys zu schützen.
- Der Key-Transport Key wird für den Schutz bei der Übertragung von Network-Keys verwendet.
- Der Data Key ist gleich dem Link-Key. Data Keys werden zum Schutz von Network und Application Layer Nachrichten verwendet.

Alle Schlüssel, welche vom Link-Key abgeleitet werden, teilen den gleichen Frame Counter wie der ursprüngliche Link-Key. Alle Schichten des ZigBee Stacks teilen sich den aktiven Network-Key und den zugehörigen ausgehenden und eingehenden Frame Counter. [3, S. 427]

3.6. Schlüsselübertragung

In ZigBee Netzwerken gibt es mehrere Arten wie ein Gerät Sicherheitsschlüssel erhalten kann und wie die Übertragung abgesichert wird. Sicherheitsschlüssel, welche nicht bereits vorinstalliert wurden, wer-

den in einem zentralisierten Netzwerk stets vom Trust Center erzeugt und verteilt.

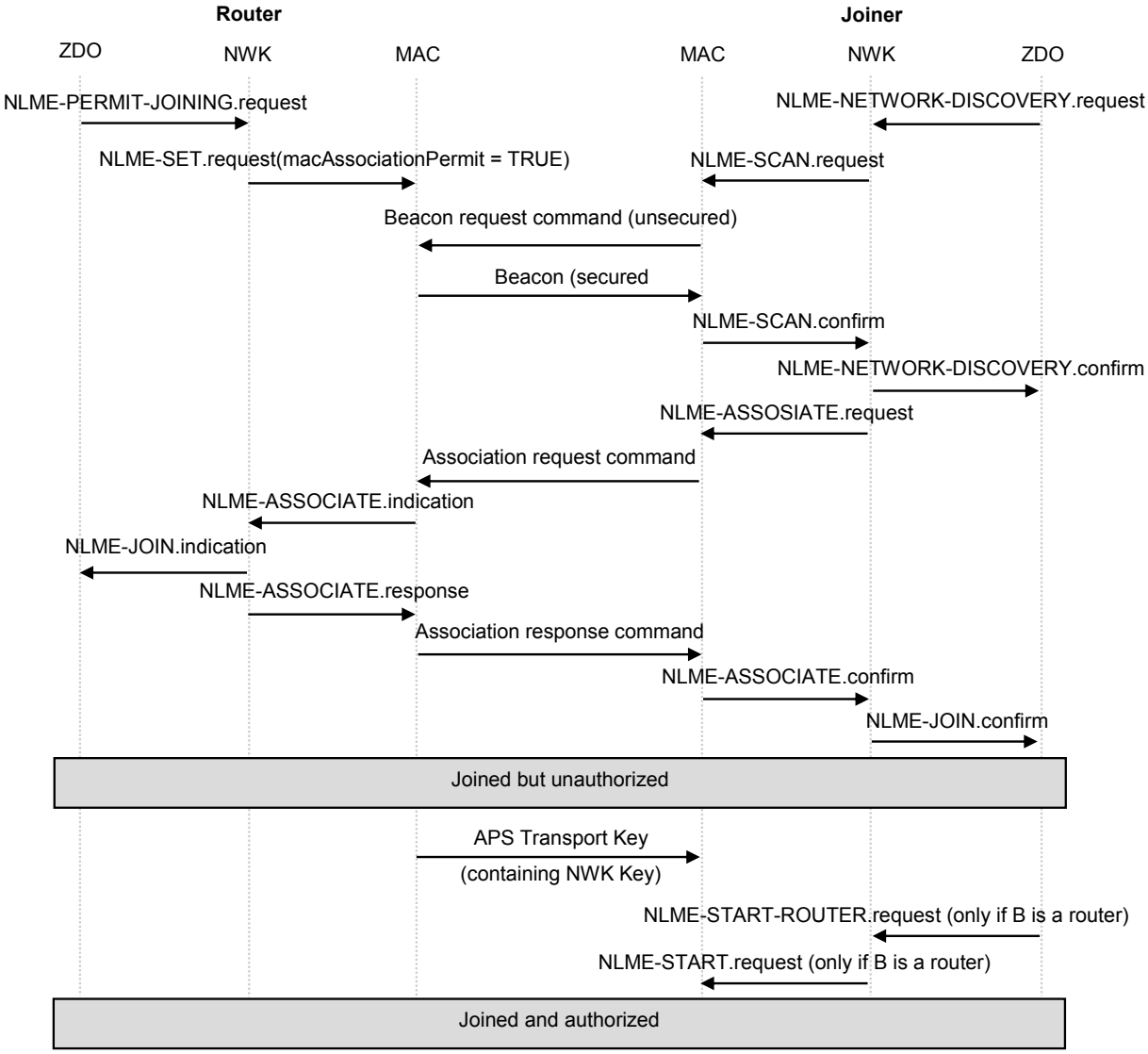

Abbildung 3.1.: Network Join Ablauf [3, S. 429]

In Abbildung 3.1 ist der Ablauf des Beitritts eines Gerätes in ein ZigBee Netzwerk abgebildet. Zunächst wird eine sogenannte „MAC Association“ durchgeführt. Hierbei sendet das beitretende Gerät (Joiner) sogenannte „Capability Information“ an das Gerät, über welches das Netzwerk beigetreten werden soll. Capability Information sind beispielsweise Gerätetyp (Router oder Endgerät), Energiequelle (Strom direkt von der Stromleitung, Batteriebetrieben) aber auch Informationen ob Nachrichten erhalten werden können, wenn das Gerät „Idle“ ist. Ist die MAC Association abgeschlossen, wird der Network Key übertragen. Die Geräte erhalten den Network-Key immer via dem Transport Key Kommando. Die Übertragung des Network Keys kann auf mehrere Arten verschlüsselt werden. Beim Erstbeitritt in ein

Netzwerk ist eine Möglichkeit die Verwendung des Global Trust Center Link-Keys, welcher einen bekannten Standardwert besitzt. Eine weitere Möglichkeit ist die Verwendung eines vorinstallierten oder von einem Install Code abgeleiteten Unique Trust Center Link Keys.
War das Gerät bereits im Netzwerk und der Network-Key wird aktualisiert, wird der alte Network-Key oder der Key-Transport Key zur Verschlüsselung der Übertragung verwendet. Der gewählte Schlüssel hängt davon ab, ob die Aktualisierung als Broadcast oder Unicast gesendet wird. [3, S. 450] Spezifika hierzu werden in Kapitel 3.7 - Key Switch beschrieben.

Link-Keys werden beim Erstbeitritt eines Gerätes entweder via dem Transport Key Kommando gesendet oder sind bereits im Vorhinein auf dem Gerät enthalten. Die Übertragung des Link-Keys wird mit dem Network-Key verschlüsselt, welcher im Vorhinein an das dem Netzwerk beitretende Gerät gesendet werden muss.
Sollte der Link-Key aktualisiert werden, wird der neue Link-Key mittels dem einem Key-Load Key verschlüsselt an das Gerät übertragen, welcher vom alten Link-Key abgeleitet wird.

Das Transport Key Kommando beschreibt wie ein Schlüssel zu einem Gerät transportiert werden soll. Beim Transport Key Kommando wird der Schlüssel von einer sogenannten Key Source an ein Gerät gesendet. In einem zentralisierten Netzwerk ist eine solche Key Source das Trust Center und in einem verteilten Netzwerk die einzelnen Router. [3, S. 379] Die Sicherheit der Kommunikation hängt von der sicheren Implementierung des Transport Key Kommandos ab.

Eine Zusammenfassung der Übertragungsarten von Sicherheitsschlüssel in zentralisierten Netzwerken ist in Tabelle 3.2 auf Seite 24 ersichtlich.

3.7. Key Switch

Bei ZigBee 3.0 Netzwerken können Network-Keys via Broadcast oder Unicast aktualisiert werden. Das Aktualisieren des Network-Keys ist hierbei eines der Hauptaufgaben des Trust Centers. Schlüsselupdates via Broadcast zu senden ist der einfachere der beiden Wege einen neuen Network-Key im Netzwerk zu verbreiten. Der neue Schlüssel wird hierbei mit dem alten Network-Key verschlüsselt und an alle Geräte im Netzwerk geschickt. Hierbei gibt es keine Möglickeit Geräte, welche den neuen Network-Key bereits besitzen, bei dieser Art von Aktualisierung auszunehmen.

Es besteht auch die Möglichkeit den neuen Network-Key via Unicast an einzelne Geräte zu verbrei-

Schlüssel	Übertragungs-grund	Verwendeter Schlüssel zur Verschlüsselung
Network Layer Sicherheit		
Network-Key	Netzwerk-beitritt	Transport-Key Service mit: • Global Trust Center Key oder • Unique Trust Center Link Key (abgeleitet von Install Code) • Unique Trust Center Link Key (vorinstalliert)
	Aktualisierung	• Broadcast: Transport-Key Service mit alten Network-Key • Unicast: Transport-Key Service mit Key-Transport Key
Application Layer Sicherheit		
Application Link-Key	Netzwerk-beitritt	• Transport-Key Service mit Network-Key • Keine Übertragung (Schlüssel vorinstalliert)
	Aktualisierung	• Transport-Key Service mit Key-Load Key
Unique Trust Center Link-Key	Netzwerk-beitritt	• Transport-Key Service mit Network-Key • Keine Übertragung (Schlüssel vorinstalliert) • Keine Übertragung (Schlüssel von Install Code abgeleitet)
	Aktualisierung	• Transport-Key Service mit Key-Load Key

Tabelle 3.2.: Zusammenfassung der Schlüsselübertragungsarten in zentralisierten Netzwerken

ten. Hierbei wird der Link-Key zur Verschlüsselung der Update Nachricht verwendet. Dies setzt jedoch voraus, dass alle Geräte im Netzwerk einen autorisierten Link-Key besitzen. Unicast stellt eine sicherere Methode dar neue Network-Key im Netzwerk zu verbreiten, da nur die Empfänger der Update Nachricht, diese entschlüsseln können. Um den Datenverkehr innerhalb des Netzwerkes zu verringern, werden Update Nachrichten nur an die Router im Netzwerk geschickt, welche den neuen Schlüssel im weiteren Verlauf an deren Endgeräte schicken.

Unabhängig davon, ob die neuen Schlüssel via Broadcast oder Unicast verteilt werden, wird das „APS Key Switch Command“ immer via Broadcast verteilt. Dieses Kommando sagt aus, dass ab diesem Zeitpunkt der neue Network-Key zu verwenden ist. Sollten Geräte diese Nachricht nicht erhalten, wechseln diese implizit zum neuen Network-Key, wenn sie mitbekommen, dass dieser zur Kommunikation ver-

wendet wird. Sollten Nachrichten mit einem alten Network-Key empfangen werden, können diese zwar noch entschlüsselt werden, die Verschlüsselung von ausgehenden Nachrichten muss jedoch mit dem neuen Network-Key erfolgen.

Um einen alten Network-Key aus dem Netzwerk zu entfernen, wird der neue Network-Key, sowie das „APS Key Switch Command“ zwei Mal gesendet. Ab diesem Zeitpunkt darf nur noch der neue Schlüssel zur Kommunikation verwendet werden.

In einem ZigBee Netzwerk ist es üblich, dass Endgeräte periodisch schlafen um Strom zu sparen. Dadurch kann es vorkommen, dass Geräte den Wechsel des Network-Keys nicht mitbekommen. In diesem Fall muss sich das Endgerät um die Problematik kümmern und dem Netzwerk via seinem Parent neu beitreten. Der Rejoin wird hierbei via dem sogenannten “Secure Rejoin„ durchgeführt. Ein Parent kann ein Router oder das Trust Center sein. Sollte auch das Parent-Gerät bereits zum neuen Schlüssel gewechselt haben, muss das Gerät einen “Trust Center Rejoin„ durchführen. [3, S.450-451]

- Secure Rejoin wird durchgeführt, wenn ein Gerät einem ZigBee Netzwerk neu beitreten muss. Hierbei wird ein sogenanntes NWK Rejoin Request Kommando an das Parent Gerät geschickt, welches mit dem alten Network-Key geschützt übertragen wird. [3, S. 433]
- Trust Center Rejoin (auch „Insecure Rejoin“ genannt) ist ein NWK Rejoin Kommando, bei dem das das Kommando ohne Network Layer Sicherheit gesendet wird und es einem Gerät erlaubt, den neuen Network-Key anzufordern. Dies ist erforderlich, wenn das Gerät den aktuell aktiven Network-Key nicht besitzt. Wenn das Netzwerk einen neuen Network-Key verwendet, wird der alte Netzwerkschlüssel abgelehnt. Daher muss das Trust Center Rejoin Kommando ohne Network Layer Sicherheit gesendet werden. [3, S. 434]

Das Aktualisieren von Network-Keys geschieht nur in zentralisierten Netzwerken. Wird ein verteiltes Netzwerk betrieben, sind keine Network-Key Aktualisierungen vorgesehen. [3, S. 451]

3.8. Network-Key Lebensdauer

Das Trust Center sollte regelmäßig neue Network-Keys verteilen. Dies hat folgende Gründe:

- Ein Update des Network-Keys setzt den NWK Frame Counter von allen Geräten im Netzwerk zurück. Geräte deren Frame Counter den Wert 0xFFFFFFFF erreicht, können keine Netzwerk verschlüsselten Nachrichten mehr senden.

- Es reduziert das Risiko, dass der Network-Key kompromittiert wird.

Der Zeitpunkt, wann ein Network-Key aktualisiert werden sollte, kann auf Basis unterschiedlicher Faktoren beruhen. Beispiele hierfür können sein, wenn das Trust Center eine Nachricht entdeckt, bei welcher der Frame Counter größer als 0x80000000 ist. Wenn das Trust Center eine eingebaute Uhr hat, sollte der Network-Key mindestens einmal jährlich aktualisiert werden. Es wird jedoch nicht empfohlen den Network-Key häufiger als alle 30 Tage zu wechseln, es sei denn, es wird vom Applikationsprofil erwartet. Trust Center, welche keine eingebaute Uhr besitzen, sollten den Network-Key erneuern, sobald der ausgehende Frame Counter den Wert 0x40000000 übersteigt. [3, S. 449-450]

3.9. Link-Key Lebensdauer

Für Link-Keys gibt es keine definierte maximale Dauer wie lange diese in Verwendung bleiben dürfen. Es wird zwar empfohlen den Link-Key periodisch zu aktualisieren, es gibt jedoch keine konkreten Vorgaben. Vorkonfigurierte Link-Keys können eine sehr lange Lebensdauer haben da nicht festgestellt werden kann, wie lange diese in Verwendung waren bevor das Gerät dem Netzwerk beigetreten ist. [3, S. 449]

3.10. Frame Counter Anforderungen

Geräte müssen Frame Counter persistent speichern und dürfen diesen auch nicht nach Wiederherstellung des Werkszustandes zurücksetzen. Hersteller können allerdings alternative Mechanismen einbauen um alle persistent gespeicherten Daten auf dem Gerät zu löschen. Die einzige Ausnahme für ein Gerät seinen Frame Counter zurückzusetzen während es sich in einem Netzwerk befindet ist, wenn es ein APSME-SWITCH-KEY Kommando empfängt oder der Frame Counter den Wert 0x80000000 übersteigt. [3, S. 385]

3.11. AES CCM*

CCM* (Counter mit CBC-MAC) ist ein generischer Verschlüsselungs- und Authentifizierungs-Block Cipher Modus. Der CCM* Modus entspricht dem CCM Modus des MAC Layers, wobei beim CCM* immer eine Verschlüsselungsfunktion mit 128-Bit Block-Cipher zu verwenden ist. Bei ZigBee wird hierbei der AES-128 für die Verschlüsselung verwendet. Ein weiterer unterschied zum CCM ist, dass beim CCM* ein Message Integrity Code (MIC) variabler Länge verwendet werden kann. Die zur Verfügung stehenden Längen sind 0, 4, 8, oder 16 Byte. [3, S. 456] Der MIC ist dafür zuständig, die Authentizität von Nachrichten zu gewährleisten.

Security Level Identifier	Security Attributes	Data encryption	Frame Authenticity (Length of MIC in Bytes)
0x00	None	No	No (M = 0)
0x01	MIC-32	No	Yes (M = 4)
0x02	MIC-64	No	Yes (M = 8)
0x03	MIC-128	No	Yes (M = 16)
0x04	ENC	Yes	No (M = 0)
0x05	ENC-MIC-32	Yes	Yes (M = 4)
0x06	ENC-MIC-64	Yes	Yes (M = 8)
0x07	ENC-MIC-128	Yes	Yes (M = 16)

Tabelle 3.3.: Verfügbare Security Level im Network und Application Layer

In Tabelle 3.3 auf Seite 27 sind die dem Network Layer und Application Layer zur Verfügung stehenden Verwendungsmodi des AES-CCM* aufgelistet. [3, S. 425]

3.12. Network Layer Sicherheit

Sicherheit auf dem Network Layer wird angewendet, wenn das Security-Flag im Netzwerk Header TRUE ist. In diesem Fall wird im Frame ein Auxiliary Header und ein Integrity Code angehängt. Der Network Layer Schutzmechanismus verwendet den Advanced Encryption Standard (AES) im CCM* Modus. Das Sicherheitsniveau wird im Auxiliary Header festgelegt. In Abbildung 3.2 ist ein Beispiel des Network Frames zu sehen, wenn Sicherheitsmechanismen aktiviert sind. [3, S. 378]

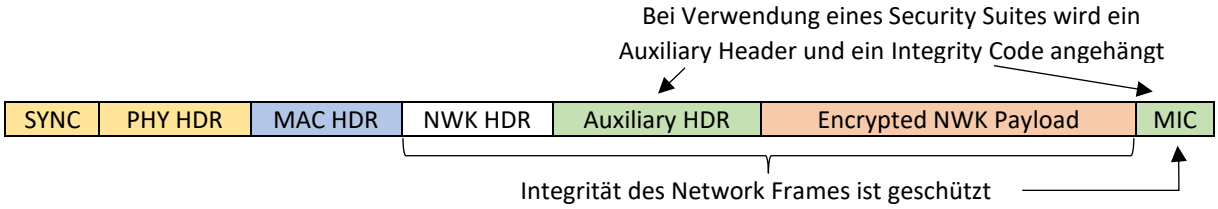

Abbildung 3.2.: Format Network Security Frames

3.13. Application Layer Sicherheit

Wenn Frames vom Application Layer ausgehen, muss sich der APS Sublayer um die Sicherheit des Frames kümmern. Die Sicherheit des APS Layers kann auf einem Link-Key oder dem Network-Key basieren. In Abbildung 3.3 ist ein Beispiel des APS Frames zu sehen, wenn Sicherheitsmechanismen aktiviert sind. [3, S. 379]

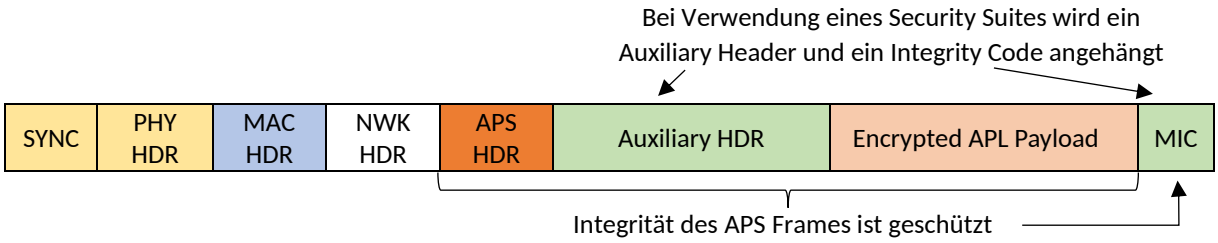

Abbildung 3.3.: Format des Application Security Frames

3.14. Auxiliary Header

Der Auxiliary Header enthält wichtige Informationen zur Sicherheit des versendeten Frames und wird entweder vom Network Layer oder vom Application Layer angehängt. Dieser Header besteht aus Security Control, Frame Control, Source Adresse und Key Sequence Number. [3, S. 424-426]

Byte: 1	4	0/8	0/1
Security Control	Frame Counter	Source Adresse	Key Sequence Number

Abbildung 3.4.: Format des Auxiliary Headers

3.14.1. Security Control

Das Security Control Feld besteht aus Security Level, Key Identifier und Extended nonce. Der Aufbau des Frame Control Feldes ist in Abbildung 3.5 ersichtlich.

Bits: 0-2	3-4	5	6-7
Security level	Key identifier	Extended nonce	Reserved

Abbildung 3.5.: Format des Frame Control Feldes im Auxiliary Header

Security Level

Dieses Feld gibt an, welche Sicherheitsmaßnahmen bei einem Frame angewendet wurden. Weiters bestimmt dieses Feld, ob die Payload verschlüsselt ist und ob die Authentizität gewährleistet ist. Die Werte, welche hier eingetragen werden können, sind in Tabelle 3.3 auf Seite 27 ersichtlich.

Key Identifier

Dieses Feld gibt an, welche Art von Schlüssel für die Sicherheit des Frame verwendet wurde. Die möglichen Werte sind 0x00 (Data Key), 0x01 (Network Key), 0x02 (Key-Transport Key) oder 0x03 (Key-Load Key). Welcher der zur Verfügung stehenden Schlüssel verwendet wird hängt vom Frame-Typen ab und und von welchem Layer aus der Frame versendet wird.

Extended Nonce

Dieses Feld gibt an, ob die Source Adresse im Auxiliary Header vorhanden ist. Ist dies der Fall, enthält dieses Feld den Wert 0x1, sonst 0x0. Wenn Network Frames geschützt werden sollen, muss der Wert dieses Feldes 0x1 betragen, das bedeutet, dass die Source Adresse im Auxiliary Header gesetzt werden muss. Bei Application Frames gibt es zwei Möglichkeiten, weshalb das Feld des Extended Nonce Feldes auf 0x1 gesetzt wird. [3, S. 381] Zum einen, wenn es sich um ein APS Command Frame handelt. Zum anderen, wenn das TxOptions Attribut in der NIB den wert 0x10 hat. [3, S. 19] Ein Wert von 0x10 bedeutet, dass die Source Addresse bei allen ausgehenden Application Frames im Auxiliary Header vorhanden sein muss. In allen anderen Fällen muss das Extended Nonce Feld den Wert 0x0 beinhalten. [3, S. 387]

3.14.2. Frame Counter

Dieses Feld soll verhindern, dass Frames mit dem selben Counter mehrmals hintereinander geschickt werden. Dieses Feld dient dem Schutz gegen sogenannte Replay-Angriffe. Bei diesen Angriffen versucht ein Angreifer oder eine Angreiferin bereits gesendete Nachrichten erneut zu schicken. Somit soll das Zielgerät zur erneuten Ausführung der aufgezeichneten Befehle gebracht werden. Der Frame Counter ist eine Zahl, welche immer dann erhöht wird, wenn eine Nachricht empfangen oder gesendet wird. Wird nun eine Nachricht empfangen bei welcher der Frame Counter niedriger ist als der momentan gespeicherte, wird die Nachricht verworfen.

3.14.3. Source Address

Dieses Feld enthält, wenn vorhanden, die 64-Bit Adresse des Gerätes, welche für den Schutz des Frames zuständig ist. Dieses Feld ist optional und nur vorhanden, wenn das „Extended Nonce“ Feld dementsprechend gesetzt wurde. Es ist anzumerken, dass es sich hierbei um die Source Adresse im Auxiliary Header handelt. Das bedeutet, dass die Source Adresse im Network Header nach wie vor mitgesendet wird.

3.14.4. Key Sequence Number

Die Key Sequence Number wird im Auxiliary Header mitgeschickt, wenn der zur Verschlüsselung verwendete Schlüssel der Network-Key ist. Dieses Feld gibt die Sequenznummer des aktuell gültigen Network-Keys an, welcher für die Ver- bzw. Entschlüsselung verwendet werden soll.

3.14.5. Nonce

Die Nonce, welche für das Ver- und Entschlüsseln von Nachrichten verwendet wird, setzt sich aus der 8-Byte Source Adresse, 4-Byte Frame Counter und 1-Byte Security Control Feld des Auxiliary Headers zusammen. Diese Werte sind explizit im Frame vorhanden, das heißt, es gibt kein eigenes Nonce Feld. Hat das „Extended Nonce“ Feld im Auxiliary einen Wert von 0x0, wird anstatt der Source Adresse im Auxiliary Header die 64-Bit IEEE Adresse des Gerätes verwendet, welches für den Schutz des Frames zuständig ist. In diesem Fall befindet sich die IEEE Adresse im Network Header.

4. ZigBee 2012 zu ZigBee 3.0

Mit ZigBee 3.0 wurden im Bereich Sicherheit einige Änderungen eingeführt. In diesem Kapitel wird der Unterschied zwischen ZigBee 3.0 und früheren Protokollversionen in Bezug auf Sicherheitsmaßnahmen beleuchtet.

Um einen Vergleich zu früheren ZigBee Versionen ziehen zu können, werden Änderungen von der ZigBee Pro 2015 Spezifikation (Revision 21) zu der ZigBee Spezifikation (Revision 20) erläutert. Revision 20 der ZigBee Spezifikation wurde 2012 veröffentlicht und beinhaltet die letzten Änderungen, bevor mit der ZigBee Pro 2015 Spezifikation ZigBee 3.0 ins Leben gerufen wurde. Zur leichteren Lesbarkeit wird in diesem Kapitel die ZigBee Pro 2015 Spezifikation als ZigBee 3.0 und die ZigBee Spezifikation 2012 als ZigBee 2012 bezeichnet.

In Tabelle 4.1 auf Seite 38 ist eine Zusammenfassung der Änderungen zu sehen, welche sich mit ZigBee 3.0 ergeben haben. Die einzelnen Änderungen werden nachfolgend im Detail beschrieben.

4.1. Applikationsprofile

Um sicherzustellen, dass ZigBee Geräte unterschiedlicher Hersteller miteinander kommunizieren können, werden sogenannte Applikationsprofile wie beispielsweise Home Automation eingesetzt. Insgesamt definiert ZigBee über 130 Gerätetypen und dazugehörige Kommandos. [14] Dennoch kommt es vor, dass Geräte unterschiedliche „Dialekte“ sprechen, wodurch es zu Kompatibilitätsproblemen kommen kann, auch wenn das selbe Applikationsprofil verwendet wird. Erschwerend kommt hinzu, dass die Spezifikationen der Applikationsprofile über mehrere Dokumente verteilt sind. Allgemein gibt es bei ZigBee 2012 sogenannte „Public Application Profiles“ und „Device Specific Application Profiles“. Für jedes Applikationsprofil gibt es ZigBee Cluster Libraries welche beschreiben, welche Funktionen und Befehle von einem Gerät unterstützt werden müssen. [13, S. 78]

Bei ZigBee 3.0 Geräten gibt es nur noch ein einziges Applikationsprofil, welches alle früheren Applika-

tionsprofile und daher auch Cluster Libraries in sich vereint. Diese sind in der ZigBee Cluster Library Spezifikation (Revision 6) beschrieben. [15] ZigBee 3.0 Profile werden via sogenannten „Cluster Identifier“ unterschieden. Ein ZigBee 3.0 Gerät muss beim Beitritt in ein Netzwerk bekanntgeben, welche Cluster unterstützt werden. Wie auch bei den Applikationsprofilen in ZigBee 2012, geben diese Cluster vor, wie Nachrichten formattiert werden müssen und wie Kommunikation zwischen Geräten stattzufinden hat.

4.2. Sicherheitsschlüssel

Bei den Sicherheitsschlüsseln wurden einige Änderungen beim Network-Key durchgeführt. Die Unterschiede beziehen sich hierbei nicht darauf, wie Nachrichten mit den Schlüsseln abgesichert werden, sondern bestimmen eher, wie die Schlüssel verwaltet und eingesetzt werden.
Bei ZigBee 2012 stehen zwei Arten von Network-Keys zur Verfügung, der „Standard Network-Key“ und der „High-Security Network-Key“. Ein Standard Network-Keys gibt an, dass der Schlüssel im „Standard Security Mode “ verwendet wird und entweder via Key-Transport oder via dem alten Network-Key transportiert wird. Ein High-Security Network-Key gibt an, dass der Schlüssel im „High-Security Mode“ verwendet wird und ausschließlich via Key-Transport transportiert werden darf. Das bedeutet, dass der neue Netzwerkschlüssel nur mit einem vom Link-Key abgeleiteten Key-Transport Key verschlüsselt via Unicast zum jeweiligen Gerät übertragen werden darf. [13, S. 428]

Der Unterschied zwischen High und Standard Security Mode liegt darin, dass beim High Security Mode das Trust Center eine Liste mit Unique TC-Link Keys für jedes Gerät im Netzwerk führen muss. Die jeweiligen Link-Keys werden beim Beitritt von Geräten vom Trust Center generiert und an diese übertragen. Weiters muss das nwkAllFresh Attribut der Network Information Base (NIB) auf TRUE gesetzt sein. Dies bewirkt, dass Frames, bei denen der Frame-Counter übergelaufen ist, ebenfalls auf Neuartigkeit überprüft werden. Dies hat zur Folge, dass Nachrichten von Geräten, bei denen der Frame Counter übergelaufen ist, nicht mehr akzeptiert werden. [13, S. 504]

Im Standard Security Mode können Geräte entweder den globalen TC-Link Key oder einen Unique TC-Link Key zur Kommunikation mit dem Trust Center verwenden. Weiters ist in diesem Fall das nwkALLFresh Attribut auf FALSE gesetzt. [13, S. 504]

Wie in Kapitel 3.4 beschrieben wurde, ist bei ZigBee 3.0 nur ein Netzwerkschlüssel im Einsatz. Dieser kann entweder verteilt oder zentralisiert eingesetzt werden. Der Standard Security Mode in ZigBee 3.0

wurde um jene Funktionen erweitert, welche bei ZigBee 2012 den High-Security Mode definiert haben. Dadurch fällt dieser bei ZigBee 3.0 weg und es wird standardmäßig der High-Security Mode verwendet. Dies bedeutet, dass in ZigBee 3.0 Netzwerken Geräte die Fähigkeit besitzen müssen, Link-Keys in ihrer Network Information Base zu verwalten. [3, S. 380]

4.3. Key Switch

Bei ZigBee 2012 werden Geräte im Netzwerk via dem „Switch-Key Service“ darüber informiert, zu einem anderen aktiven Netzwerkschlüssel zu wechseln. [13, S. 432] In der ZigBee Spezifikation (Revision 20) wird jedoch nicht beschrieben was geschieht, wenn ein alter Network-Key zur Kommunikation verwendet wird. Weiters scheint es keine maximale Dauer zu geben welche definiert, wie lange ein Netzwerkschlüssel in Verwendung sein darf. Wird der Network-Key im High-Security Mode verwendet, wird dieser via Unicast an die jeweiligen Geräte im Netzwerk gesendet. Der Network-Key wird hierbei mittels den zugehörigen Link-Keys verschlüsselt übertragen. Wird der Standard-Security Mode verwendet, wird der neue Network-Key mittels dem alten Network-Key verschlüsselt übertragen.

Wie in Kapitel 3.7 auf Seite 23 beschrieben wurde, wurden mit ZigBee 3.0 Regelungen und Vorgaben zum Ablauf beim Wechseln des Netzwerkschlüssels festgelegt oder genauer spezifiziert. Schlüssel können via Broadcast oder Unicast verteilt werden, wobei bei Broadcast der alte Netzwerkschlüssel und bei Unicast der entsprechende Link Key zum Schutz des neuen Netzwerkschlüssels verwendet wird. Weiters wurden Regelungen eingeführt, dass sobald ein neuer Netzwerkschlüssel in Verwendung ist, nur noch dieser zum Versenden von Nachrichten genutzt werden darf. Wie in Kapitel 3.8 auf Seite 25 beschrieben wurde, gibt es nun auch Regelungen dazu, wie lange ein Netzwerkschlüssel verwendet werden darf bis dieser ersetzt werden muss. [3, S. 450-451]

4.4. Install Codes

Damit ZigBee 2012 Geräte bei der erstmaligen Verbindung mit dem Netzwerk den aktiven Netzwerkschlüssel erhalten können, wird entweder der Default Trust Center Link Key (ZigBeeAlliance09) oder ein vordefinierter Schlüssel verwendet. [13, S. 432] Der Default Trust Center Link Key hat den Nachteil, dass ein Angreifer oder eine Angreiferin die erste Verbindung aufzeichnen und so den Netzwerkschlüssel erhalten können. Ein vordefinierter Schlüssel hat den Nachteil, dass das Trust Center den Schlüssel ebenfalls kennen muss, was zu Kompatibilitätsproblemen zwischen unterschiedlichen Herstellern führen kann. Die Verwendung von Installationscodes ist zwar in Revision 20 der ZigBee Spezifikation enthal-

ten, wird jedoch nur beiläufig erwähnt. [13, S. 431]

Bei ZigBee 3.0 wird neben dem Default Trust Center Link Key und vordefinierten Schlüsseln, ebenfalls die Verwendung von Installationscodes unterstützt und als eigene Kategorie von Link-Keys aufgenommen. Von einem Install Code abgeleitete Schlüssel werden hierbei „Install Code Link Keys“ genannt. Diese Codes können beispielsweise in Form von QR-Codes mit den jeweiligen Geräten mitgeliefert werden. Von diesem Installationscode wird im weiteren Verlauf ein Unique Trust Center Link-Key abgeleitet, welcher für die weitere Kommunikation und zur Übertragung des Netzwerkschlüssels verwendet wird. Der Vorteil dieser Methode ist, dass jedes Gerät bei der erstmaligen Verbindung einen unterschiedlichen Schlüssel verwendet. [3, S. 378, 380]

4.5. Frame Counter

Bei ZigBee 2012 Geräten gibt es keine Vorgaben, wie Frame Counter verwaltet beziehungsweise gespeichert werden müssen. Dies führt dazu, dass Angriffe wie die „Energy Depletion Attack“, welcher in Kapitel 1.3 auf Seite 2 beschrieben wurde, zur Zurücksetzung des Frame Counters geführt haben. Dies hat zur Folge, dass bereits gesendete Frames erneut gesendet werden können. Der Grund dafür ist, dass Frame Counter nicht persistent gespeichert und bei einem Neustart oder beim Zurücksetzen von Geräten gelöscht und neu initialisiert werden.

Wie in Kapitel 3.10 auf Seite 26 beschrieben wurde, dürfen Frame Counter bei ZigBee 3.0 Geräten unter keinen Umständen zurückgesetzt werden. Dies inkludiert auch die Wiederherstellung des Werkszustandes. Die einzige Ausnahme, in welcher ein Frame Counter zurückgesetzt werden darf ist, wenn das Trust Center im Netzwerk einen neuen Netzwerkschlüssel ausstellt. [3, S. 385]

4.6. Netzwerkbeitritt

In ZigBee 2012 Netzwerken war es möglich das Netzwerk unendlich lange für Beitritte von Geräten zu öffnen. Möglich machte dies das Mgmt_Permit_Joining_req Kommando. Dieses beinhaltet die Felder PermitDuration und TC_Significance. PermitDuration kann einen Wert von 0x00 bis 0xFF annehmen und beschreibt die maximale Zeitdauer in Sekunden, in der dem Netzwerk beigetreten werden kann. 0x00 sagt aus, dass keine Netzwerkbeitritte erlaubt sind und 0xFF setzt den Timer auf „unendlich“. TC_Sagnificance kann den Wert 0x00 oder 0x01 annehmen und bestimmt, ob die Trust Center Policy durch den Befehl geändert wird. Durch das Senden eines Mgmt_Permit_Joining_req Kommandos mit

einem PermitDuration Wert von 0xFF war es in ZigBee 2012 Netzwerken somit möglich, die Dauer in der Netzwerkbeitritte erlaubt sind auf unbegrenzte Zeit zu erlauben.

In ZigBee 3.0 Netzwerken ist dies nicht mehr möglich, da ein PermitDuration Wert von 0xFF immer als 0xFE interpretiert wird. Das bedeutet, dass das Netzwerk maximal für eine Dauer von 254 Sekunden für Beitritte geöffnet werden kann. [3, S. 125]

4.7. Insecure Rejoin

In ZigBee 2012 können Geräte einen sogenannten „Insecure Rejoin“ durchführen. Dadruch ist es für ein Engerät möglich, ohne Kenntnis über den aktuellen Network-Key, einen neuen Network-Key anzufordern. In ZigBee 3.0 Netzwerken ist standardmäßig nicht mehr möglich, da bei Trust Centern das sogenannte „allow-Rejoins“ Attribut auf FALSE gesetzt werden sollte. Dieses Attribut sagt aus, ob es einem Endgerät gestattet ist mit Hilfe des Default Trust Center Link Keys einen Rejoin durchzuführen. Ist das Attribut auf FALSE gesetzt, muss ein Unique Trust Center Link Key verwendet werden um den Rejoin in das Netzwerk durchzuführen. Damit das Gerät dem Netzwerk wieder beitreten kann, muss im vorhinein eine legetime Verbindung zum Trust Center bestanden haben. Andernfalls wäre das Endgerät nicht im Besitz eines Unique Trust Center Link Keys. Es ist jedoch anzumerken, dass ein Insecure Rejoin auch in ZigBee 3.0 Netzwerken als letzte Option möglich ist, sollte der Hersteller des Gerätes dies zulassen. [3, S. 371] Das bedeutet, es kann von Gerät zu Gerät unterschiedlich sein, ob Insecure Rejoins in ZigBee 3.0 Geräten möglich sind oder nicht.

4.8. End Device Aging

In ZigBee 3.0 wurde der „End Device Aging Mechanismus“ eingeführt. Dieser sorgt dafür, dass Endgeräte nach einer definierten Dauer veralten und das Netzwerk verlassen müssen. Die Dauer, bis ein Geräte auf Grund des Aging Mechanismus aus dem Netzwerk ausgeschlossen wird, wird vom jeweiligen Parent (Router oder Trust Center) festgelegt. Alle ZigBee 3.0 Geräte, die einem ZigBee 3.0 Netzwerk beitreten, werden mit einer vordefinierten Timeout-Länge initiiert. Der Standardwert ist im sogenannten “nwkEndDeviceTimeoutDefault“ Attribut in der NIB definiert und kann auf einen Wert zwischen

Octets: 1	1
Permit Duration	TC_Significance

Abbildung 4.1.: Format des Mgmt_Permit_Joining_req Kommandos

10 Sekunden und 16384 Minuten (ungefähr 11 Tage) gesetzt werden. Die Höhe des darin befindlichen Wertes ist von Hersteller zu Hersteller unterschiedlich und kann auch durch diesen definiert werden. Die Einführung dieses Mechanismus hat den Hintergrund, dass somit Informationen über verwaltete Endgeräte von Routern aktuell gehalten werden können. Ein Endgerät muss periodisch sogenannte „keepalive“ Nachrichten schicken, um den Aging Timer zurückzusetzen. [3, S. 363]

ZigBee 2012	ZigBee 3.0
Applikationsprofile	
• Public und Device Specific Application Profiles • Spezifikationen über mehrere Dokumente verteilt	• 1 Applikationsprofil • Beschrieben in der ZigBee Cluster Library Spezifikation (Revision 6)
Sicherheitsschlüssel	
• 1 Network-Key im Standard oder im High Security Mode • Security-Mode bestimmen das Sicherheitsniveau beim Schlüsselaustausch	• 1 Network-Key • 1 Security Mode (Standard Security Mode) • ZigBee 2012 High Security Mode = ZigBee 3.0 Standard Security Mode
Key Switch	
• Keine konkreten Vorgaben zur maximalen Lebensdauer von Sicherheitsschlüssel	• Regelungen, wann der Network-Key aktualisiert werden sollte • Maximale Lebensdauer von Network-Keys definiert • Regelungen zur Verwendung von alten Network-Keys • Keine Vorgaben für Link-Keys
Install Codes	
• Install Codes nur herstellerspezifisch unterstützt • Im Standard nicht verankert • Geräte müssen Install Codes nicht unterstützen	• Install Codes als Methode zum sicheren Netzwerkbeitritt im Standard verankert • Trust Center und Router müssen Install Codes zum Beitritt unterstützen
Frame Counter	
• Nicht persistent gespeichert • Werden beim Neustart und Zurücksetzen von Geräten neu initialisiert	• Persistent gespeichert • Dürfen nur durch Ausstellen eines neuen Schlüssels durch das Trust Center zurückgesetzt werden • Implementierung von Methoden zum löschen von persistenten Daten (z.B.: Frame Counter) ist Herstellern überlassen

ZigBee 2012	ZigBee 3.0
Insecure Rejoin	
• Geräte können Trust Center Rejoins durchführen	• Sollte standardmäßig deaktiviert sein, hängt jedoch vom Hersteller ab
Netzwerkbeitritt	
• Netzwerk kann auf unbegrenzte Zeit für Beitritte geöffnet werden	• Netzwerk kann maximal 254 Sekunden für Beitritte geöffnet werden
End Device Aging	
• Mechanismus nicht vorhanden	• Geräte werden nach 10 Sekunden bis 16384 Minuten (11 Tage) Inaktivität vom Trust Center aus dem Netzwerk entfernt • Geräte müssen periodisch Keep-Alive Nachrichten an das Trust Center schicken

Tabelle 4.1.: Zusammenfassung der Änderungen zu ZigBee 3.0

5. Angriffsmöglichkeiten

In diesem Kapitel werden Angriffe erläutert, welche gegen ZigBee Netzwerke und Geräte in der Vergangenheit erfolgreich durchgeführt werden konnten. Basierend auf den Erkenntnissen, welche in Kapitel 3 - ZigBee 3.0 - Sicherheit und Kapitel 4 - ZigBee 2012 zu ZigBee 3.0 gewonnen wurden, wird evaluiert, ob diese Angriffe gegen ZigBee 3.0 Geräte und Netzwerke ebenfalls möglich sind. Die Evaluierung basiert hierbei auf einer Analyse der ZigBee PRO 2015 Spezifikation. [3]

5.1. Überblick

Im Bereich der ZigBee Sicherheit gab es mehrere Forschungsarbeiten, welche sich mit ZigBee Sicherheit allgemein und mit möglichen Angriffen auf ZigBee Netzwerke und Geräte beschäftigt haben. [6][8][7] Angriffe, welche erfolgreich durchgeführt werden konnten, führten jedoch stets auf folgende Szenarien zurück:

- Entschlüsselung der Erstübertragung des Network-Keys
- Replay-Angriff durch Zurücksetzen des Frame Counters
- Übernahme von Geräten
- Insecure Rejoin

Nachfolgend werden die einzelnen Angriffsszenarien im Detail erklärt und evaluiert, ob diese Angriffe bei ZigBee 3.0 nach wie vor möglich sind.

5.2. Erstübertragung des Network-Keys

Wenn ein Gerät einem ZigBee Netzwerk beitreten will, muss dieses bei der ersten Verbindung einen Network-Key erhalten um mit anderen Geräten im Netzwerk kommunizieren zu können. Wie in Kapitel 3.6 beschrieben wurde, wird der Network-Key beim Netzwerkbeitritt entweder mit dem Global

Trust Center Link-Key oder einem Unique Trust Center Link-Key verschlüsselt übertragen. Dieser Angriff nutzt die Tatsache aus, dass viele Geräte den Global Trust Center Link-Key zur Absicherung der Schlüsselübertragung verwenden.

5.2.1. Ablauf des Angriffes

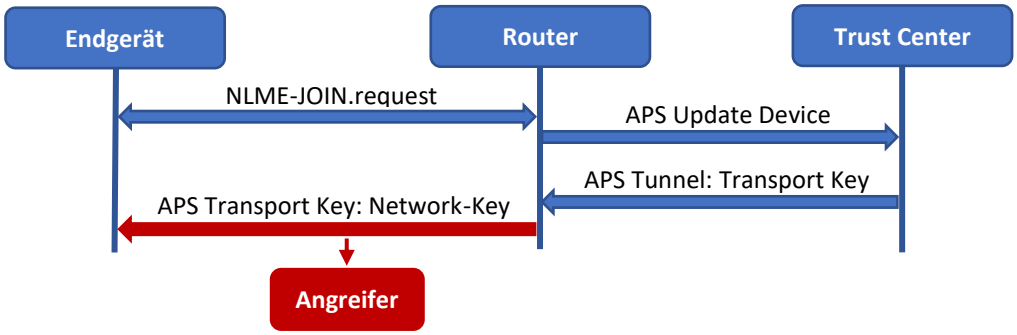

Abbildung 5.1.: Übertragung des Network-Keys beim Netzwerkbeitritt

In Abbildung 5.1 ist der Zeitpunkt der Schlüsselübertragung abgebildet, bei welchem der Network-Key übertragen wird. Um diesen Angriff erfolgreich durchzuführen, muss ein Angreifer oder eine Angreiferin in der Lage sein die erste Verbindung eines Gerätes mitlesen zu können. Weiters beruht dieser Angriff darauf, dass für die Absicherung der Schlüsselübertragung der Global Trust Center Link-Key (GTCLK) verwendet wird.

Wird diese Übertragung erfolgreich mitgelesen, ist der Angreifer oder die Angreiferin im Besitz des mit dem Global Trust Center Link-Key verschlüsselten Network-Keys. Wie in Kapitel 3.4 beschreiben wurde, hat der Global Trust Center Link Key den Standardwert “ZigBeeAlliance09„. Somit kann der Network-Key unter Anwendung des AES-CCM* Algorithmus und der entsprechenden Nonce, beschrieben in Kapitel 3.14, entschlüsselt werden.

5.2.2. Auswirkung

Ab dem Zeitpunkt, an dem der Network-Key bekannt ist, kann jegliche Network Layer und bestimmte Application Layer Kommunikation entschlüsselt werden, was die Integrität des gesamten Netzwerks schädigt.
Wie in Kapitel 3.6 beschrieben wurde kommt hinzu, dass wenn ein Gerät dem Netzwerk beitritt und noch keinen Link-Key besitzt, dieser mit dem Network-Key verschlüsselt übertragen wird. Dadurch kann potentiell zusätzlich zum Network-Key auch der Link-Key von beitretenden Geräten entschlüsselt werden.

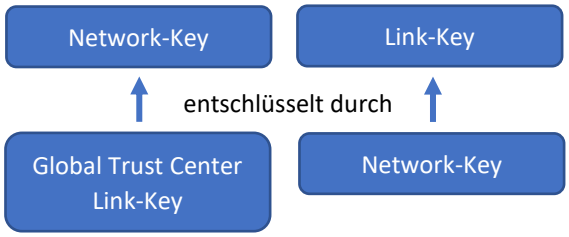

Abbildung 5.2.: Auswirkung der Kompromittierung des Network-Keys

5.2.3. Erfolgschance bei ZigBee 3.0

Dieser Angriff ist auch bei ZigBee 3.0 Geräten und Netzwerken noch möglich. In der ZigBee PRO Spezifikation wurden zwar Install Codes als Möglichkeit zum sicheren Netzwerkbeitritt festgelegt, diese Möglichkeit muss jedoch nicht verpflichtend verwendet werden. Die Routine, wie ein Gerät beim Beitreten eines Netzwerks den Network-Key erhält, hat sich zu ZigBee 3.0 nicht verändert.

Die Tatsachen, dass bei der ersten Schlüsselübertragung der Network-Key mit dem Global Trust Center Link Key abgesichert wird und somit das Netzwerk verwundbar wird, ist auch in der ZigBee Pro Spezifikation angemerkt und als bekanntes Risiko akzeptiert. [3, S. 380]

5.3. Replay-Angriff

Bei einem Replay-Angriff versucht ein Angreifer oder eine Angreiferin bereits gesendete Frames erneut an Geräte im Netzwerk zu schicken. Hierbei ist das Ziel, bereits aufgezeichnete Kommunikation an ein Gerät senden zu können, damit dieses Befehle oder Aktionen erneut durchführt, ohne Zugriff auf Schlüsselmaterial wie den Network-Key oder Link-Keys zu haben. Um in ZigBee Netzwerken Geräte vor Replay-Angriffen zu schützen, wird der sogenannte Frame Counter eingesetzt. Dieser Frame Counter wird im Auxiliary Header mitgesendet, welcher in Kapitel 3.14 beschrieben wurde.

5.3.1. Ablauf des Angriffes

Wie in Kapitel 4.5 auf Seite 34 beschrieben wurde, werden Frame Counter in Geräten, die eine ältere ZigBee Version verwenden, nicht persistent gespeichert. Diese Tatsache können Angreifer oder Angreiferinnen ausnutzen, um auch integritäts- und authentizitätsgesicherte Frames erneut senden zu können. Um dies zu erreichen, muss das Gerät zurückgesetzt oder neu gestartet werden, damit dieses den Frame Counter löscht und dem Netzwerk erneut beitritt.

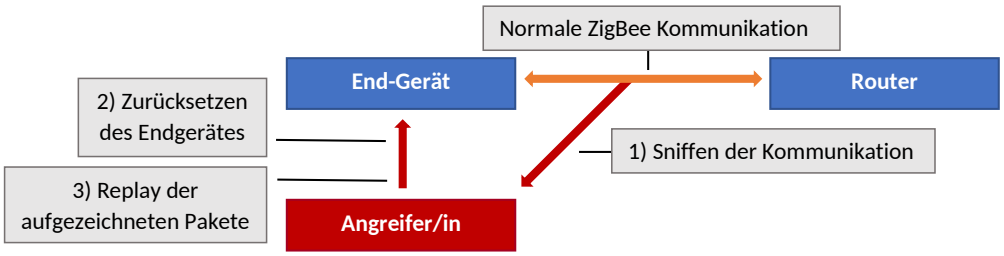

Abbildung 5.3.: Ablauf eines Replay-Angriffes

Bei physischem Zugriff auf das Zielgerät, kann das Gerät manuell zurückgesetzt werden. ZigBee Geräte haben meist herstellerspezifische Möglichkeiten ein Gerät, beispielsweise via einem Reset-Knopf, zurückzusetzen.

Ist kein physischer Zugriff gegeben, könnte eine sogenannte „Energy Depletion Attack“ [8] durchgeführt werden. Hierbei werden verschlüsselt Nachrichten an ein Endgerät gesendet, wodurch dieses versucht diese zu entschlüsseln. Die Nachrichten werden hierbei mit einem zufälligen Schlüssel verschlüsselt, wodurch das Zielgerät die Nachricht nicht entschlüsseln und verarbeiten kann. Ist das Gerät Batteriebetrieben, wird die Batterie dadurch schneller aufgebraucht und das Gerät muss früher oder später neu gestartet werden. Dadurch wird der Frame Counter neu initialisiert und zurückgesetzt. Diese Methode funktioniert, da der Frame Counter im Auxiliary Header nicht verschlüsselt wird. Dadurch kann ein Angreifer oder eine Angreiferin Nachrichten mit einem höheren Frame Counter senden, als das Gerät momentan verwendet und dieses wird versuchen die Nachrichten zu verarbeiten.

5.3.2. Auswirkung

Wenn ein Angreifer in der Lage ist ZigBee Nachrichten erneut zu senden, hat dies fatale Folgen für die Sicherheit des Netzwerkes. Wird solch ein Angriff beispielsweise bei einem ZigBee-Türschloss durchgeführt, kann ein Angreifer oder eine Angreiferin den Befehl für das Entsperren des Schlosses aufzeichnen und erneut abspielen. Das selbe Prinzip lässt sich ebenfalls auf ZigBee-Alarmanlagen übertragen, wobei diese durch einen erfolgreichen Replay-Angriff deaktiviert werden könnten.

5.3.3. Erfolgschance bei ZigBee 3.0

Wie in Kapitel 3.10 auf Seite 26 beschrieben wurde, dürfen bei ZigBee 3.0 Geräten Frame Counter, sowohl im Network-Layer als auch im APL-Layer, unter keinen Umständen zurückgesetzt werden. Dies inkludiert auch Neustarts und das Zurücksetzen in den Werkszustand. Die einzige Möglichkeit zum Zurücksetzen des Frame Counters ist durch das Ausstellen eines neuen Sicherheitsschlüssels, wobei aufge-

zeichnete Kommunikation nicht mehr gültig wäre, da diese mit einem veralteten Schlüssel verschlüsselt wurde. Dadurch kann dieser Angriff bei ZigBee 3.0 Geräten nicht mehr durchgeführt werden.

5.4. Übernahme von Geräten

Dieser Angriff kann bei ZigBee Geräten durchgeführt werden, welche das ZigBee Ligh Link Applikationsprofil [16] verwendet. Dieser Angriff wurde im „ZIGBEE EXPLOITED The good, the bad and the ugly“ [6] beschrieben und erfolgreich durchgeführt. Um den Angriff genauer beleuchten zu können, wird zunächst ein Überblick über die Spezifika des ZigBee Light Link Applikationsprofils [16] gegeben.

5.4.1. ZigBee Light Link Applikaationsprofil

Bei dem ZigBee Light Link Applikationsprofil handelt es sich um das am weitesten verbreitetste Applikationsprofil, welches von ZigBee Geräten eingesetzt wird. Wie der Name des Profiles bereits verrät, handelt es sich hierbei um Geräte die mit Beleuchtung zusammenhängen. Beispiele hierfür sind Glühbirnen, Lichtschalter und Dimmer-Controller.

Touchlink Commissioning

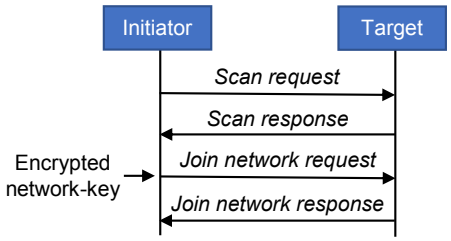

Abbildung 5.4.: Touchlink Commissioning Inter-PAN Transaktion

Geräte, welche unter dem ZigBee Light Link Applikationsprofil betrieben werden, verwenden häufig das sogenannte ZigBee Touchlink Commissioning um Netzwerken beizutreten. Hierbei handelt es sich um eine ZigBee Light Link spezifische Art, wie ein Gerät einem Netzwerk beitreten kann. Touchlink erlaubt es Geräten über einen Controller einem ZigBee Netzwerk beizutreten, ohne dass der Besitzer oder die Besitzerin des Gerätes mit dem beitretenden Gerät interagieren muss. Touchlink sollte nur dann funktionieren, wenn das beitretende Gerät und der Controller nahe beeinander sind. Abhängig von der verwendeten Hardware, kann der Beitritt via Touchlink jedoch über mehrere Meter Reichweite durchgeführt werden. In Abbildung 5.4 ist der Ablauf beim Beitreten eines Gerätes zu einem Netzwerk nach Touchlink Commissioning zu sehen. Ein Initiator sendet einen „Scan Request“ Befehl an ein Zielge-

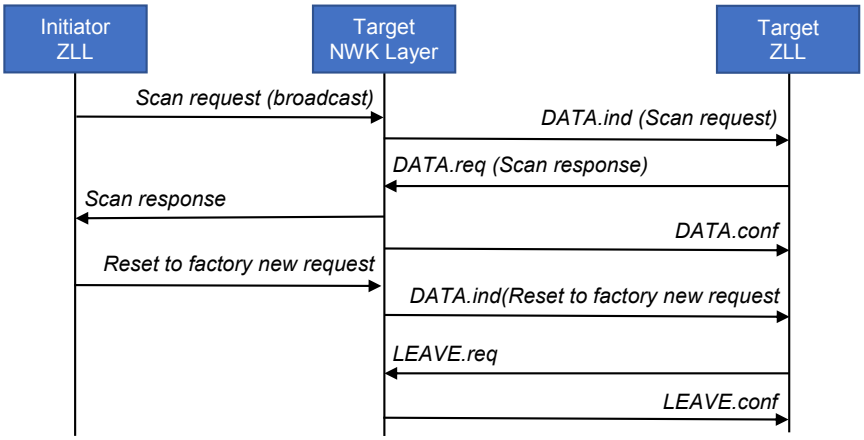

Abbildung 5.5.: ZLL Reset To Factory New

rät das Touchlink unterstützt. Ist dieses bereit einem Netzwerk beizutreten, teilt es dies dem Initiator in siner „Scan Response“ mit. Danach sendet der Initiator einen „Join Network Request“ Befehl. Dieser Befehl beinhaltet den verschlüsselten Network-Key welcher benötigt wird, damit das Gerät im Netzwerk mit anderen Geräten kommunizieren kann. Das Zielgerät sendet eine „Join Network Response“ um dem Initiator mitzuteilen, ob der Beitritt erfolgreich war.

Light Link Standardschlüssel

Alle ZigBee Light Link zertifizierten Geräte besitzen einen vorinstallierten Link-Key, welcher als ZigBee Light Link Master-Key bekannt ist. Dieser Link-Key wird von der ZigBee Alliance an Hersteller, welche zertifizierte Geräte produzieren, ausgegeben und muss geheim gehalten werden. Hintergrund hierfür ist, dass somit alle zertifizierten Geräte „sicher“ beitreten können, ohne den Default Trust Center Link-Key zu verwenden. Das Problem hierbei ist, dass dieser Link-Key in unterschiedlichen Quellen wie Twitter, Reddit, sowie mehreren Foren, geleaked wurde und somit bekannt ist. Der Light Link Master Key Lautet „9F 55 95 F1 02 57 C8 A4 69 CB F4 2B C9 3F EE 31“. Die Sicherheit von ZigBee Light Link gilt somit als kompromittiert.

Wie auch bei ZigBee 3.0 oder beim ZigBee Home Automation Applikationsprofil, kann auch bei ZigBee Light Link der Default Trust Center Link-Key mit dem Standardwert „ZigBeeAlliance09“ verwendet werden. Dies führt zu den selben Verwundbarkeiten wie beim initialen Austausch des Network-Keys, welcher im Kapitel 5.2 beschrieben wurde.

5.4.2. Ablauf des Angriffes

Um ein Gerät übernehmen zu können, muss dieses zunächst dazu gebracht werden erneut nach verfügbaren Netzwerken zu suchen. Bei Glühbirnen, welche das ZigBee Light Link Applikationsprofil verwenden, kann dies durch das Senden eines „Reset To Factory Default“ Befehles geschehen. [6][17] Um diesen Befehl erfolgreich senden zu können, muss der aktive Network-Key nicht im Besitz des Angreifers oder der Angreiferin sein.

In Abbildung 5.5 ist der Ablauf zu sehen, wie ein Gerät via dem „Reset To Factory Default“ Befehles zurückgesetzt wird. Hierzu muss der Angreifer oder die Angreiferin zunächst ein „Scan Request“ Kommando an das Zielgerät schicken. Damit beginnt das Gerät die zur Verfügung stehenden Channel zu scannen. Danach sendet der Angreifer oder die Angreiferin den „Reset To Factory New“ Befehl. Bei diesem Kommando handelt es sich um ein inter-PAN Kommando. Sind notwendige Parameter wie Source, Destination Addresse und command identifier (0x07 - reset to factory new request) korrekt gesetzt, wird das Zielgerät den Befehl akzeptieren und das Netzwerk verlassen. [16, S. 56] Beim Zurücksetzen wird im weiteren Verlauf gespeichertes Schlüsselmaterial gelöscht und das Gerät sucht erneut nach verfügbaren Netzwerken, denen beigetreten werden kann.

Es gibt auch alternativen zum Zurücksetzen via dem „Reset to factory new“ Kommando, hierzu muss das Gerät jedoch physisch zurückgesetzt werden. Hierbei ist das Vorgehen herstellerspezifisch, bei Glühbirnen können jedoch meist sogenannte „Energiezyklen“ durchgeführt werden. Ein Energiezyklus ist das Ein- beziehungsweise Ausschalten des Gerätes in definierten Zeitabständen. Ein Beispiel hierfür ist, dass zum Zurücksetzen das Gerät fünf Mal hintereinander für drei Sekunden eingeschalten und für drei Sekunden ausgeschalten werden muss. Nach der fünften Runde wird das Gerät noch einmal für fünf Sekunden eingeschalten. Nun befindet sich das Gerät im sogenannten „Pairing“ Modus und ist bereit einem neuen Netzwerk beizutreten. [18]

Egal wie das Gerät zurückgesetzt wird, es sucht nun nach verfügbaren Netzwerken. Betreibt ein Angreifer oder eine Angreiferin nun einen bösartigen Controller, kann das Gerät mittels dem bekannten ZigBee Light Link Master-Key verbunden werden, indem ein „Network Join End Device Request“ an das zurückgesetzte Gerät gesendet wird. Hierbei kann der Angreifer oder die Angreiferin einen eigenen Network-Key ausstellen, welcher mit dem geleakten Link-Key verschlüsselt wird und im Zuge des Beitrittes des Geräte an dieses übertragen wird.

5.4.3. Auswirkungen

Wird dieser Angriff erfolgreich durchgeführt, ist das ZigBee Light Link Gerät effektiv im Besitz des Angreifers oder der Angreiferin und der Besitzer oder die Besitzerin des Gerätes muss dieses zurücksetzten, um es wieder zum eigenen Netzwerk hinzuzufügen zu können.

Das größte Problem hierbei ist, dass es für ZigBee Geräte, welche Touchlink Commissioning zum Beitritt in Netzwerke unterstützen, keine Möglichkeit gibt diesen Angriff zu verhindern. Zur Durchführung dieses Angriffes ist in der Theorie ein Wandlichtschalter, welcher die Energiezufuhr zum Gerät trennen kann, bereits ausreichend.

5.4.4. Erfolgschancen bei ZigBee 3.0

Wie in Kapitel 4.1 beschrieben wurde, wurden frühere Applikationsprofile in die ZigBee Cluster Library Spezifikation [15] aufgenommen. Touchlink wird bei ZigBee 3.0 im sogenannten „Touchlink Commissionig“ Cluster beschrieben.

Dieser Angriff ist auch bei ZigBee 3.0 konformen Geräten noch durchführbar. In dem Paper „Insecure to the Touch: Attacking ZigBee 3.0 via Touchlink Commissioning“ [17] wurde die Umsetzung dieses Angriffes auf ZigBee 3.0 Geräte beschreiben. Das Vorgehen ist hierbei gleich dem Ablauf zum Übernehmen von älteren ZigBee Geräten. Das Gerät muss zurückgesetzt und zum erneuten Suchen nach Netzwerken gebracht werden. Auch hier war es möglich mit Hilfe des geleakten ZigBee Light Link Master-Keys ein Gerät zum Netzwerk des Angreifers oder der Angreiferin hinzuzufügen, was im weitern Verlauf bedeutet, dass der Master-Key auch in ZigBee 3.0 nicht geändert wurde. Weiters wurde bewiesen, dass obwohl Touchlink Commissioning nur in „naher Umgebung“ funktionieren sollte, dieser Angriff auf eine Reichweite von bis zu 190 Meter bei direktem Sichtkontakt und entsprechend starken Antennen durchgeführt werden konnte.

Der Grund, weshalb ZigBee Light Link ohne Änderungen in ZigBee 3.0 aufgenommen wurde, liegt sehr wahrscheinlich an der Rückwärtskompatibilität von ZigBee 3.0. Da ZigBee Light Link eines der verbreitetsten Applikationsprofile ist, wäre eine Änderung des Master-Keys eine große Herausforderung. Hersteller von Geräten die ZigBee Light Link verwenden und Touchlink Commissioning unterstützen, müssten den Master-Key in all ihren Geräten aktualisieren. Dies setzt vorraus, dass das Gerät eine Möglichkeit hat, den Schlüssel zu tauschen. Da es jedoch auch in ZigBee 3.0 keine Vorgaben zur Aktualisierung von Link-Keys gibt, vor allem wenn diese vorinstalliert sind, ist es sehr wahrscheinlich, dass

solche Aktualisierungsmethoden nicht für alle Geräte zur Verfügung stehen. Dies würde dazu führen, dass Geräte unterschiedlicher Hersteller unter Umständen nicht mehr kompatibel sind.

Als weiterer Punkt kommt hinzu, dass die Sicherheit von Geräten, welche via Touchlink Commissioning einem Netzwerk beitreten, auf der Geheimhaltung des ZigBee Light Link Master-Keys beruht. Die Sicherheit eines gesamten Netzwerkes auf die Geheimhaltung eines Master-Keys zu reduzieren, welcher einem Großteil der Hersteller von zertifizierten ZigBee 3.0 Geräten bekannt ist, würde auch bei einem neu ausgestellten Master-Key nicht sehr lange funktionieren.

5.5. Insecure Rejoin

Der „Insecure Rejoin“, auch Trust Center Rejoin genannt, ist eine Möglichkeit für ein Endgerät einem Netzwerk erneut beizutreten, sollte dieses nicht den aktuellen Netzwerkschlüssel besitzen. Dies kann vorkommen, wenn das Gerät beispielsweise den Tausch des Netzwerkschlüssels verpasst. Nachfolgend wird der Ablauf eines Insecure Rejoin erläutert und ein mögliches Angriffsszenario ausgehend vom Insecure Rejoin vorgestellt.

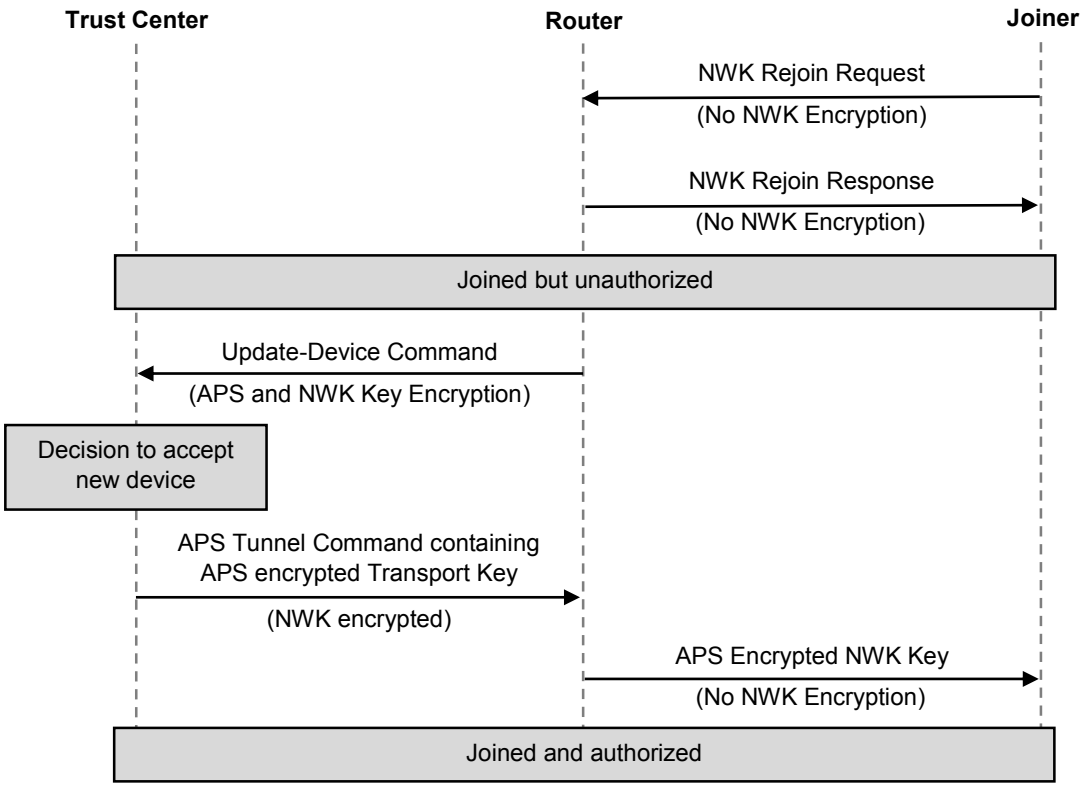

Abbildung 5.6.: Insecure Rejoin Ablauf [3, S. 435]

5.5.1. Ablauf

In Abbildung 5.6 ist der Ablauf eines Insecure Rejoins zu sehen. Im Gegensatz zum sogenannten „Secure Rejoin“, wird beim „Incecure Rejoin“ der NWK Rejoin Request vom Endgerät unverschlüsselt an sein Parentgerät gesendet. Das Parentgerät fügt das beitretende Gerät vorübergehend in das Netzwerk hinzu. Dieses ist hierbei noch nicht autorisiert. Der Router sendet im weiteren Verlauf ein „Update-Device Command“ and das Trust Center und dieses überprüft, ob das Gerät, welches dem Netzwerk beitreten möchte, akzeptiert wird. Basis davon ist, ob das beitretende Gerät bereits in der Network Information Base des Trust Centers eingetragen ist beziehungsweise war. Akzeptiert das Trust Center das beitretende Gerät, sendet dieses einen „Transport Key“ and das Parentgerät und dieses sendet den Network Key via APS Verschlüsselung an das Endgerät. Der neue Network-Key ist wie auch beim initialen Schlüsselaustausch hierbei mit dem Default Trust Center Link Key verschlüsselt. Das Endgerät muss nun eine valide NWK verschlüsselte ZigBee Nachricht an das Parentgerät senden. Wird diese Nachricht erfolgreich verarbeitet, wird das Endgerät dem Netzwerk als autorisiertes Gerät hinzugefügt. Der gesamte Prozess muss innerhalb von „apsSecurityTimeOutPeriod“ definierten Millisekunden geschehen. Andererseits wird das Endgerät wieder aus dem Netzwerk entfernt und dieses muss erneut versuchen einen Rejoin durchzuführen. [3, S. 435-436]

5.5.2. Angriffsszenario

Ein mögliches Angriffsszenario wurde in der Forschungsarbeit „ZIGBEE EXPLOITED The good, the bad and the ugly“ von T. Zillner vorgestellt.[6] Hierbei stört ein Angreifer gezielt die Netzwerkverbindung eines Endgerätes. Nachdem das Endgerät sich nicht mehr beim Parentgerät oder Trust Center melden kann, wird dieses aus dem Netzwerk entfernt. Versucht nun das Gerät via einem Insecure Rejoin dem Netzwerk wieder beizutreten, kann die Kommunikation von einem Angreifer oder einer Angreiferin mitgelesen werden. Wie auch beim initialen Schlüsselaustausch, wird der Network Key mit dem Default Trust Center Link Key verschlüsselt übertragen. Dies führt zu der selben Verwundbarkeit wie bei der initialen Schlüsselübertragung, welche in Kapitel 5.2 beschrieben wurde.

5.5.3. Erfolgschancen bei ZigBee 3.0

Auch in der ZigBee Pro 2015 Spezifikation wird ein Insecure Rejoin noch als Möglichkeit zum Wiederbeitritt in ein Nezwerk beschrieben. Die Entscheidung, ob ein Secure oder ein Insecure Rejoin möglich ist, hängt von der Implementierung des Herstellers des Gerätes ab. [3, S. 371] Wie auch bei der initialen Übertragung des Netzwerkschlüssels, ist auch dieser Angriff bei ZigBee 3.0 Geräten noch möglich. Es muss jedoch erwähnt werden, dass einige Hersteller die Möglichkeit bereitstellen Insecure Rejoins im

Netzwerk zu verbieten. Ein Beispiel wäre hierbei das SmartThings Hub, welches über die mitgelieferte App entsprechend konfiguriert werden kann. [19]

6. ZigBee 3.0 Scanner - Überblick

In diesem Kapitel werden jene Abhängigkeiten und Vorgaben definiert, welche für die Entwicklung des ZigBee 3.0 Scanners notwendig sind. Ziel des ZigBee 3.0 Scanners ist es, Daten über die Verbreitung von ZigBee 3.0 Netzwerken zu sammeln und dessen implementierten Sicherheitsmechanismen zu evaluieren.

6.1. Gesammelte Daten

Nachfolgend werden die Datenarten festgelegt, welche via dem Scanner gesammelt werden sollen. Hauptfokus der gesammelten Daten liegt darauf, Rückschlüsse auf die Verbreitung von ZigBee 3.0 Netzwerken und deren verwendeten Sicherheitsniveau schließen zu können.

- Prozentanteil an ZigBee 3.0 Netzwerken im Vergleich zu älteren Zigbee Versionen
- Geografische Aufteilung von ZigBee 3.0 Netzwerken
- Aufteilung von ZigBee 3.0 Netzwerken im Bezug auf Wohn- und Industriegebiete
- Häufigkeit von ZigBee Geräten nach Hersteller
- Häufigkeit von ZigBee Geräten nach Gerätetyp
- Implementierte Sicherheitsmaßnahmen der Netzwerke und Geräte

6.1.1. Anteil ZigBee 3.0 Geräte

Die Information ob es sich bei dem gefundenen Gerät um ein ZigBee 3.0 Gerät handelt, befindet sich im Network Header des ZigBee Frames. Im Network Header muss bei jeder Übertragung das Sub-Feld „Protocol Version“ in der Frame Control Feld gesetzt werden.

Wie in Tabelle 6.1 entnommen werden kann, gibt es drei unterschieliche Protokollversionen, welche im Network-Header spezifiziert werden können. ZigBee 2006 und ZigBee Pro teilen sich hierbei den selben Identifikator 0x02, wodurch ZigBee 3.0 Frames nicht eindeutig identifiziert werden können. Es handelt

Spezifikation	Protokollversion
ZigBee Green Power	0x03
ZigBee Pro ZigBee 2006	0x02
ZigBee 2004	0x01

Tabelle 6.1.: ZigBee Protokollversionen

sich nur dann um einen ZigBee 3.0 Frame, wenn der Frame nach der ZigBee Pro 2015 (Revision 21) Spezifikation formattiert ist. Der Grund, weshalb sich ZigBee Pro und ZigBee 2006 einen Identifikator bei der Protokollversion teilen ist, dass die beiden Protokollversionen miteinander kompatibel sind. Da der Aufbau von Frames bei ZigBee Pro und ZigBee 2006 gleich ist, macht es für ein Gerät keinen Unterschied, welcher der beiden Protokollversionen verwendet wurde um den Frame zu generieren.

Auf Basis der Protokollversion kann somit nur zwischen ZigBee Green Power, ZigBee Pro beziehungsweise ZigBee 2006 und ZigBee 2004 unterschieden werden. [3, S. 7]

6.1.2. Geographische Aufteilung

Zu den gefundenen Netzwerken werden zusätzlich GPS-Daten gespeichert. Diese sollen im weiteren Verlauf Aufschluss darüber bieten, wie ZigBee Netzwerke geografisch verteilt sind. Die gesammelten Daten werden hierbei um Längengrad und Breitengrad der momentanen Position angereichert.

Die Aufteilung in Industrie und Wohngebiete muss manuell geschehen. Um relevante Daten sammeln zu können, muss bei der Wahl der Route darauf geachtet werden, dass eine gleiche Aufteilung zwischen Wohn- und Industriegebieten vorliegt.

6.1.3. Geräte nach Hersteller

Hersteller von Geräten können mit Hilfe der Source IEEE Adresse im Network Header oder via der Source Adresse im Auxiliary Header identifiziert werden. Wenn ein Gerät beispielsweise die Source IEEE Adresse „00:17:88:01:01:c0:61:33“ hat, handelt es sich bei den ersten sechs Stellen um den Präfix des Herstellers des Gerätes. In diesem Fall wäre dies „00:17:88“ und etspricht „Philips Lighting BV“ [20].

Bei dem Präfix handelt es sich um einen sogenannten „Oranizationally Unique Identifier“. Hersteller

können von der IEEE Standards Association [21] einen solchen OUI erwerben, welcher bei der Verwendung von IEEE Adressen als Präfix angehängt wird.

6.1.4. Geräte nach Gerätetyp

Die Festlegung des Gerätetypen hat die Vorraussetzung, dass der Application Header im ZigBee Frame nicht verschlüsselt ist. Via dem „Profile Identifier“ Feld im Application Header kann das verwendete Applikationsprofil ausgelesen werden, was einen Rückschluss auf den ungefähren Gerätetypen zulässt. Die Problematik hierbei ist, dass Geräte mehrere Applikationsprofile verwenden können. Beispielsweise eine Glühbirne kann entweder unter dem ZigBee Light Link Profil oder dem Home Automation Profil betrieben werden. Wird ein Gerät unter ZigBee Light Link betrieben, kann zumindest darauf zurückgeschlossen werden, dass es sich hierbei um ein Gerät handelt, dass in irgendeiner Art und Weise mit Beleuchtung zusammenhängt. Beim Home Automation Profil ist der Rückschluss auf einen Gerätetyp nicht mehr möglich, da hierbei die Variation von Geräten zu hoch ist.

Weiters kommt hinzu, dass Informationen wie der „Profile Identifier“ nur dann im Application Header angehängt werden, wenn das sogenannte „ACK Format“ Sub-Feld im Frame Control Feld des Application Headers auf einen Wert von 0x1 gesetzt ist. Detaillierte Informationen zum Aufbau des Application Header sind im Anhang D ersichtlich.

6.1.5. Implementierte Sicherheitsmaßnahmen

Informationen über die Sicherheit von ZigBee Netzwerken werden aus dem Auxiliary Header der ZigBee Kommunikation entnommen. Wie in Kapitel 3.14 beschrieben wurde, können aus dem Auxiliary Header Informationen wie das Security Level, verwendete Sicherheitsschlüssel und Frame Counter entnommen werden. Für die Auswertung der allgemein verwendeten Sicherheitsfunktionen von ZigBee 3.0 Netzwerken, ist aus dem Auxiliary Header vorwiegend der verwendete Sicherheitsschlüssel und das Security Level relevant.

6.2. Testgeräte

Nachfolgend werden die Testgeräte beschrieben, welche für die Entwicklung des Scanners verwendet werden. Um zu gewährleisten, dass die verwendeten Geräte tatsächlich ZigBee 3.0 zur Kommunikation verwenden, werden ZigBee 3.0 zertifizierte Geräte verwendet. Bei ZigBee 3.0 zertifizierten Geräten ist gewährleistet, dass alle Vorgaben und Voraussetzungen der ZigBee Pro (Revision 21) Spezifikation kor-

Produkt	Anzahl
Glühbirne	53
Dimmer Controller / Lichtschalter	24
Steckdose	4
Gateway / Hub / Coordinator	6
Rauchmelder	1
Carbon Monoxid Detector	1
Thermostat	2
Thermometer	2
Schalousie Controller	3
Range Extender	1

Tabelle 6.2.: ZigBee 3.0 zertifizierte Produkte

rekt implementiert wurden.

6.2.1. ZigBee 3.0 zertifizierte Produkte

Um für die Entwicklung eines Warwalking-Tools genügend Testdaten zu erhalten, werden für den Testaufbau mehrere Geräte benötigt um ein funktionierendes ZigBee Netzwerk abbilden zu können. Im Idealfall beinhaltet das Netzwerk:

- Einen Coordinator beziehungsweise Trust Center
- Einen Gerät mit Routing-Funktionalität
- Ein oder mehr Endgeräte

Da vor allem die sicherheitstechnische Implementierung der Geräte relevant ist, werden bei der Auswahl von Testgeräten, Geräte bei denen ein hohes Sicherheitsniveau kritisch ist, bevorzugt ausgewählt. Zu diesen Geräten zählen beispielsweise Alarmanlagen und Türschlösser.

Zum Zeitpunkt der Evaluierung von geeigneten Testgeräten, waren 97 Geräte auf der ZigBee Alliance Hompage gelistet [22]. In Tabelle 6.2 ist eine Auflistung der zum Zeitpunkt der Evaluierung ZigBee 3.0 zertifizierten Geräte ersichtlich. Das Problem hierbei ist, dass viele der gelisteten Geräte noch nicht ver-

fügbar, beziehungsweise noch nicht im Handel erhältlich sind.

Bei der angeführten Liste ist anzumerken, dass es sich hierbei um zertifizierte ZigBee 3.0 Geräte handelt. Viele Hersteller von Geräten geben an, ZigBee 3.0 konform zu sein. Das bedeutet, dass es neben zertifizierten ZigBee 3.0 konformen Geräten auch nicht zertifizierte ZigBee 3.0 Geräte gibt. Da diese Konformität jedoch nicht durch eine Zertifizierung bestätigt wurde, werden dennoch zertifizierte Geräte für den Testaufbau verwendet.

6.2.2. Auswahl der Testgeräte

Von den sechs gelisteten Gateways, ist im Moment nur eines Verfügbar und dieses wird nicht an Privatpersonen verkauft. Die einzigen Geräte, welche im Handel erhältlich sind, sind Glühbirnen und Dimmer Controller beziehungsweise Lichtschalter. Diese werden meist im Rahmen von herstellerspezifischen Ökosystemen angeboten. Das bedeutet, dass Glübirnen und Dimmer Controller beziehungsweise Lichtschalter in Kombination mit unterstützen Gateway, meist vom selben Hersteller, eingesetzt werden müssen.

Die Auswahl der Testgeräte ist schlussendlich auf das „Philips Hue Ambiance Starter Set“ gefallen. Philips Hue ist eine der am weitest verbreitetsten Lösungen für Beleuchtung. Darüber hinaus sind die inkludierten Glühbirnen „Philips Hue White Ambiance“ ZigBee 3.0 zertifizert. Im Set ist ein Gateway bezeihungsweise ein Coordinator, die „Philips Hue Bridge“, enthalten. Die Philips Hue Bridge ist nicht ZigBee 3.0 zertifiziert, hat jedoch ein Update für ZigBee 3.0 erhalten. [23] Weiters ist ein Lichtschalter beziehungsweise Dimmer Controller inkludiert, über welchen die Glühbirnen gesteuert werden können. Die Philips Hue Bridge kümmert sich um die Verwaltung des ZigBee Netzwerkes und die Konfiguration der Glübirnen und des Dimmer Controllers.

6.3. Geographisches Gebiet der Datensammlung

Bei der Sammlung von Echtdaten wird darauf geachtet, dass sowohl Daten aus Industire- als auch aus Wohngebieten gesammelt werden. Auf diese Art kann evaluiert werden, in welchen Gebieten ZigBee 3.0 eher zum Einsatz kommt. Die Datensammlung findet in Wien statt. Folgende Gebiete wurden für die Datensammlung ausgewählt:

- Mariahilfer Straße
- Kärntner Straße sowie Innere Stadt

- Wohngebiet abseits der Mariahilfer Straße

Die Gebiete Mariahilfer Straße und Kärntner Straße sollen Daten für Industriegebiete liefern. Diese Gegenden bieteten sich durch die dichte Verteilung von Geschäften an. Die beiden Straßen werden im Zuge der Datensammlung mindestens drei Mal komplett abgegangen.

Wohngebiete abseits der Mariahilfer Straße und die Innere Stadt Wien sollen Daten über die Verbreitung in Wohngebieten liefern. Hierbei kann keine fixe Route festgelegt werden, da es keine Garantie dafür gibt, in den gewählten Gebieten ZigBee Geräte zu finden. Daher werden diese Gegenden so flächendeckend wie möglich abgegangen.

7. ZigBee 3.0 Scanner - Hardware

Auf dem Markt sind mehrere Geräte verfügbar, welche in der Lage sind nach ZigBee Netzwerken zu suchen und die Kommunikation mitzulesen. Im Zuge der Evaluierung von geeigneten Geräten die für Warwalking eingesetzt werden können, wurden folgende Lösungen getestet:

- HackRF One von Great Scott Gadgets [24]
- CC2531 USB Dongle von Texas Instruments [25]

Nachfolgend werden die Vor- und Nachteile der einzelnen Lösungen beschrieben. Die Evaluierung der Geräte wurde im Betriebssystem Ubuntu 18.04 LTS [26] und anhand folgender Kriterien durchgeführt:

- Komplexität der Inbetriebnahme
- Leistungsfähigkeit der Antenne
- Funktionsumfang
- Eignung für Warwalking

Ubuntu 18.04 LTS wurde als Betriebssystem für Evaluierung gewählt, da Ubuntu zum einen eines der meist verwendedsten Distributionen ist und zum anderen, da es sich bei der Version 18.04 LTS um die aktuellste „Long Time Support“ Version handelt. [27] Um zu gewährleisten, dass das Vorgehen bei der Installation der Geräte konsistent ist, wurde die Testumgebung vor jeder Installation und Inbetriebnahme der einzelnen Geräte zurückgesetzt. Daher werden neben spezifischen Abhängigkeiten der Geräte auch allgemeine Abhängigkeiten für verwendete Programme und Module angeführt.

7.1. HackRF One

Beim HackRF One handelt es sich um ein Software Defined Radio (SDR) Periferiegerät, welches Signale in einer Spanne von einem bis sechs GHz senden und empfangen kann. Das Senden und Empfangen von Signalen ist hierbei nicht gleichzeitig möglich. SDR bedeutet, dass die Signalverarbeitung nicht in

Hardware, beispielsweise durch vorgefertigte Chips, sondern in Software umgesetzt wird.

Die in der Evaluierung verwendete Software zu Verarbeitung der empfangenen Signale ist GNURadio [28]. GNURadio bietet eine graphische Benutzeroberläche, in welcher Module oder Blöcke im Baukastenprinzip zu einem Flussdiagramm zusammengeschlossen werden können, um Signale zu verarbeiten.

7.1.1. Abhängigkeiten und verwendete GNURadio Module

Der HackRF One an sich kann direkt ohne Konfiguration in Betrieb genommen werden. Um jedoch ZigBee Kommunikation mittels GNURadio sniffen zu können, muss die Demodulation des Funksignales in Software umgesetzt werden. Hierzu müssen Module installiert werden, damit der HackRF One mit GNURadio verwendet werden kann. Für die Demodulation der ZigBee Funkkommunikation wurde der IEEE 802.15.4 ZigBee Transceiver von Bastibl verwendet. [29] Der IEEE 802.15.4 ZigBee Transceiver wurde auf Basis von Thomas Schmid's Implementierung eines GNURadio 802.15.4 En- und Decoders entwickelt.[30] Der Grund, weshalb der ZigBee Transceiver von Bastibl verwendet wurde ist, da dieser die Funktionalität des GNURadio 802.15.4 En- und Decoders von Thomas Schmid beinhaltet und diesen um die Interpretation von ZigBee Kommunikation erweitert.

7.1.2. Installation und Einrichtung

Zur Installation von GNURadio und des IEEE 802.15.4 ZigBee Transceivers wurde PyBOMBS verwendet. [31] PyBOMBS ist der offizielle Installer von GNURadio, über welchen ebenfalls diverse GNURadio Erweiterungen installiert werden können.

Da unter Ubuntu 18.04 ein paar Konfiguration nachjustiert werden müssen, um die erfolrderlichen Programme und Module verwenden zu können, wird nachfolgend die Einrichtung von GNURadio im Detail beschrieben. Zunächst muss python-pip installiert werden, was im weiteren Verlauf für die Installation von PyBOMBS verwendet wird. Um die Installation zu beschleunigen wird empfohlen, ebenfalls python-apt zu installieren. Da es sich um eine neue Ubuntu 18.04 Installation handelt, muss ebenfalls libssl1.0-dev und libvolk1-dev nachinstalliert werden.

```
sudo apt install python-pip python-apt libssl1.0-dev libvolk1-dev
sudo pip install git+https://github.com/gnuradio/pybombs.git
pybombs auto-config
pybombs recipes add-defaults
```

Nun muss PyBOMBS für die Verwendung der libssl Version 1.0 konfiguriert werden, da sonst die Installation von Apache Thrift fehlschlägt. Apache Thrift wird im Zuge der Installation von GNURadio als Abhängigkeit automatisch mitinstalliert.

```
vim ~/.pybombs/recipes/gr-recipes/ssl.lwr
# Zeile "deb:" anpassen:
deb:libssl1.0-dev
```

Nun können GNURadio und GNURadio-Blöcke für HackRF (gr-osmosdr) und zur 802.15.4 Demodulierung (gr-ieee-802154) installiert werden.

```
# GNURadio Installation
pybombs prefix init ~/env/gnuradio -a gnuradio -R gnuradio-default
source ~/prefix/gnuradio/setup_env.sh
# HackRF und 802.15.4 Bloecke
sudo pybombs install gr-osmosdr
sudo pybombs install gr-ieee-802154
sudo ldconfig
```

Nun muss noch eine udev Regel installiert werden, in der Benutzern in der Gruppe „sudo“ der Zugriff auf den HackRF erlaubt wird.

```
sudo vim /etc/udev/rules.d/52-hackrf.rules
# Folgende Zeile hinzufuegen:
ATTR{idVendor}=="1d50", ATTR{idProduct}=="6089", SYMLINK+="hackrf-one
   ↪ -%k", MODE="660", GROUP="sudo"
```

Jetzt kann GNURadio mit den notwendigen Blöcken für HackRF und zur 802.15.4 Demodulation gestartet werden.

```
source ~/env/gnuradio/setup_env.sh
gnuradio-companion
```

War die Installation erfolgreich können ZigBee Signale mit Hilfe der installierten Blöcke „IEEE802.15.4 OQPSK PHY“ und „IEEE802.15.4 MAC“ wie in Abbildung 7.1 ersichtlich demoduliert werden.
Via dem „Wireshark Connector“ Block kann das Signal in ein pcap umgewandelt werden. Dadurch lässt sich die aufgezeichnete Kommunikation in Wireshark analysieren.

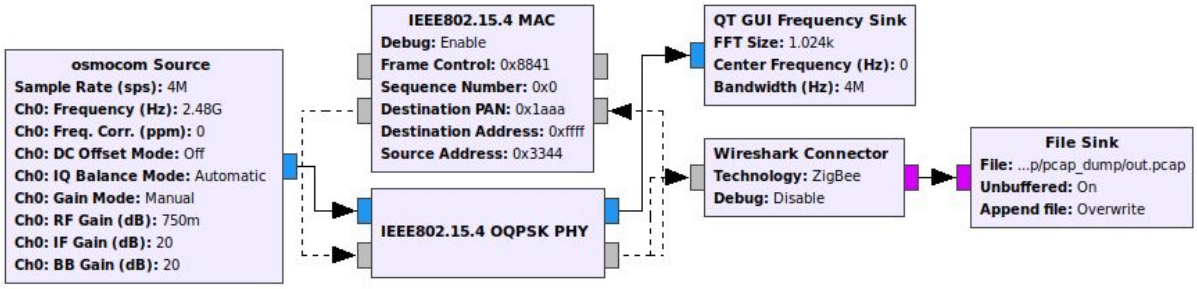

Abbildung 7.1.: GNURadio Flussdiagramm

7.1.3. Funktionsumfang

Da es sich bei dem HackRF One um ein SDR handelt, kann mit diesem so gut wie jede Funktionalität erreicht werden. Die Einstiegshürde zum Programmieren von SDRs ist jedoch relativ hoch und es erfordert tiefgehendes Vorwissen über die Art von Funkkommunikation, welche mittels einem SDR analysiert werden soll. Das bedeutet, um zum Beispiel ZigBee Kommunikation mittels SDR zu analysieren, benötigt man nicht nur Wissen über den Aufbau des Funkprotokolles, sonder auch Wissen darüber, wie IEEE 802.15.4 Funksignale moduliert beziehungsweise demoduliert werden.

7.1.4. Eignung für Warwalking

Der HackRF One bringt im Bezug auf Warwalking ein Problem mit sich. Der HackRF One ist relativ sperrig, was kein Problem darstellt, solange man nur einen HackRF benötigt. Da ZigBee Kommunikation jedoch im 2.4 GHz Frequenzbereich abläuft, stehen 16 Kanäle zur Kommunikation zur Verfügung. Ein HackRF One kann nur auf einem der Kanäle gleichzeitig scannen. Das bedeutet, dass um so wenig Kommunikation wie möglich zu verpassen, vier HackRF One optimal wären. Drei HackRF One für die Hauptkanäle 15, 20, 25 und 26, wobei ein HackRF One die beiden Kanäle 25 und 26 übernimmt, sowie einen HackRF One für die restlichen Channel. [32] Diese Anzahl an HackRF One ist für Warwalking nicht mehr geeignet.

7.2. CC2531

Bei dem CC2531 USB Dongle handelt es sich um ein ZigBee Evaluationsmodul von Texas Instruments.[25] Dieser USB Stick ist für den Einsatz unter dem Betriebssystem Windows mit der von Texas Instruments bereitgestellten „PACKET-SNIFFER“ Software gedacht. Der CC2531 ist ein sogenanntes System-on-Chip (SoC), was bedeutet, dass die Demodulation von ZigBee Kommunikation bereits auf dem USB Stick geschieht.

Um den CC2531 USB Dongle unter Linux verwenden zu können, wurde auf ein Projekt namens „802.15.4 monitor“ von mitshell zurückgegriffen. [33]. Dieses Projekt bietet ein Python Modul, mit welchen ohne Firmwareupdates auf den CC2531 USB Dongle zugegriffen werden kann. Standardmäßig liefert dieses Modul nur Daten aus dem MAC Layer, daher wurde im Rahmen der Programmierung des ZigBee 3.0 Scanners das Projekt um die Interpretation der restlichen Kommunikation erweitert. Dadurch sollen auch Daten aus dem Network Layer und Application Layer interpretiert werden können.

Der Grund, weshalb der CC2531 Dongle nicht unter Windows eingesetzt wird ist, dass die PACKET-SNIFFER Software von Texas Instruments kein Channel Hopping unterstützt und somit die Channel händisch durchgegangen werden müssen, bis ZigBee Kommunikation gefunden wird.

7.2.1. Abhängigkeiten

Der CC2531 USB Dongle kann in der Standardkonfiguration verwendet werden. Um diesen jedoch unter Linux einsetzen zu können, muss zusätzliche Software installiert werden, welche den Zugriff auf die vom CC2531 Dongle gesammelten Daten zulässt. Zum einen wird libusb-1.0.0-dev und python-libusb1 benötigt um auf die USB Schnittstelle zum CC2531 Dongle zugreifen zu können. Für das Management des CC2531 Dongles unter Linux wird die „libmich library“ verwendet.

7.2.2. Installation

Die Installation der Abhängigkeiten ist relativ einfach, es muss jedoch darauf geachtet werden, dass Python 2 verwendet wird, da die libmich Bibliothek in Python 2 geschrieben wurde.

```
# Zugriff auf USB
sudo apt-get install libusb-1.0-0-dev
pip install libusb1
# Installation der libmich Bibliothek
git clone https://github.com/mitshell/libmich.git
cd libmich
python setup.py install
```

Sind die Abhängigkeiten installiert, kann auf den CC2531 Dongle via Python zugegriffen werden. Der Nachteil des CC2531 Dongles ist jedoch, dass es keine Möglichkeit gibt eine stärkere Antenne anzubringen. Weiters muss die Interpretation der ZigBee Frames eigens programmiert werden.

Um via Python den CC2531 Dongle zu steuern, muss lediglich das CC2531.py File vom „802.15.4 monitor“ als Modul importiert werden.

7.2.3. Funktionsumfang

Da es sich bei dem CC2531 USB Dongle um ein ZigBee Evaluationsmodul handelt, kann mit der Standard-Firmware auch nur ZigBee Kommunikation mitgelauscht werden. Der Vorteil ist, dass bei den empfangen Paketen nicht manuell geprüft werden muss, ob es sich um ein valides oder fehlerhaftes Paket handelt, da diese Aufgaben vom CC2531 Dongle selbst übernommen wird.

7.2.4. Eignung für Warwalking

Durch das kompakte Profil des CC2531 USB-Dongles, können ohne Probleme mehrere beim Warwalking gleichzeitig verwendet werden. Der größte Nachteil dieser Lösung ist, dass es keine Möglichkeit gibt eine stärkere Antenne an die jeweiligen CC2531 Dongles anzuschließen. Bei dem Test der Reichweite wurde festgestellt, dass bei einem freien Sichtfeld Signale auf 20 bis 30 Meter Entfernung empfangen werden konnten. In Gebäuden ist die Reichweite auf 10 bis 15 Meter limitiert. Signale konnten jedoch durch bis zu drei 30 cm dicke Betonwände hindurch empfangen werden.

7.3. GPS Modul

Zur Sammlung von GPS-Daten wird ein GPS/GLONASS U-blox 7 USB-Stick verwendet, über welchen Positionsdaten gewonnen werden können. Bei diesem USB-Stick handelt es sich um ein generisches GPS-Modul, welches für die Entwicklung des ZigBee Scanners via dem sogenannten „pySerial“ Modul angesprochen werden kann. Zu der aufgezeichneten Kommunikation werden Längengrade (Longitude) und Breitengrade (Latitude) gespeichert. Damit kann zu einem späteren Zeitpunkt ermittelt werden, wo die Kommunikation aufgezeichnet wurde. Weiters kann mit Hilfe der Positionsdaten ermittelt werden, ob sich die Geräte in einem Industriegebiet oder einem Wohngebiet befinden.

Um das GPS Modul via Python verwenden zu können, muss das „pySerial“ Modul installiert werden. Dieses erlaubt den Zugriff auf serielle Schnittstellen.

```
# Zugriff auf serielle Schnittstelle via Python
pip install pyserial
```

Der GPS Dongle registriert sich unter dem Pfad „/dev/ttyACM0“ am System, über welchen auf das Gerät via Python zugegriffen werden kann.

8. ZigBee 3.0 Scanner - Entwicklung

Zur Aufzeichnung von ZigBee Kommunikation werden vier CC2531 Dongles verwendet. Die Verarbeitung der Daten, sowie das Management der CC2531 Dongles geschieht in Python unter Verwendung des CC2531 Moduls des „802.15.4 monitor“ Projektes [33]. Da zur Verarbeitung der Daten ZigBee Frames interpretiert werden müssen, werden nachfolgend die relevanten Felder aus den unterschiedlichen Schichten des ZigBee Stacks und deren Zusammenhang mit der Auswertung der Daten beleuchtet.

8.1. Relevante Felder des ZigBee Frames

Daten, welche im Zuge der Ermittlung der Verbreitung von ZigBee 3.0 Geräten gesammelt werden sollen, können aus de MAC, Network und Application Layer eines ZigBee Frames entnommen werden. Nachfolgend wird erläutert, welche Felder der unterschiedlichen Header relevant sind. Eine Zusammenfassung der Informationen aus den einzelnen Leyern des ZigBee Stacks ist in Tabelle 8.1 ersichtlich.

8.1.1. Generelle Informationen

Die aufgezeichneten Frames werden im Zuge der Datensammlung mit einem Timestamp und Positionsdaten angereichert. Durch den Timestamp kann zu einem späteren Zeitpunkt festgestellt werden, wann ein Frame aufgezeichnet wurde. Die Positionsdaten werden dazu genutzt um festzustellen, wo die Geräte gefunden wurden. Weiters werden diese Daten zur Aufteilung der gefundenen Geräte in Industrie- und Wohngebiete genutzt. Positionsdaten können außerdem zur Unterscheidung von unterschiedlichen ZigBee Netzwerken herangezogen werden. Mit einer Kombination aus Positionsdaten, Source PAN ID und Source Addresse können Geräte eindeutig identifiziert und einem Netzwerk zugewiesen werden.

MAC Header Daten

Aus dem MAC Header werden all jene Daten entnommen, um einen ZigBee Frame zu einem Gerät zuordnen zu können. Zu den relevanten Feldern gehören „Destination PAN ID“, „Source PAN ID“, „Destination Address“ und „Source Address“.

Layer	Field name
General Information	Time
	Position Longitude
	Position Latitude
	Vendor
MAC	Destination PAN ID
	Source PAN ID
	Destination Address
	Source Address
NWK	Protocol Version
	Source IEEE Address
	Security Flag
APL	Frame Type
	Security Flag
AUX	Key Identifier
	Security Level
	Source Address

Tabelle 8.1.: Relevante Felder der unterschiedlichen Layer

Die Source PAN ID kann in Kombination mit der Source Addresse und den Positionsdaten zur eindeutigen Identifizierung von Geräten genutzt werden. Die Destination PAN ID ist ein Indikator dafür, dass sich weitere Netzwerke in Reichweite befinden. Die Destination Addresse kann, falls keine Frames von diesen Geräten gesendet werden, zur Auflistung der im Netzwerk befindlichen Geräten genutzt werden.

8.1.2. NWK Header Daten

Durch den Network Header kann die genutzte Protokollversion festgestellt werden. Wie in Kapitel 6.1.1 bereits erwähnt wurde, kann via diesem Feld nicht zwischen ZigBee 3.0 und ZigBee Versionen ab 2006 unterschieden werden. Dies liegt daran, dass sich alle Protokollversionen ab 2006 den gleichen Identifikator teilen.

Weiters können aus dem Network Header die IEEE Short und Long Adressen gewonnen werden. Bei der Destination und Source Short Adress handelt es sich um eine 16 Bit Adresse, welche gleich der Source und Destination Adress aus dem MAC Header sind. Die IEEE Long Adressen haben eine länge von 64

Bit und beinhalten als Präfix den sogenannten Organizational Unique Identifier (OUI). Ist eine der beiden IEEE Long Adressen gesetzt, kann somit auf den Hersteller des Gerätes zurückgeschlossen werden. Durch die Destination Addressen kann festgestellt werden, ob Daten, welche via Broadcast oder Unicast versendet werden, anders geschützt werden.

Durch das Security Flag im Network Header kann herausgefunden werden, ob der Frame im Network Layer verschlüsselt wurde. Ist das Security Flag auf diesem Layer gesetzt wird ein Auxiliary Header angehängt und es können weitere Daten aus diesem entnommen werden. Daten aus dem Auxiliary Header werden im Punkt 8.1.4 beschrieben.

8.1.3. APL Header Daten

Aus dem Application Layer kann wie auch beim Network Header entnommen werden, ob Frames von diesem Layer verschlüsselt wurde. Ist dies der Fall, wird das Security Flag gesetzt. Aus dem angehängten Auxiliary Header können anschließend Informationen über den implementierten Sicherheitslevel gewonnen werden.

Weiters können aus dem Application Layer Informationen über den Typen des Frames (Data, Command, Acknowlegde oder Inter-PAN APS) entnommen werden um zu evaluieren, ob der Typ des Frames Auswirkungen auf das Sicherheitsniveau hat.

Die Porblematik hierbei ist, dass auch wenn eine Nachricht aus dem Application Layer aus versendet wird, diese zusätzlich auf dem Network Layer verschlüsselt ist. Dadurch können Daten aus dem Application Layer nur dann gelesen werden, wenn die Nachricht entschlüsselt werden kann, was außerhalb des Scopes dier Diplomarbeit ist.

8.1.4. AUX Header Daten

Der Auxiliary Header liefert Daten über das Sicherheitsniveau des Frames. Relevante Informationen aus dem Auxiliary Header sind der Key Identifier, Security Level und Source Address.

Der Key Identifier gibt Aufschluss darüber, welcher Sicherheitsschlüssel für den Schutz des Frames eingesetzt wird. Die zur Verfügung stehenden Schlüssel sind der Network Key, Data Key, Key-Transport Key und Key-Load Key. Spezifika zu den einzelnen Schlüsseln sind im Kapitel 3.4 beziehungsweise Kapitel 3.5 ersichtlich.

Bei der Source Addresse im Auxiliary Header handelt es sich um die IEEE Source Adresse des Gerätes, welche den Frame schützt. Diese Adresse kann zur Ermittlung des Herstellers eines Gerätes herangezogen werden, sollte die IEEE Adresse im Network Header nicht mitgesendet werden.

8.2. Scanner - Features und verwendete Projekte

In diesem Kapitel wird der Entwicklungsprozess des ZigBee 3.0 Scanners beschrieben. Es werden Details zu Entwicklungsentscheidungen, Problemen sowie Abhängigkeiten zu anderen Projekten beleuchtet, welche zur Entwicklung des Scanners verwendet wurden.

8.2.1. Verwendete Hardware, Projekte und Abhängigkeiten

In Kapitel 7.2 wurde beschrieben, wie mittels dem dem „802.15.4 monitor“ von mitshell 802.15.4 Kommunikation mit CC2531 USB Dongles mitgelesen werden kann. Dieses Projekt wurde als Grundlage für die Entwicklung des ZigBee Scanners herangezogen und um einen Parser für den ZigBee Network und Applikation Layer erweitert. Da die vom „802.15.4 monitor“ verwendet „libmich“ Bibliothek in Python 2 entwickelt wurde, musste auch der ZigBee Scanner in Python 2 geschrieben werden. Neben den in Kapitel 7.2.2 beschriebenen Abhängigkeiten, sind keine weiteren für die Entwicklung des ZigBee Scanners hinzugekommen.

8.2.2. Network, Application und Auxiliary Interpreter

Der „802.15.4 monitor“liefert eine hexadezimale Repräsentation der aufgezeichneten ZigBee Frames. Die Interpretation der ZigBee Kommunikation wurde nach den Formaten wie sie in den Anhängen B, C, D und Kapitel 3.14 beschrieben wurden vorgenommen.

Die Daten werden nicht direkt nach der Aufzeichnung interpretiert, sondern im Nachhinein. Gesammelte Daten werden zunächst in hexadezimaler Repräsentation mit Positionsdaten und dem Zeitpunkt der Aufzeichnung abgespeichert. Die Interpretation der Daten geschieht im Nachhinein über ein seperat entwickeltes „Interpreter“ Programm.

Dieses Vorgehen hat den Vorteil, dass ZigBee Frames als Rohdaten vorliegen und wenn notwendig, zu einem späteren Zeitpunkt Anpassungen am Interpreter vorgenommen werden können. Das bedeutet, dass der ZigBee Scanner aus zwei Teilen besteht. Zum einen der „Sniffer“, welcher sich lediglich um die

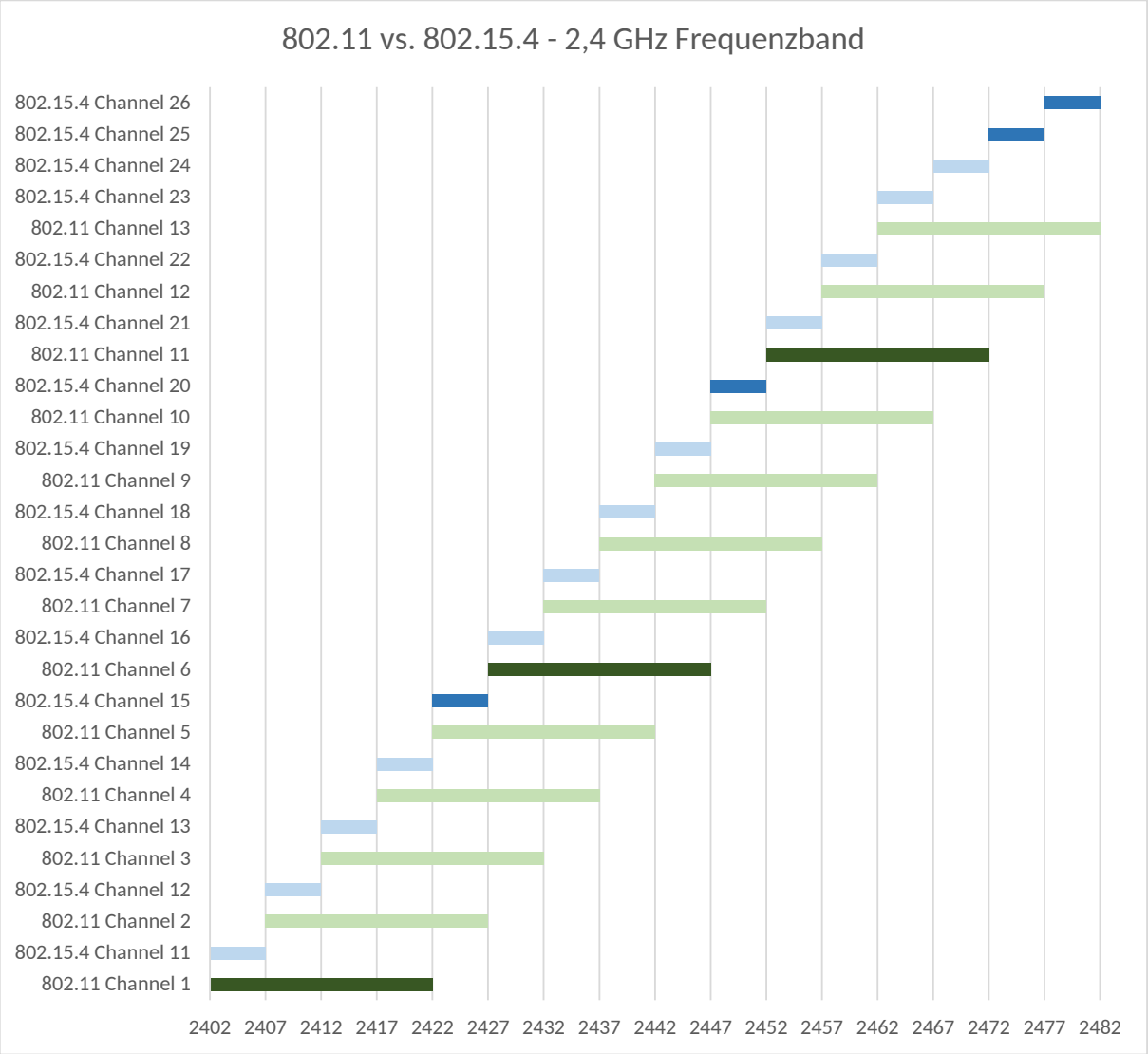

Abbildung 8.1.: 802.11 vs. 802.15.4 - 2,4 GHz Frequenzband

Aufzeichnung von Daten kümmert und den „Interpreter“, welcher die Daten interpretiert. Der Interpreter wertet jene Daten aus, welche im Kapitel 8.1 definiert wurden.

8.2.3. Auzeichnung von ZigBee Kommunikation

Um während des Warwalking so wenig Kommunikation wie möglich zu verpassen, müssen mindestens die vier Hauptchannel 15, 20, 25 und 26 gleichzeitig aufgezeichnet werden. In Abbildung 8.1 ist die Aufteilung des 2,4 GHz Frequenzbandes im 802.11 [34] und 802.15.4 Standard ersichtlich. Daraus ist erkennbar, dass sich diese Channel zwischen den Hauptchannel des 802.11 2,4 GHz Frequenzbandes befinden. Da sich 802.15.4 und 802.11 einen Frequenzbereich Teilen, sind die Hauptchannel von ZigBee Geräten die Channel 15, 11, 25 und 26. Dies dient dazu Störungen bei der Funkkommunikation zu ver-

meiden.

Für die Sammlung von Daten wurde somit festgelegt, dass vier CC2531 Dongles optimal sind. Für Channel 15, 20 und 25-26 ist jeweils ein CC2531 zugewiesen. Ein weiterer CC2531 Dongle scannt die restlichen Channel. Auf diese Weise sind zu jeder Zeit alle Hauptchannel abgedeckt, wobei die restlichen Channel (im weiteren Verlauf Nebenchannel genannt) durch den vierten CC2531 Dongle abgedeckt werden. Die Nebenchannel, sowie die beiden Channel 25 und 26 werden alle 1,5 Sekunden gewechsel. Grund hierfür ist, dass der CC2531 Dongle ungefähr 0,5 Sekunden benötigt, um den Channel zu wechseln und die Datensammlung wieder aufzunehmen.

8.2.4. Positionsdaten

Positionsdaten werden via einem GPS/GLONASS U-blox 7 USB-Stick ermittelt. Dieser USB-Stick liefert die Daten im sogennanten „NMEA“ Format. Hierbei werden die „$GPRMC“ Informationen verwendet. Beim $GPRMC handelt es sich um das empfohlene Minimum bei GPS/Transit Daten („Recommended minimum specific GPS/Transit data“). [35]

$GPRMC Daten sind folgendermaßen aufgebaut:

$GPRMC,225446,A,4916.45,N,12311.12,W,000.5,054.7,191194,020.3,E*68

- 225446 - Time of fix 22:54:46 UTC
- A - Navigation receiver warning A = OK, V = warning
- 4916.45,N - Latitude 49 deg. 16.45 min North
- 12311.12,W - Longitude 123 deg. 11.12 min West
- 000.5 - Speed over ground, Knots
- 054.7 - Course Made Good, True
- 191194 - Date of fix 19 November 1994
- 020.3,E - Magnetic variation 20.3 deg East
- *68 - mandatory checksum

Via der „Latitude“ und „Longitude“ kann die Position festgestellt werden, an der ein Netzwerk gefunden wurde. Um die Positionsdaten einfacher auswerten zu können, werden diese in Dezimalgrade umgerechnet. Beispielsweise kann die NMEA Latitude 4916,45,N (49 deg. 16,45 min North) folgendermaßen umgerechnet werden: 49 deg. + 16,45 min / 60. Dies ergibt 49 + 0,274166667 sec und somit 49,274167 Dezimalgrade. [36]

9. Auswertung der gesammelten Daten

In diesem Kapitel werden die gesammelten Informationen ausgewertet. Wie in Kapitel 6.1 beschrieben wurde, bezieht sich die Auswertung auf:

- Prozentanteil an ZigBee 3.0 Netzwerken im Vergleich zu älteren Zigbee Versionen
- Geografische Aufteilung von ZigBee 3.0 Netzwerken
- Aufteilung von ZigBee 3.0 Netzwerken im Bezug auf Wohn- und Industriegebiete
- Häufigkeit von ZigBee Geräten nach Hersteller
- Häufigkeit von ZigBee Geräten nach Gerätetyp
- Implementierte Sicherheitsmaßnahmen der Netzwerke und Geräte

Nachfolgend wird auf die einzelnen Punkte eingegangen und die Ergebnisse präsentiert, welche sich für diese ergeben haben.

9.1. Geografische Aufteilung

Die Sammlung der Daten hat an folgenden Orten stattgefunden:

- Baden bei Wien, Fußgängerzone Wassergasse / Neustiftgasse
- Vösendorf, Shopping City Süd
- Wien, Kärntnerstraße
- Wien, Mariahilferstraße
- Wien, Stadioncenter
- Wien, Wohngebiet abseits der Mariahilferstraße
- Wien, Innere Stadt

Die Ergebnisse beziehen sich ausschließlich auf industrielle Gebiete, da in Wohngebieten keine ZigBee Kommunikation gefunden werden konnte. Die Sammlung von Daten in Wohngebieten wurde wie in Kapitel 6.3 in der Inneren Stadt Wien und den Wohngebieten abseits der Mariahilferstraße durchgeführt. Die Tatsache, dass keine ZigBee Kommunikation gefunden werden konnte, kann mehrere Gründe haben. Einerseits könnten die Verwendeten CC2531 Dongles zu schwache Antennen besitzen um auch ZigBee Geräte in Wohnungen ausfindig zu machen. Grundsätzlich ist in Wohngebieten die Distanz zu potentiellen ZigBee Installationen höher als in Industriegebieten, wie beispielsweise in einer Fußgängerzone, da an den meisten Geschäften näher vorbeigegangen werden kann als an Wohnungen. Dies liegt daran, dass die meisten Mehrfamilienhäuser nicht betreten werden können und so Funksignale aus dem zweiten oder dritten Stock nicht mehr stark genug sind, um vom CC2531 verarbeitet werden zu können. Andererseits kann es an einer niedrigen Durchdringung von ZigBee Geräten in privaten Haushalten in den ausgewählten Wohngebieten liegen.

9.2. Häufigkeit von Geräten nach Hersteller und Gerätetyp

Insgesamt wurden 116 ZigBee Netzwerke durch die passive Sammlung von ZigBee Kommunikation gefunden. Die Anzahl der Netzwerke wurde anhand der gefunden Source PAN IDs bestimmt. Da im Zuge der Datensammlung wenig Zeit an einem Ort verbracht wurde, sind in den meisten gefundenen Netzwerken durchschnittlich eines bis drei Geräte vorhanden.

In Abbildung 9.1 ist die Anzahl der aufgezeichneten ZigBee Nachrichten zu sehen. Die Nachrichten wurden in die einzelnen ZigBee Versionen 2004, 2006 und ZigBee Pro, sowie ZigBee Green Power aufgeteilt. Insegamt sind 2187 Nachrichten aufgezeichnet worden. 95,7% der ZigBee Kommunikation ist hierbei von ZigBee 2006 beziehungsweise ZigBee Pro Geräten ausgegangen. Dies war zu erwarten, da wie die Protokollversion ZigBee 2006 bereits vermuten lässt, die Geräte zum Zeitpunkt der Datensammlung bereits zwölf Jahre alt sein können. Dennoch wurden auch noch 88 Nachrichten aufgezeichnet, welche von ZigBee 2004 Geräten ausgingen. Letztlich wurden 6 Nachrichten von ZigBee Green Power Geräten aufgezeichnet. Die Aufzeichnung dieser Nachrichtung kann als „Glücksfall“ gewertet werden, da diese Geräte meist durch „Energy Harvesting“ funktionieren. Das bedeutet, dass Energie aus der Umgebung genutzt wird, beispielsweise kleine Solarzellen oder die Energie, die beim Druck einer Taste entsteht. Diese Geräte besitzen häufig keine Batterien oder sonstige Energiezufuhr, daher werden Nachrichten sehr selten oder nur dann gesendet, wenn das Gerät aktiv verwendet wird. Beispielsweise durch die Betätigung eines Lichtschalters. [37]

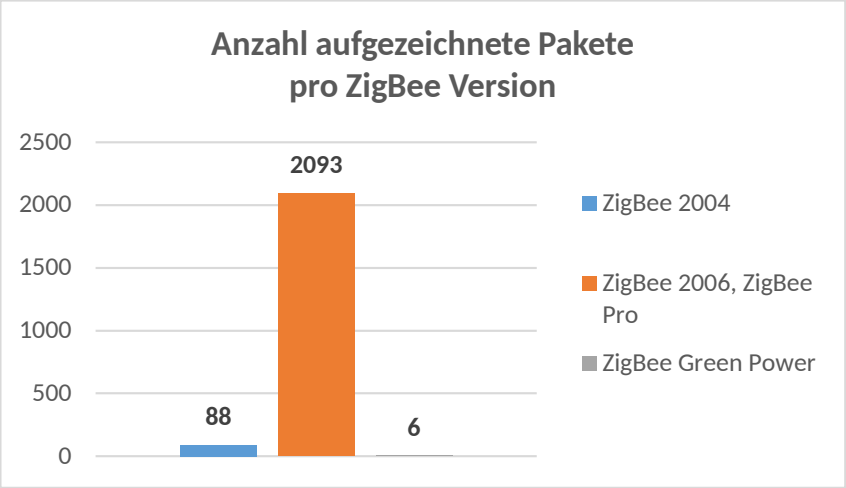

Abbildung 9.1.: Aufgezeichnete Pakrete pro ZigBee Version

9.3. Gefundene Geräte und Gerätetypen

Insgesamt konnten 147 eindeutige Geräte endeckt werden. 73 dieser Geräte, 49,7%, konnten Herstellern zugewiesen werden. Da aus den aufgezeichneten ZigBee Nachrichten nicht herausgefunden werden kann, um welche Art von Gerät es sich handelt, konnte nur eruiert werden, welche Arten von Geräten von den einzelnen Herstellern entwickelt werden.

In Abbildung 9.2 ist die Anzahl der gefundenen Geräte pro Hersteller zu sehen. Hierbei ist zu erkennen, dass Philips Beleuchtungssysteme mit 74,3% der Geräte mit Abstand am häufigsten vertreten sind. Mit 7 Geräten ist die WAREMA electronic GmbH und ihren Beleuchtungssystemen [37] am zweithäufigsten vertreten. Silicon Laboratories und Ember Corporation sind mit jeweils 4 Geräten an dritter Stelle. Silicon Laboratories stellt größtenteils „System on Chip“ (SoC) Lösungen her, welche in einer Vielzahl an unterschiedlichen Geräten verbaut sein können. [38] Die Ember Corporation wurde 2012 von Silicon Labs aufgekauft. Welche Geräte von Ember hergestellt wurden, konnte nicht herausgefunden werden. Viconics Electronics Inc. stellt Thermostate und Umgebungssensoren her. [39] Die OSRAM GmbH stellt ebenfalls Beleuchtungssysteme her. [40] Durch die Analyse der Hersteller und deren Produktportfolio kann die Aussage getroffen werden, dass Beleuchtungssysteme mit Abstand die verbreitetsten ZigBee Geräte in dem Gebieten der Datensammlung sind.

Die ZigBee Kommunikation, welche Herstellern zugeordnet werden konnte, war bis auf eine Ausnahme ausschließlich in der Protokollversion ZigBee 2006 und ZigBee Pro. Lediglich bei WAMERA konnte ein Gerät gefunden werden, welches noch die Protokollversion ZigBee 2004 verwendet.

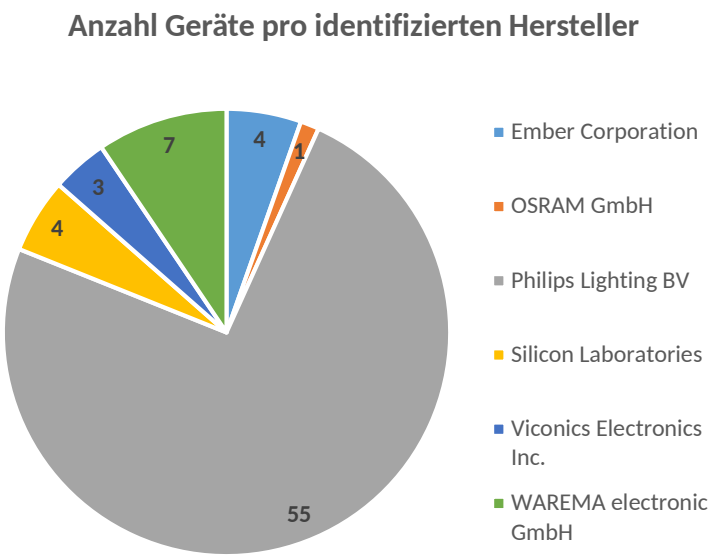

Abbildung 9.2.: Anzahl Geräte pro Hersteller

9.4. Sicherheitsmaßnahmen

Das allgemeine Sicherheitsniveau der gefundenen Netzwerke konnte nicht ermittelt werden, da das Security Level nach Definition des Standards auf „0“ gesetzt wird, wenn eine gesicherte Nachricht versendet wird. Dennoch können mit den gesammelten Daten Aussagen darüber getroffen werden, wie das Management des Network Keys implementiert wurde.

In Abbildung 9.3 ist die Anzahl der versendeten Nachrichten zu sehen, welche auf dem Network Layer gesichert wurden. Zusätzlich ist die Key Sequence Number angegeben, welche aussagt, wie oft der Network Key im Netzwerk bereits gewechselt wurde. Hierbei ist erkennbar, dass ein Großteil der ZigBee Netzwerke den Network Key seit der Inbetriebnahme nicht gewechselt haben. Dies ist darauf zurückzuführen, dass der periodische Wechsel des Network Keys nur eine Empfehlung und keine Vorgabe des Standards ist. Daraus resultiert, wenn ein Angreifer oder eine Angreiferin im Besitz des aktiven Network Keys ist, dieser den Network Key in den meisten Netzwerken auch sehr lange weiter verwenden kann, um Nachrichten in das Netzwerk zu schicken oder Kommunikation zu entschlüsseln.

9.5. Aufgetretene Probleme

Während der Entwicklung des Scanners und bei der Auswertung der Daten haben sich einige Probleme ergeben, welche sich auf die Ermittlung von ZigBee 3.0 Geräten und das Sicherheitsniveau auswirken. Auf die einzelnen Probleme wird eingegangen und es wird beleuchtet, weshalb diese nicht gelöst werden

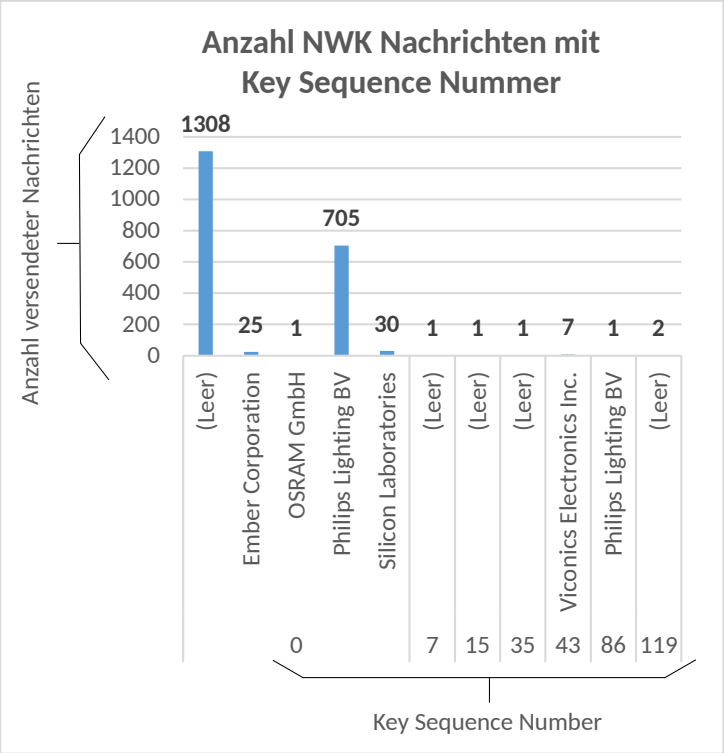

Abbildung 9.3.: Anzahl Network Keys nach Key Sequence Nummern

konnten.

9.5.1. Identifikation von ZigBee 3.0 Geräten

Da es im Aufbau eines ZigBee Frames zwischen den Versionen 2006 und ZigBee 3.0 keine Änderungen gegeben hat, kann über den Frame an sich nicht herausgefunden werden, ob dieser von einem ZigBee 3.0 Gerät gesendet wurde. Die meisten Änderungen, welche mit ZigBee 3.0 eingeführt wurden, beziehen sich auf allgemeine Abläufe und Vorgaben, beispielsweise wie Frame Counter gespeichert werden müssen. Wie im Kapitel 4.8 erwähnt wurde, ist mit ZigBee 3.0 ein End Device Aging Mechanismus eingebaut worden. Um diesen Mechanismus implementieren zu können, wurde zwei neue Network Commands hinzugefügt, der „End Device Timeout Reqeust“ und der „End Device Timeout Response“. Nachfolgend werden die beiden Commands im Detail beleuchtet und evaluiert, ob diese für das Aufspüren von ZigBee 3.0 Geräten verwendet werden können.

Timeout Request

Das „End Device Timeout Request“ Kommando ist ein Network Command und wird dementsprechend im Network Layer verschlüsselt. Dieses Kommando wird von einem Endgerät an seinen Parent gesendet

Requested Timeout Enumeration Value	Actual Timeout Value
0	10 Seconds
1	2 Minutes
2	4 Minutes
3	8 Minutes
4	16 Minutes
5	32 Minutes
6	64 Minutes
7	128 Minutes
8	256 Minutes
9	512 Minutes
10	1024 Minutes
11	2048 Minutes
12	4096 Minutes
13	8192 Minutes
14	16384 Minutes

Tabelle 9.1.: Mögliche Timeout Enumeration Werte

um diesen über Timout Voraussetzungen zu informieren. Dadurch kann der Parent einen Timout für dieses spezifische Endgerät setzten, welcher zwischen 10 Sekunden und 16384 Minuten (ungefähr 11 Tage) liegt. In Tabelle 9.1 sind die möglichen Timeout-Werte ersichtlich. Meldet sich das Endgerät innerhalb der spezifizierten Zeit nicht mehr beim Endgerät, wird das Endgerät aus dem Neighbor Table des Parents gelöscht. Dadurch ist das Gerät nicht mehr im Netzwerk und muss diesem erneut beitreten, um Nachrichten im Netzwerk senden zu können. Um den Timeout zurückzusetzen, muss das Endgerät innerhalb des spezifizierten Timeouts einen weiteren Timout Request senden. [3, S. 289-291]

Timeout Response

Das „End Device Timeout Response“ Kommando ist ebenfalls ein Network Command und wird auf im Network Layer verschlüsselt. Dieses Kommando wird vom Parent and das Endgerät gesendet um dieses darüber zu informieren, ob der Timout Request akzeptiert wurde. Weiters informiert der Parent das Endgerät darüber, in welcher Form Keep Alive Nachrichten akzeptiert werden. Dies kann einerseits

via „MAC Data Poll Keepalive Nachrichten“ oder „End Device Timeout Requests“ geschehen. [3, S. 291-292]

9.5.2. Identifikation des Security Levels

Das Security Level sagt aus, ob ein Frame verschlüsselt, integritätsgesichert, oder beides wird. Während der Entwicklung des ZigBee Scanner ist jedoch folgende Problematik aufgetreten:

> „8. The security level sub-field of the security control field shall be over-written by the 3-bit all-zero string ’000’.“ [3, S. 381]

Dies bedeutet, dass bevor ein geschützter Frame versendet wird, das Security Level Feld im Auxiliary Header mit „000“ überschrieben wird. Dadurch ist bei allen Frames lediglich das Security Level „None“ ersichtlich. Dies hat zur Folge, dass anhand des Security Level Feldes kein Auswertung über das allgemeine Sicherheitsniveau durchgeführt werden kann. Da das Security Level, welche in einem ZigBee Netzwerk vorherrscht, einem Gerät beim Beitreten in das Netzwerk mitgeteilt wird, müsst das „nwkSecurityLevel“ Attribut aus der NIB eines Gerätes ausgelesen werden, um den tatsächlichen Security Level zu ermitteln.

Um im Zuge des Warwalking nun das Sicherheitsniveau in einem Netzwerk ermitteln zu können, müsste in jedes gefundene Netzwerk ein Gerät eingebunden werden. Dadurch würde dieses vom Parent Gerät, über welches beigetreten wird, Netzwerkinformationen erhalten und in der NIB abspeichern. Hierfür müssten automatisiert und dynamisch Angriffe gegen gefundene ZigBee Netzwerke durchgeführt werden. Da sich diese Diplomarbeit mit der passive Sammlung von Daten befasst, wurden aktive Angriffe nicht umgesetzt.

10. Fazit und zukünftige Arbeit

In diesem Kapitel werden die einzelnen Forschungsfragen auf Basis der gesammelten Informationen beantwortet, sowie weiterführende Forschungsgebiete im Gebiet ZigBee 3.0 vorgestellt. Die präsentierten Ergebnisse basieren auf einer Analyse der ZigBee Pro Spezifikation [3], sowie der ZigBee Spezifikation R20 [13].

10.1. ZigBee 3.0 Sicherheitsmechanismen und Änderungen

Nachfolgend werden folgende Forschungsfragen beantwortet:

Welche Sicherheitsmechanismen bietet ZigBee 3.0 und wie sind diese implementiert?

Wurden sicherheitstechnische Schwachstellen von früheren ZigBee Protokollversionen in ZigBee 3.0 behoben?

ZigBee 3.0 verlässt sich bei dem Schutz der Integrität der Kommunikation auf den starken und erprobten Verschlüsselungsalgorithmus AES mit 128 Bit Schlüssellängen. Die Authentizität von Nachrichten wird durch den Einsatz des CCM-Modus gewährleistet und verhindert, dass nachträglich unbemerkte Änderungen bei Nachrichten vorgenommen werden. Schwachstellen aus älteren ZigBee Protokollversionen wurden in ZigBee 3.0 teilweise behoben. Zu diesen Änderungen gehören:

- Nur noch ein Network-Key mit einem Security Mode, welcher mit dem früheren High Security Mode gleichzusetzen ist.
- Empfehlungen zum Tauschen des Network-Keys mit maximaler Lebensdauer, Regelungen zur Verwendung von alten Network-Keys.
- Install Codes sind im Standard verankert und müssen unterstützt werden.
- Frame Counter werden persistent gespeichert und dürfen unter keinen Umständen zurückgesetzt werden.

- Netzwerke können maximal 254 Sekunden für Beitritte geöffnet werden.
- Geräte im Netzwerk müssen periodisch Keep-Alive Nachrichten an das Trust Center senden, um nicht aus dem Netzwerk entfernt zu werden.

10.2. Kritik und Verbesserungsvorschläge

Nachfolgend werden Kritikpunkte und zugehörige Verbesserungsvorschläge vorgestellt, welche bei der Analyse der ZigBee Pro Spezifikation aufgefallen sind.

Es gibt zwar Vorgaben, wann und wie ein Network-Key in einem ZigBee 3.0 Netzwerk aktualisiert werden muss, diese Vorgaben beziehen sich jedoch nicht auf Link-Keys. Link-Keys und deren Geheimhaltung sind ebenfalls ein essenzieller Bestandteil, wenn es um die Sicherheit eines ZigBee 3.0 Netzwerkes geht. Daher sollten auch diese regelmäßig aktualisiert und erneuert werden, sowie Vorgaben diesbezüglich im Standard festgelegt werden.

Install Codes sind in der ZigBee Pro Spezifikation verankert und müssen auch von Geräten unterstützt werden. Dies bezieht sich jedoch nur auf Geräte mit Routing-Funktionalität, also Router und Trust Center. Hersteller sind nicht verpflichtet Install Codes für die Einrichtung von Endgeräten zu verwenden. Install Codes sind mit Abstand die sicherste Methode, wie ein ZigBee 3.0 Gerät einem Netzwerk beitreten kann und gleichzeitig Kompatibilität zwischen Geräten unterschiedlicher Hersteller gewährleistet. Somit sollten Install Codes als Standardmethode für alle Arten von ZigBee 3.0 Geräten verwendet werden.

Der Erstaustausch des Network-Keys via dem Default Global Trust Center Link Key ist nach wie vor ein akzeptiertes Risiko in der ZigBee Pro Spezifikation. Mit der Vorraussetzung, dass alle ZigBee 3.0 Geräte Install Codes für den Beitritt in ZigBee 3.0 Netzwerke verwenden müssen, würde dieses Risiko wegfallen und die Sicherheit von ZigBee 3.0 Netzwerken würde allgemein gesteigert werden.

Die Rückwärtskompatibilität sowie die Unterstützung von alten Applikationsprofilen ist ein großer Kritikpunkt an ZigBee 3.0. Dies wird vor allem beim ZigBee Light Link Applikationsprofil deutlich. Wie in Kapitel 5.4 beschrieben wurde, wurden die Schwachstellen des Applikationsprofiles auch in ZigBee 3.0 übernommen. Die Sicherheit von Geräten, welche via Touchlink Commissioning einem Netzwerk beitreten, beruht auf einem geleakten ZigBee Light Link Master-Key. Dieser Master-Key ist auf allen ZigBee

3.0 Geräten, die Touchlink unterstützen vorinstalliert und wurde auch mit ZigBee 3.0 nicht geändert. Abgesehen von dieser Tatsache ist es eine schlechte Idee die Sicherheit eines gesamten Netzwerkes auf die Geheimhaltung eines Master-Keys zu reduzieren, welcher einem Großteil der Hersteller von ZigBee 3.0 Geräten bekannt ist.

Insecure Rejoins sind in ZigBee 3.0 Netzwerken nach wie vor möglich. Da für die Durchführung eines Insecure Rejoins sich das Gerät bereits im Netzwerk befunden haben muss, gibt es in ZigBee 3.0 Netzwerken keinen Grund mehr diese nicht komplett zu verbieten. Dadurch würde bei einem Wiederbeitritt von Geräten der Link-Key verwendet werden, welcher für jedes Gerät einzigartig ist.

10.3. ZigBee 3.0 Verbreitung und Sicherheitsniveau

Nachfolgend wird auf die folgende Forschungsfrage eingegangen:

Wie ist die Verbreitung von ZigBee 3.0 Geräten und welche Sicherheitsmechanismen werden tatsächliche eingesetzt?

Die Frage hat nur teilweise beantwortet werden können, da gewisse Informationen wie das Sicherheitsniveau oder die verwendete Protokollversion, nicht aus dem Header der ZigBee Frames gewonnen werden konnten. Bei der Protokollversion besteht das Problem, dass sich alle ZigBee Protokolle ab ZigBee 2006 den selben Identifikator teilen. Das bedeutet, alle Protokolle ab 2006 laufen unter dem Namen „ZigBee 2006 / ZigBee Pro“. Eine Alternative um dennoch darauf schließen zu können, ob es sich bei gefundener ZigBee Kommunikation um ZigBee 3.0 handelt, wäre durch die Verwendung von sogenannten „Keep Alive“ Nachrichten. Diese werden im Zuge des „Child Aging“ Mechanismus verwendet, welcher mit ZigBee 3.0 neu hinzugekommen ist. Das Problem hierbei ist jedoch, dass es sich bei diesen Nachrichten um Network Commands handeln würde. Das bedeutet, dass das Gerät, welches diese Nachrichten versendet, einen aktiven und validen Network Key besitzen muss. Um in den Besitz des aktiven Network Keys zu gelangen, müssten laufend Angriffe gegen ZigBee Netzwerke während der Datensammlung durchgeführt werden und beispielsweise ein Trust Center Rejoin provoziert werden, indem die Funkverbindung von gezielten Geräten blockiert wird. Dieser Aspekt war außerhalb des Scopes dieser Diplomarbeit, ist jedoch ein interessanter Aspekt, welcher in zukünftigen Arbeiten verfolgt werden kann.

Das Sicherheitsniveau kann per Definition des ZigBee Protokolls nicht ermittelt werden, da das „Security Level“ Feld im Network Header durch „0“ ersetzt wird, sobald ein geschützter Frame versendet

wird. Somit wird der Security Level aller empfangenen Nachrichten als „None“ angezeigt, sollten diese auf dem Network Layer geschützt worde sein. Um das Tatsächliche Sicherheitsniveau eines ZigBee Netzwerkes herauszufinden zu können, müsste ein Gerät in das Netzwerk eingebunden werden. Dadurch würde die Network Information Base des beitretenden Gerätes aktualisiert und Informationen über die Sicherheitseinstellungen des Netzwerkes eingetragen werden. Wie auch bei der Ermittlung der Protokollversion, müssten hierfür ein Gerät in ein ZigBee Netzwerk eingeschleust werden, was zu den vorhin genannten Problemen führt.

Bei den aufgezeichneten Testdaten ist jedoch herausgestochen, dass bei fast allen gefundenen Netzwerken, der Network Key die Key Sequence Number „0“ hat. Dies bedeutet, dass der Network-Key in diesen Netzwerken seit deren Inbetriebnahme nicht geändert wurde.

Es kann nur eine generelle Aussage über die Verbreitung von ZigBee Netzwerken getroffen werden, da ab ZigBee 2006 nicht mehr zwischen Protokllversionen unterschieden wird. ZigBee Geräte sind in Gebieten wie Einkaufsstraßen relativ häufig anzutreffen. Dies ist auf die dichte Streuung von Geschäften zurückzuführen. Weiters ist die Distanz zu den Geräten an sich ziemlich gering. Dadurch ist die Wahrscheinlichkeit höher, ZigBee Geräte zu finden, da die benötigten Antennen nicht so stark sein müssen, um Funkkommunikation in diesen Gebieten zu empfangen.

10.4. Schlusswort

Allgemein ist ein ZigBee Netzwerk, sobald alle Geräte eingerichtet sind, sehr gut abgesichert. Viele Sicherheitsaspekte, wie beispielsweise die Unterstützung von Install Codes, werden jedoch den Herstellern von Geräten überlassen und müssen nicht von diesen in ihren Produkten eingesetzt werden. Auch der Tausch von Schlüsselmaterial ist eine Empfehlung und keine Vorgabe die erfüllt werden muss. Daher ist es auch mit ZigBee 3.0 möglich unsichere Netzwerke zu betreiben. Die größte Problematik in ZigBee Netzwerken ist nach wie vor der initiale Schlüsselaustausch, der unsichere Wiederbeitritt (Insecure Rejoin) zu Netzwerken und die Rückwärtskompatibilität zu alten ZigBee Versionen und Applikationsprofilen mit bekannten Schwachstellen, wie beispielsweise ZigBee Light Link. ZigBee 3.0 hat ein paar gute Änderungen im Hintergrund mit sich gebracht, wie beispielsweise nicht löschbare Frame Counter. Um ein rundum sicheres ZigBee Netzwerk betreiben zu können, müssten jedoch auch die Verwendung von Install Codes erzwungen und auf die Kompatibilität mit veralteten ZigBee Versionen verzichtet werden. Bis dahin ist es jedoch noch ein weiter Weg und erfordert sehr wahrscheinliche eine weitere Iteration des ZigBee Standards.

A. Physical (PHY) Layer

Dies ist die unterste Schicht des ZigBee Stacks, welche für die physischen Übermittlungsmedien zuständig ist und den Austauscht von Datenbits regelt. Diese Schicht gibt im weiteren Verlauf Daten an den MAC Layer weiter, welcher diese für die weitere Verarbeitung aufbereitet. [12, S. 34]

A.1. Frequenzbänder

Die Kommunikation kann in drei verschiedenen Frequenzen erfolgen, 868-, 915- oder 2400-MHz. Diese Frequenzen sind für den unlizenzierten Einsatz, je nach geographischer Lage, verfügbar.
Wie in Tabelle A.1 auf Seite 81 zu sehen ist, bietet das 2400-MHz Frequenzband den Vorteil, dass es weltweit unlizenziert einsetzbar ist. Es bietet höhere Datenraten und mehr Kanäle als die Frequenzbänder 868- und 915-MHz und ist generell vom Markt besser verstanden und akzeptiert. Ein weiterer Vorteil ist, dass weniger Energie verbraucht wird um Daten zu senden, da das Empfangen und Senden von Daten auf Grund der höheren Datenraten in einer kürzeren Zeitspanne abgeschlossen werden kann. Dennoch bieten die Frequenzbänder 868- und 915-MHz andere Vorteile wie weniger Benutzer, weniger Störungen und weniger Absorption und Reflexion von Funksignalen. Diese Vorteile überwiegen jedoch nicht jene des 2400-MHz Frequenzbandes und daher wird bei ZigBee Geräten meist das 2400-MHz Frequenzband verwendet, auch wenn es möglich ist, ein ZigBee Netzwerk in den anderen IEEE 802.15.4 Frequenzbändern zu betreiben. [12, S. 25]

Frequenzband	Frequenz-bereich (MHz)	Datenrate (kbps)	Kanal Nummer(n)	Geographisches Gebiet
868 MHz	868.3	20	0 (1 Kanal)	Europa
915 MHz	902-928	40	1-10 (10 Kanäle)	Amerika Australien
2400 MHz	2405-2480	250	11-26 (16 Kanäle)	Weltweit

Tabelle A.1.: Funkfrequenzbänder [12, S. 25]

A.2. Reichweite

Die Funkreichweite hängt von der Umgebung ab, in der die Kommunikation stattfindet. Ein mit entsprechender Ausrüstung ausgestattetes Gerät, kann in einem offenen Gebiet eine Reichweite von über 1 Kilometer erreichen. Innerhalb von Gebäuden wird die Reichweite meist durch Absorption und Reflexion von Funksignalen beeinträchtigt, die von Wänden und andere soliden Hindernissen ausgeht. [12, S. 25] Da ZigBee Geräte jedoch auf niedrigen Stromverbrauch ausgelegt sind und damit Peripherie wie Antennen ebenfalls schwächer ausfallen, ist bei diesen Geräten eine Reichweite von 10-100 Meter zu erwarten.

A.3. PPDU Frame Format

Der PHY Layer sendet Daten in Form von PHY Protocol Data Units (PPDU). In Abbildung A.1 auf Seite 82 ist der Aufbau eines PPDUs zu sehen. Ein PPDU besteht aus dem Synchronization Header, PHY Header und PHY Payload. Nachfolgend werden die einzelnen Felder einer PPDU beschrieben. [11, S. 160]

Synchronization Header		PHY Header		PHY Payload
4 B	1 B	1 B		X B
Preamble	SFD	Frame lenght (7 bits)	Reserved (1 bit)	PSDU

Abbildung A.1.: Format des PPDU

A.3.1. Preamble

Das Preamble Feld wird zur Synchronisation bei einer eingehenden Nachricht verwendet und beinhaltet 32 Bit Nullen. [11, S. 160]

A.3.2. SFD - Start-Of-Frame Delimiter Feld

Dieses Feld markiert das Ende des Preamble Feldes und den Beginn der Paketdaten. Dieses Feld muss wie in Abbildung A.2 ersichtlich formatiert sein. [11, S. 160]

Bits: 0	1	2	3	4	5	6	7
1	1	1	0	0	1	0	1

Abbildung A.2.: Format des SDF Feldes

A.3.3. Frame Length

Dieses Feld gibt die Anzahl der im Physical Service Data Unit (PSDU) enthaltenen Bytes an. Der Wert kann zwischen 0 und 127 liegen. Aus Tabelle A.2 auf Seite 83 können die verfügbaren Werte entnommen werden.

Frame length values	Payload
0-4	Reserved
5	MPDU (Acknowledgment)
6-7	Reserved
8-127	MPDU

Tabelle A.2.: Frame Length Werte [11, S. 161]

Die Unterstütze maximale Größe, welche für das Frame Length Feld zur Verfügung steht hängt von der jeweiligen Hardware ab und kann während der Operation eines Gerätes nicht verändert werden. Information über die maximale Länge des PSDU werden in einer sogenannten PAN Information Base (PIB) verwaltet. [11, S. 160]

A.3.4. PSDU - Physical Service Data Unit

Dieses Feld hat eine Variable Länge und beinhaltet die Daten des PHY Paketes. Bei allen Paketen, bei denen die Länge gleich fünf oder größer sieben Byte ist, beinhaltet die PSDU einen MAC Sublayer Frame (z.B.: MAC Protocol Data Unit - MPDU). [11, S. 160]

B. Medium Access Control (MAC) Layer

Diese Schicht ist für die Adressierung zuständig. Es bestimmt wo ausgehende Pakete hingesendet werden und bei eingehenden Paketen bestimmt sie wo die Pakete hergekommen sind. [12, S. 34]

B.1. Optionale Sicherheitsmaßnahmen

B.1.1. Integrität

Die Datenintegrität wird überprüft, indem mit der Nachricht ein Message Integrity Code (MIC) mitgeschickt wird. Der MIC wird berechnet, indem eine Hashfunktion über die Nachricht und den Preshared Key gelegt wird. Die Integrität der Nachricht kann überprüft werden, indem der Empfänger dieselbe Hashfunktion auf seinen Preshared Key und die empfangene Nachricht anwendet. Der MIC kann in 32-bit, 64-bit oder 128-bit Länge angehängt werden. [8]

B.1.2. Vertraulichkeit

Um die Vertraulichkeit der Nachricht zu gewährleisten, wird beim AES-CTR und AES-CCM Security Suite eine 13-bit Nonce im Klartext mit der verschlüsselten Nachricht mitgesendet. Die Nonce besteht aus der Source-Adresse und einem Framecounter, welcher nach jeder Nachricht erhöht wird. [8]

B.1.3. Replay-Schutz

Um Replay-Attacken zu verhindern, wird ein Framecounter mit jeder Nachricht mitgesendet. Erhält eine Node eine Nachricht mit demselben Framecounter mehrmals, werden diese Nachrichten verworfen. Im IEEE 802.15.4 Standard wird ein 32-bit Counter verwendet, das bedeutet, dass ein Replay-Angriff erst nach 2^{32} Frames oder Nachrichten durchgeführt werden kann. Zusätzlich wird der Framecounter als Input für die Nounce verwendet. [8]

Security level/Id	Security suite	Vertraulichkeit	Authentizität
000	None	X	X
001	AES-CBC-MAC-32	X	✓
010	AES-CBC-MAC-64	X	✓
011	AES-CBC-MAC-128	X	✓
100	AES-CTR	✓	X
101	AES-CCM-32	✓	✓
110	AES-CCM-64	✓	✓
111	AES-CCM-128	✓	✓

Tabelle B.1.: IEEE 802.15.4 Security Suites [8]

B.2. Security Suites

Wie in Tabelle B.1 auf Seite 85 zu sehen ist, unterstützt der IEEE 802.15.4 Standard drei unterschiedliche Security Suites. Die Security Suites unterscheiden sich in ihrer Fähigkeit bei Daten die Vertraulichkeit, Authentizität oder eine Kombination der Beiden sicherzustellen. Wie im Kapitel 2.4.2 beschrieben, werden diese Security Suites in ZigBee Netzwerken nicht verwendet.

B.2.1. AES-CBC-MAC

Die AES-CBC-MAC Security Suite sendet Nachrichten unverschlüsselt und fügt am Ende der Payload einen Message Integrity Code (MIC) hinzu. Zur Erstellung des Cipher Block Chaining Message Authentication Code (CBC-MAC) wird ein symmetrischer Schlüssel (AES) verwendet. Die Integrität der Nachricht kann ermittelt werden, indem erneut aus der Payload und dem Schlüssel der CBC-MAC errechnet wird. Stimmt der übermittelte und errechnete CBC-MAC überein, ist die Integrität der Nachricht nachgewiesen. [41, S. 170]

B.2.2. AES-CTR

Der Counter Mode (CTR) symmetrische Verschlüsselungsalgorithmus sendet Nachrichten verschlüsselt, es wird jedoch kein MIC erzeugt um die Integrität der Nachricht zu gewährleisten. Für die Verschlüsselung wird ein 128 Bit AES Schlüssel verwendet. Bei der CTR Betriebsart wird der Klartext in 128 Bit Blöcke unterteilt, welche mit einem Zwischenschlüssel verschlüsselt werden. Jeder Block hat seinen eigenen Zwischenschlüssel, welcher aus einer Nonce und einem Zähler erzeugt wird, welcher mit dem symmetrischen Schlüssel (AES) verschlüsselt wird. [41, S. 170]

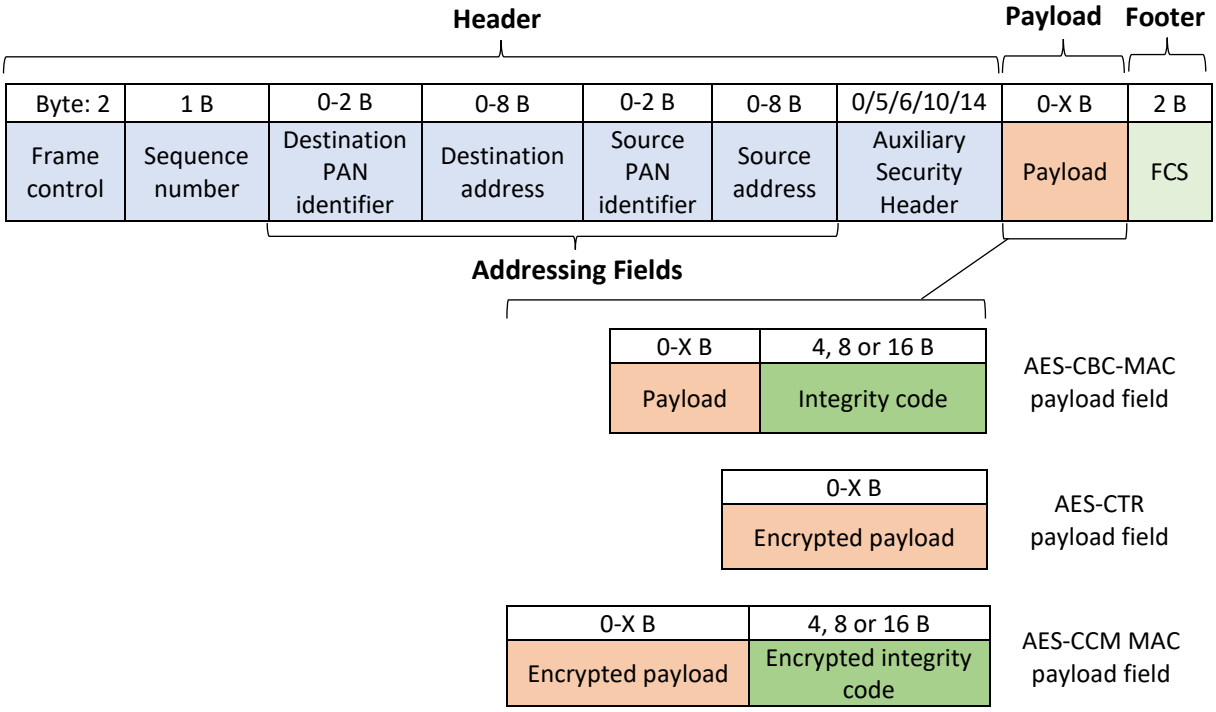

Abbildung B.1.: MAC Security Suite Frame Format

B.2.3. AES-CCM

Die AES-CCM Security Suite ist eine Kombination aus CTR und CBC-MAC. Bei dieser Suite wird zunächst ein MIC für den Klartext erstellt und im Nachhinein der Klartext und der MIC verschlüsselt. Dadurch kann sowohl die Vertraulichkeit als auch die Integrität der Nachricht gewährleistet werden. [41, S. 170]

B.3. MAC Frame Format

In Abbildung B.1 auf Seite 86 ist der Aufbau eines MAC-Frames zu sehen. Der generelle MAC Frame besteht aus MAC Header, Payload und Footer. Im MAC Header befindet sich die Frame Control, Sequence Number, Destination Address und Source Address. In der MAC Payload befinden sind die zu übermittelnden Daten und im MAC Footer befindet sich die Frame Check Sequence (FCS), welche für die Sicherstellung der fehlerfreien Übertragung zuständig ist. Nachfolgend werden die einzelnen Felder des MAC Frames beschrieben. [11, S. 57-61]

Frame type value $b_2b_1b_0$	Description
000	Beacon
001	Data
010	Acknowledgement
011	MAC command
100-111	Reserved

Tabelle B.2.: Werte des Frame Type Subfeldes

B.3.1. Frame Control

Das Frame Control Feld hat eine Länge von 16 Bit und definiert den Frame-Typen, Adressmodus, sowie weiter Kontroll-Flags. [11, S. 57-59]

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enabled	Frame pending	Ack request	PAN ID Compression	Reserved	Dest. adressing mode	Frame Version	Source adressing mode

Abbildung B.2.: Format des Frame Control Feldes

Frame Type

Dieses Feld hat eine Länge von 3 Bit und legt den Typen der Nachricht fest. Ein Frame kann den Typ Beacon, Data, Acknowledgement oder MAC Command haben. Die spezifischen Werte können aus der Tabelle B.2 auf Seite 87 entnommen werden.

Security enabled

Dieses Feld hat den Wert 0, wenn der Frame nicht kryptographisch gesichert werden soll. Ist der Wert des Feldes auf 1 gesetzt, wird der Frame verschlüsselt übertragen.

Frame Pending

Dieses Feld hat den Wert 1, wenn weitere Frames zu senden sind und hat den Wert 0, wenn keine weiteren Daten an den Empfänger gesendet werden.

Ack request

Dieses Feld gibt an, ob eine Empfangsbestätigung des Empfängers benötigt wird. Ein Wert von 1 gibt an, dass ein Achnowledgment Frame vom Empfänger gesendet werden soll. Bei 0 wird kein Acknowledgment Frame erwartet.

PAN ID Compression

Diese Feld soll verhindern, dass der gleiche PAN Identifier mehrmals gesendet wird. Ist der Wert des Feldes auf eins gesetzt, wird nur der Destination PAN Identifier im Frame mitgesendet und für den Source PAN Identifier wird der Wert vom Destiantion PAN Identifier angenommen.

Destination Addressing Modes

Dieses Feld kann auf einen Wert gesetzt werden, welche in Tabelle B.3 auf Seite 88 zu entnehmen sind. Wenn der Wert des Feldes 0 ist und das Frame Type Feld diesen Frame nicht als Acknowledgment Frame spezifiziert, darf das Source Addressing Mode Feld nur auf einen anderen Wert als 0 gesetzt werden.

Frame Version

Dieses Feld gibt die Version des Frames an. Wenn das Feld auf null gesetzt wird, ist der Frame mit IEEE Std. 802.15.4-2003 kompatibel. Bei einem Wert von eins handelt es sich u einen IEEE 802.15.4 Frame. Alle anderen Werte sind reserviert.

Source Addressing Mode

Dieses Feld kann auf einen Wert gesetzt werden, welche in Tabelle B.3 auf Seite 88 zu entnehmen sind. Wenn der Wert des Feldes 0 ist und das Frame Type Feld diesen Frame nicht als Acknowledgment Frame spezifiziert, darf das Destination Addressing Mode Feld nur auf einen anderen Wert als 0 gesetzt werden.

Addressing Mode Wert $b_1 b_0$	Beschreibung
00	PAN identifier und Adressfelder sind nicht vorhanden
01	Reserviert
10	Adressfeld beinhaltet 16 Bit Adresse
11	Adressfeld beinhaltet 64 Bit Adresse

Tabelle B.3.: Werte der Source und Destination Address Mode Felder

B.3.2. Sequence Number

Dieses Feld hat eine Länge von 8 Bit und stellt einen eindeutigen Identifikator für den Frame dar.
Bei deinem Beacon Frame wird eine Beacon Sequence Number (BSN) eingetragen. Jeder Coordinator speichert seine momentane BSN in seiner MAC Personal Area Network Information Base (PIB). Die BSN wird zufällig initialisiert und nach jedem ausgesendeten Beacon Frame inkrementiert.
Bei Data, Acknowledgment oder MAC Command Frames, wird in diesem Feld eine Data Sequence Number (DSN) eingetragen, welche dazu verwendet wird den Acknowledgment Frame mit dem Data oder MAC Command Frame abzustimmen. Jedes Gerät verwaltet genau eine DSN und verwaltet diese in seiner MAC PIB. Die DSN wird zufällig initialisiert und nach jedem versendeten Data oder MAC Command Frame inkrementiert.
Wird ein Acknowledgment Frame angefordert, wird die erhaltene DSN kopiert und in das Sequence Number Feld eingefügt. [11, S. 59]

B.3.3. Destination PAN Identifier

Das Destination PAN Identifier Feld hat eine Länge von 16 Bit und enthält einen einzigartigen Identifikator des PANs, in welchem sich der Empfänger der Nachricht befindet. Ein Wert von 0xffff gibt an, dass es sich um einen Broadcast handelt und sollte als valider PAN Identifier von allen im gleichen Channel befindlichen Geräten akzeptiert werden. Dieses Feld wird im MAC Header nur dann angehängt, wenn das Destination Addressing Mode Feld einen anderen Wert als Null hat. [11, S. 59]

B.3.4. Destination Address

Das Destination Address Feld hat eine Länge von 16 oder 64 Bit, je nachdem welcher Wert im Destiantion Addressing Mode Feld eingetragen wurde und beinhaltet die Netzwerkadresse des Empfängers der Nachricht. Bei einem 16 Bit Wert von 0xffff handelt es sich um eine Broadcast Adresse, welche von allen Geräten als valide Adresse akzeptiert werden sollte. Wie auch beim Destination PAN Identifier Feld wird dieses Feld nur im MAC Header angehängt, wenn das Destination Addressing Mode Feld einen anderen Wert als Null hat. [11, S. 60]

B.3.5. Source PAN Identifier

Das Source PAN Identifier Feld hat eine Länge von 16 Bit und enthält einen einzigartigen Identifikator des PANs, aus welchem die Nachricht versendet wurde. Dieses Feld wird im MAC Header nur dann angehängt, wenn das Source Addressing Mode Feld und das Intra PAN Feld im Frame Control einen anderen Wert als Null haben. [11, S. 60]

B.3.6. Source Address

Das Source Address Feld hat eine Länge von 16 oder 64 Bit, je nachdem welcher Wert im Source Addressing Mode Feld eingetragen wurde und beinhaltet die Netzwerkadresse des Senders der Nachricht. Dieses Feld wird im MAC Header nur dann angehängt, wenn sich im Source Addressing Mode Feld der Frame Control ein anderer Wert als Null befindet. [11, S. 60]

B.3.7. Auxiliary Security Header

Dieses Feld enthält Informationen für die sicherheitstechnische Verarbeitung des Frames. Dieses Feld wird nur dann im Frame inkludiert, wenn das Security Enabled Flag auf „TRUE“ gesetzt ist. Das Format des Auxiliary Security Headers ist in Abbildung B.3 zu sehen. [11, S. 139-142]

Bytes: 1	4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Abbildung B.3.: Format des Auxiliary Security Header

Security Control

Dieses Feld gibt an, welche Art von Schutz auf den Frame angewendet wird. In Abbildung B.4 ist der Aufbau des Security Control Feldes zu sehen.

Bit: 0-2	3-4	5-7
Security Level	Key Identifier Mode	Reserved

Abbildung B.4.: Format des Security Control Feldes

Security Level: Dieses Feld gibt an, welcher Security Suite eingesetzt wurde, um den Frame zu schützen. In Tabelle B.1 sind die zur Verfügung stehenden Security Suite mit dazugehörigen Werten ersichtlich.
Key Identifier Mode: Dieses Feld gibt an, ob der verwendete Schlüssel implizit oder explizit abgeleitet werden kann. Die zur Verfügung stehenden Werte könne aus Tabelle B.4 entnommen werden. Ist der Modus 0x00 in Verwendung, wird das Key Identifier Feld des Auxiliary Security Headers nicht inkludiert.

Frame Counter

Dieses Feld enthält einen Zähler, welcher zum Schutz vor Replay-Angriffen dient. Weiters dient der Zähler als Input für eingesetzte kryptographische Funktionen.

Key identifier mode	Key Identifier Mode Feld b_1b_0	Beschreibung	Key Identifier Feld Länge (Byte)
0x00	00	Schlüssel wird implizit vom Sender und Empfänger des Frames bestimmt	0
0x01	01	Schlüssel wird vom Key Index in Verbindung mit macDefaultKeySource bestimmt	1
0x02	10	Schlüssel wird explizit vom 4-Byte Key Source Feld und dem Key Index Feld bestimmt	5
0x03	11	Schlüssel wird explizit vom 8-Byte Key Source Feld und dem Key Index Feld bestimmt	9

Tabelle B.4.: Werte des Key Itentifier Mode Feldes

Key Identifier

Dieses Feld gibt an, welcher Schlüssel für die Verschlüsselung der Daten verwendet wird. In Abbildung B.5 ist der Aufbau des Key Identifier Feldes zu sehen.

Bytes: 0/4/8	1
Key Source	Key Index

Abbildung B.5.: Format des Key Identifier Feldes

Key Source: Dieses Feld gibt den Ursprung des Schlüssels an. Wenn das Key Identifier Mode Feld vier Byte vorsieht, wird dieses Feld mit der Source PAN ID in Verbindung mit der Source Short Address befüllt. Sind 8 Byte vorgesehen, wird dieses Feld mit der Extendet Source Address befüllt.
Key Index: Dieses Feld hilft bei der Unterscheidung von unterschiedlichen Schlüsseln, sollte ein Geräte mehrere Schlüssel von einem Ursprungs-Gerät haben.

B.3.8. Payload

Das Payload Feld hat eine variable Länge und wird je nach ausgewähltem Security Suite verschlüsselt übertragen. [41, S. 115]

B.3.9. FCS

Das FCS Feld hat eine Länge von 16 Bit und enthält einen 16 Bit ITU-T CRC, welcher über den MAC Header und die MAC Payload berechnet wird. [11, S. 60]

C. Network Layer

In diesem Kapitel wird der Aufbau eines Network Layer Frames im Detail beschrieben.

C.1. Generelles Network Frame Format

Im Network Layer wird der Network Frame erstellt und als MAC Payload mitgesendet. Der Network Frame besteht aus dem Header, welcher für Frame Control, Adressierung und Sequenz-Informationen beschreibt, sowie aus der Payload, welche die Informationen des Frames beinhaltet. In Abbildung C.1 ist der generelle Aufbau eines Network Frames zu sehen. Nachfolgend werden die einzelnen Felder des Frames beschrieben. [3, S. 263-264]

	Header								Payload
Bytes: 2	**2**	**2**	**1**	**1**	**0/8**	**0/8**	**0/1**	**Varibale**	**Variable**
Frame control	Destination address	Source address	Radius	Sequence number	Destination IEEE Address	Source IEEE Address	Multicast control	Source route subframe	Frame payload

Abbildung C.1.: Format des Network Frames

C.1.1. Frame Control

Das Frame Control Feld hat eine Länge von 16 Bits und beschreibt den Frame Typen, Adressierung, sowie weitere Control Flags. In Abbildung C.2 ist der Aufbau des Frame Control Feldes zu sehen. [3, S. 264-266]

Bits: 0-1	**2-5**	**6-7**	**8**	**9**	**10**	**11**	**12**	**13**	**14-15**
Frame type	Protocol version	Discover route	Multicast flag	Security	Source Route	Destination IEEE Address	Source IEEE Address	End Device Initiator	Reserved

Abbildung C.2.: Format des NWK Frame Control Feldes

Frame Type

Dieses Feld gibt den Typen des Frames an und kann auf einen der Werte ersichtlich in Tabelle C.1 gesetzt werden.

Frame Type Value b_1 b_0	Frame Type Name
00	Data
01	NWK command
10	Reserved
11	Inter-PAN

Tabelle C.1.: Werte des NWK Frame Type Feldes

Protocol Version

Dieses Feld beschreibt die verwendete Version des ZigBee NWK Protokolls. Jedes ZigBee Gerät muss seine verwendet Protokoll Version als Konstante „nwkcProtocolVersion“ abgespeichert haben.

Discover Route Sub-Field

Dieses Feld gibt an, ob der Frame über neue Routen geschickt werden darf oder nicht. Ein Wert von 0x00 bedeutet, dass keine neuen Routen entdeckt werden dürfen, bei einem Wert von 0x01 dürfen hingegen neue Routen entdeckt werden. Handelt es sich bei dem gesendeten Frame um ein NWK Command Frame, muss der Wert des Feldes auf 0x00 gesetzt werden. Die Werte 0x02 und 0x03 sind reserviert.

Multicast Flag

Bei einem Wert von 0x0 handelt es sich bei diesem Frame um ein Unicast oder Multicast Frame. Ein Wert von 0x1 bedeutet, dass es sich um einen Multicast Frame handelt. Das Multicast Control Feld darf im NWK Header nur vorhanden sein, wenn dieses Feld den Wert 0x1 hat.

Security

Dieses Feld darf nur dann den Wert 0x1 haben, wenn dieses Frame NWK Sicherheitsoperationen aktiviert haben soll. Ist die Sicherheit des Frames in einem anderen Layer implementiert oder gar deaktiviert, hat dieses Feld den Wert 0x0.

Source Route

Dieses Feld gibt an, ob ein Source Route Sub Frame im Header inkludiert wird oder nicht. Bei einem Wert von 0x1 ist ein Source Route Sub Frame vorhanden, bei einem Wert von 0x0 wird das Feld im Header nicht angefügt.

Destination und Source IEEE Address

Wenn die volle IEEE Adresse des Ziels bzw. des Empfängers im Header inkludiert werden soll, hat dieses Feld den Wert 0x1, ansonsten 0x0.

End Device Initiator

Dieses Feld gibt an, ob der Frame von einem Endgerät aus gesendet wird. Ist dies der Fall, hat dieses Feld eine Wert von 0x1, ansonsten 0x0.

C.1.2. Destination Address

Dieses Feld beinhaltet die Netzwerkadresse des Empfängers, welche den Wert der MAC Short Adresse hat. Bei einem Multicast Frame wird hier die Gruppen-ID der Multicast-Gruppe eingetragen, an welche die Nachricht gesendet werden soll. [3, S. 266]

C.1.3. Source Address

Dieses Feld beinhaltet die Netzwerkadresse des Senders und ist auf den Wert der MAC Short Adresse zu setzen. [3, S. 266]

C.1.4. Radius

Diese Feld gibt die Anzahl an Hops an, welche der Frame passieren darf. Jedes Gerät, welches den Frame erhält senkt den Wert des Feldes um 0x1. [3, S. 266]

C.1.5. Sequence Number

Dieses Feld enthält einen Zähler welcher nach jedem versendeten Frame erhöht wird. Die Sequence Number in Verbindung mit Wert der Source Adresse kann dazu verwendet werden, um einen Frame eindeutig zu identifizieren. [3, S. 266]

C.1.6. Destination und Source IEEE Address

Dieses Feld enthält, wenn vorhanden, die volle 64-Bit IEEE Adresse des Empfängers beziehungsweise des Senders. [3, S. 266-267]

C.1.7. Multicast Control

Dieses Feld enthält Control Flags für Mulicast Frames und ist nur dann im Header inkludiert, wenn das Multicast Flag den Wert 0x1 hat. In Abbildung C.3 ist der Aufbau des Multicast Control Feldes zu sehen. [3, S. 267]

Bits: 0-1	2-4	5-7
Multicast mode	NonmemberRadius	MaxNonmemberRadius

Abbildung C.3.: Format des NWK Multicast Control Feldes

Multicast Mode

Dieses Feld gibt an ob der Frame nur zu Mitgliedern der Multicast-Gruppe oder auch über Geräte weitergeleitet werden darf, welche nicht in der Multicast-Gruppe sind. Ein Wert von 0x0 bedeutet, dass auch Geräte außerhalb der Multicast-Gruppe den Frame weiterleiten dürfen. Ein Wert von 0x1 bedeutet, dass der Frame nur innerhalb der Multicast-Gruppe gesendet werden darf. Die Werte 0x2 und 0x3 sind reserviert.

NonmemberRadius

Dieses Feld enthält einen Zähler, welcher angibt wie viele Geräte, die nicht zur Multicast-Gruppe gehören, den Frame weiterleiten dürfen. Erhält ein Gerät außerhalb der Multicast-Gruppe den Frame und dieses Feld hat den Wert 0x0, wird der Frame verworfen. Hat das Feld einen Wert zwischen 0x6 und 0x1 wird der Zähler um 0x1 reduziert bevor der Frame weitergeleitet wird. Ein Wert von 0x7 bedeutet, dass der Frame unbegrenzt weitergeleitet werden darf und der Zähler wird nicht reduziert. Erhält ein Gerät innerhalb der Multicast-Gruppe den Frame, setzt es dieses Feld auf den Wert des MaxNonmemberRadius Feldes bevor der Frame weitergeleitet wird.

MaxNonmemberRadius

Der Wert in diesem Feld gibt an, wie oft der Frame maximal von Geräten außerhalb der Multicast-Gruppe weitergeleitet werden darf.

C.1.8. Source Route Subframe

Der Source Route Subframe enthält eine Liste an Relays, über welche Frames weitergeleitet werden. In Abbildung C.4 ist der Aufbau des Source Route Subframes zu sehen.

Byte: 1	1	Variable
Relay count	Relay index	Relay list

Abbildung C.4.: Format des NWK Source Route Subframe Feldes

Relay Count

Dieses Feld gibt an, wie viele Relays in der Relay List eingetragen sind.

Relay Index

Dieses Feld verweist auf einen Eintrag in der Relay List, an welchen der Frame als nächstes gesendet werden soll. Der Index wird auf eine Größe initialisiert, welche der Anzahl der eingetragenen Relays in der List minus 1 entspricht. Jeder Relay reduziert diesen Wert um 1 bevor der Frame weitergeleitet wird.

Relay List

In diesem Feld sind die Adressen der Relays eingetragen. Der Relay, welcher der Destination am nächsten ist, soll als erstes gelistet werden. Der Relay, welcher dem Ursprung am nächsten ist, soll als letztes gelistet werden.

C.1.9. Frame Payload

Das Frame Payload Feld hat eine variable Größe und enthält Informationen, spezifisch zum Frame Typen.

D. Application Layer

In diesem Kapitel wird der Aufbau eines Application Layer Frames im Detail beleuchtet.

D.1. Generelles Application Frame Format

Der Application Frame besteht aus dem Application Header und der Application Payload. Der Application Header beseht aus Frame Control, optionalen Adressierungsfeldern, APS Counter und einem optionalen erweiterten Header. In Abbildung D.1 ist der generelle Aufbau des Application Frames zu sehen. [3, S. 42-46]

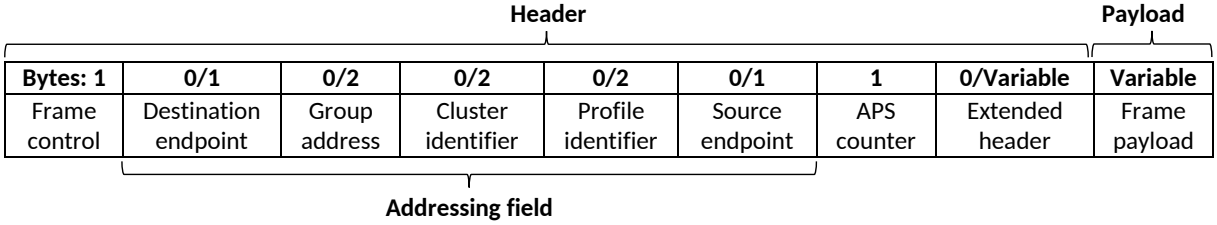

Abbildung D.1.: Format des Application Frames

D.1.1. Frame Control

Das Frame Control Feld hat eine Länge von 8 Bits und besteht aus den Feldern Frame Type, Delivery Mode, Ack. Format, Security, Ack. Request und Extended Header Present. In Abbildung D.2 ist der Aufbau des Frame Control Feldes zu sehen.

Bits: 0-1	2-3	4	5	6	7
Frame type	Delivery mode	Ack. format	Security	Ack. request	Extended header present

Abbildung D.2.: Format des APL Frame Control Feldes

Frame Type Value b_1 b_0	Frame Type Name
00	Data
01	Command
10	Acknowledgement
11	Inter-PAN APS

Tabelle D.1.: Werte des APL Frame Type Feldes

Frame Type

Dieses Feld gibt den Typen des Frames an und kann auf einen der ersichtlichen Werte in Tabelle D.1 gesetzt werden.

Delivery Mode

Dieses Feld bestimmt wie der Frame gesendet wird. Die möglichen Werte dieses Feldes können aus Tabelle D.2 entnommen werden.

Ack Format

Dieses Feld gibt an, ob der Destination Endpoint, Cluster Identifier, Profile Identifier und Source Endpoint im Acknowledgement Frame angehängt werden.

Security

Dieses Feld gibt an, ob dem Header ein Auxiliary Header angehängt werden soll. Hat das Feld einen Wert von 0x1, wird ein AUX Header angehängt.

Delivery Mode Value b_1 b_0	Delivery Mode Name
00	Normal unicast delivery
01	Reserved
10	Broadcast
11	Group addressing

Tabelle D.2.: Werte des APL Delivery Mode Feldes

Acknowledgement Request

Dieses Feld bestimmt, ob der Empfänger des Frames ein Acknowledgment Frame senden sollen. Bei einem Wert von 0x1 wird ein Acknowledgement Frame vom Empfänger erwartet. Bei Frames, die via Broadcast oder Multicast gesendet werden, soll der Wert dieses Feldes immer 0x0 sein.

Extended Header Present

Dieses Feld bestimmt, ob das Extended Header Sub-Field im Application Header vorhanden ist. Ist der Wert des Feldes 0x1, wird dem Application Header ein Extended Header Sub-Field angehängt.

D.1.2. Destination Endpoint

Dieses Feld hat eine Länge von 8 Bit und spezifiziert die finale Destination des Frames. Dieses Feld wird nur im Application Header angehängt, wenn der Wert des Delivery Mode Feldes im Frame Control einen Wert von 0b0 (Normal Unicast) oder 0b10 (Broadcast) hat.

D.1.3. Group Address

Das Group Address Feld hat eine Länge von 16 Bit und wird nur im Application Header angehängt, wenn das Delivery Mode Feld im Frame Control einen Wert von 0b11 (Group Addressing) hat. Wenn dieses Feld im Application Header vorhanden ist, darf das Destination Endpoint Feld nicht angehängt werden.

D.1.4. Cluster Identifier

Das Cluster Identifier Feld hat eine Länge von 16 Bit und spezifiziert den Cluster, zu welchem der Frame gehört. Dieses Feld darf nur dann angehängt werden, wenn es sich bei dem Frame um ein Data oder Acknowledgement Frame handelt.

D.1.5. Profile Identifier

Das Profile Identifier Feld hat eine Länge von 16 Bit und spezifiziert das ZigBee Profil, welches für diesen Frame verwendet wird.

D.1.6. Source Endpoint

Das Source Endpoint Feld hat eine Länge von 8 Bit und bestimmt, welcher Endpoint den Frame ursprünglich gesendet hat. Ein Wert von 0x00 sagt aus, dass der Frame vom ZigBee Device Object (ZDO)

generiert wurde. Bei einem Wert von 0x01-0xFe wurde der Frame von einer Applikation auf dem Gerät generiert.

D.1.7. APS Counter

Dieses Feld hat eine Länge von 8 Bit und beinhaltet einen Frame Counter um das erneute Senden von Frames zu verhinder und somit vor Replay Angriffen zu schützen. Der Wert dieses Feldes soll mit jedem neuen Frame erhöht werden.

D.1.8. Extended Header

Das Extended Header Feld beinhaltet weitere Sub-Felder und muss wie in Abbildung D.3 ersichtlich formatiert sein.

Byte: 1	0/1	0/1
Extended frame control	Block number	ACK bitfield

Abbildung D.3.: Format des Extended Headers

Extended Frame Control

Das Extended Frame Control Feld hat eine Länge von 8 Bit und beinhaltet Informatione bezüglich dem Umgang mit Fragmentierung. Das Extended Frame Control Feld muss wie in Abbildung D.4 ersichtlich formatiert sein.

Bits: 0-1	2-7
Fragmentation	Reserved

Abbildung D.4.: Format des Extended Frame Control Feldes

Das Fragmentation Feld darf auf einen nicht reservierten Wert ersichtlich in Tabelle D.3 gesetzt werden.

Block Number

Das Block Number Feld hat eine Länge von 8 Bit und wird für die Kontrolle der Fragmentierung verwendet.

Wenn das Fragmentation Feld einen Wert von 0b00 hat, wird dieses Feld nicht angehänt. Wenn das Fragmentation Feld einen Wert von 0b01 hat, soll dieses Feld die Anzahl an Blöcken beinhalten, welche

Fragmentation Value b1 b0	Description
00	Transmission is not fragmented.
01	Frame is first fregment of a fragmented transmission.
10	Frame is part of a fragmented transmission but not the first part.
11	Reserved

Tabelle D.3.: Werte des Fragmentation Sub-Feldes

im Zuge der fragmentierten Übertragung übermittelt werden. Wenn das Fragmentation Feld einen Wert von 0b10 hat, soll dieses Feld die aktuelle Blocknummer beinhalten (0x01 für den ersten Block, 0x02 für den zweiten Block und so weiter).

Ack Bitfield

Dieses Feld hat eine Länge von 8 Bit und wird für APS Acknowledgement Frames verwenden um zu verifizieren, ob die einzelnen Blöcke erfolgreich empfangen wurden. Dieses Feld wird nur angehängt, wenn Acknowledgment Frames erwartet werden.

D.1.9. Frame Payload

Dieses Feld beinhaltet die Daten, welche im Zuge der Kommunikation übertragen werden sollen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] ZigBee Alliance, “Zigbee alliance homepage,” http://www.zigbee.org/, o.D., zugegriffen am: 04. Jänner 2018.

[2] ——, “Zigbee 3.0,” http://www.zigbee.org/zigbee-for-developers/zigbee-3-0/, o.D., zugegriffen am: 05. Jänner 2018.

[3] ——, *ZigBee Pro 2015 Specification*, 2015.

[4] Z-Wave, “Z-wave homepage,” http://www.z-wave.com/, o.D., zugegriffen am: 01. Juni 2018.

[5] Thread, “Thread homepage,” https://www.threadgroup.org/, o.D., zugegriffen am: 01. Juni 2018.

[6] T. Zillner, “Zigbee exploited - the good, the bad and the ugly,” 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[7] X. Fan, “Security analysis of zigbee,” 2017. [Online]. Available: https://courses.csail.mit.edu/6.857/2017/project/17.pdf

[8] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, “Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, Oct 2016.

[9] Praetorian, “Internet of things map,” https://p16.praetorian.com/iotmap/#14/30.2679/-97.7440, o.D., zugegriffen am: 18. Jänner 2018.

[10] Texas Instruments, “What’s new in zigbee 3.0,” 2018, zugegriffen am: 13. Mai 2018. [Online]. Available: http://processors.wiki.ti.com/index.php/What’s_New_in_ZigBee_3.0

[11] IEEE Standard for Information Technology, “Ieee standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans),” *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.

[12] NXP, *ZigBee 3.0 Stack User Guide*, 2016. [Online]. Available: https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf

[13] ZigBee Alliance, *ZigBee Specification*, 2012.

[14] ——, "Application level standardization," http://www.zigbee.org/zigbee-for-developers/applicationstandards/, o.D., zugegriffen am: 31. Mai 2018.

[15] ——, *ZigBee Cluster Library Specification*, 2016.

[16] ——, *ZigBee Light Link Standard*, 2012.

[17] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: Attacking zigbee 3.0 via touchlink commissioning," https://www1.cs.fau.de/filepool/publications/wisec2017_touchlink.pdf, 2017, abgerufen am: 11. August 2018.

[18] SmartThings, "How to reset zigbee bulbs," https://support.smartthings.com/hc/en-us/articles/213137623-How-to-reset-ZigBee-bulbs, o.D., zugegriffen am: 11. August 2018.

[19] SmartThings . Zigbee ïnsecure rejoin"faq. Zugegriffen am: 05.11.2018. [Online]. Available: https://support.smartthings.com/hc/en-us/articles/208201243-ZigBee-Insecure-Rejoin-FAQ

[20] IEEE Standard for Information Technology. oui.txt. Abgerufen am: 15.08.2018. [Online]. Available: http://standards-oui.ieee.org/oui.txt

[21] ——. Ieee standards association. Zugegriffen am: 15.08.2018. [Online]. Available: http://standards.ieee.org/index.html

[22] ZigBee Alliance. Zigbee certified products. Zugegriffen am: 08.06.2018. [Online]. Available: https://www.zigbee.org/zigbee-products-2/

[23] Philips. Zigbee 3.0 support in hue ecosystem. Zugegriffen am: 19.08.2018. [Online]. Available: https://developers.meethue.com/zigbee3

[24] Great Scott Gadgets. Hackrf one. Zugegriffen am: 17.08.2018. [Online]. Available: https://greatscottgadgets.com/hackrf/

[25] Texas Instruments. Cc2531 usb evaluation module kit. Zugegriffen am: 17.08.2018. [Online]. Available: http://www.ti.com/tool/CC2531EMK

[26] Cononical Ltd. (o.D.) Ubuntu homepage. Zugegriffen am: 06.01.2019. [Online]. Available: https://www.ubuntu.com/

[27] (2018) Ubuntu releases. [Online]. Available: https://wiki.ubuntu.com/Releases

[28] GNURadio. Gnuradio homepage. Zugegriffen am: 17.08.2018. [Online]. Available: https://www.gnuradio.org/

[29] bastibl. Ieee 802.15.4 zigbee transceiver. Zugegriffen am: 17.08.2018. [Online]. Available: https://github.com/bastibl/gr-ieee802-15-4

[30] T. Schmid, "Gnu radio 802.15.4 en- and decoding," 2006.

[31] GNURadio. Pybombs. Zugegriffen am: 17.08.2018. [Online]. Available: https://github.com/gnuradio/pybombs

[32] Mobius Consulting. (o.D.) Avoiding rf interference between wifi and zigbee. Zugegriffen am: 11.09.2018. [Online]. Available: https://www.mobiusconsulting.com/papers/ZigBeeandWiFiInterference.pdf

[33] mitshell. 802.15.4 monitor. Zugegriffen am: 10.07.2018. [Online]. Available: https://github.com/mitshell/CC2531

[34] IEEE Standard for Information Technology, "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac)and physical layer (phy) specifications amendment 5: Enhancements for higher throughput," *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, pp. 1–565, Oct 2009.

[35] G. Baddeley. (2001) Gps - nmea sentence information. Zugegriffen am: 04.11.2018. [Online]. Available: http://aprs.gids.nl/nmea/

[36] Not In The Manual. (2008) Convert nmea latitude & longitude to decimal. Zugegriffen am: 01.07.2018. [Online]. Available: http://notinthemanual.blogspot.com/2008/07/convert-nmea-latitude-longitude-to.html

[37] WAREMA electronic GmbH, "Homepage," https://www.warema.at/, o.D., zugegriffen am: 07. November 2018.

[38] Silicon Labs. (o.D.) Homepage. Zugegriffen am: 07. November 2018. [Online]. Available: https://www.silabs.com/products/wireless/mesh-networking/zigbee

[39] Viconics Electronics Inc. . (o.D.) Homepage. Zugegriffen am: 07. November 2018. [Online]. Available: http://www.viconics.com/

[40] OSRAM GmbH . (o.D.) Homepage. Zugegriffen am: 07. November 2018. [Online]. Available: https://www.osram.de/cb/lightify/lightify-pro/lightify_pro_system.jsp

[41] IEEE Standard for Information Technology, "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans)," *IEEE Std 802.15.4-2003*, pp. 0_1–670, 2003.