Fakultät Informatik/Mathematik

HOCHSCHULE FÜR
TECHNIK UND WIRTSCHAFT
DRESDEN
UNIVERSITY OF APPLIED SCIENCES

Sensornetze

LoRa / LoRaWAN

Salaml

Wintersemester 2021/2022

Inhaltsverzeichnis

Symbolverzeichnis

Bezeichnung	Beschreibung
B	Bandbreite der Signalübertragung
CR	Code Rate für Fehlerkorrektur
f_{max}	maximale Frequenz des Chirps bei der Signalübertragung
f_{min}	minimale Frequenz des Chirps bei der Signalübertragung
R_b	Bitrate der Signalübertragung
$R_{b,netto}$	Nettobitrate der Signalübertragung
R_c	Chiprate der Signalübertragung
R_s	Symbolrate der Signalübertragung
SF	Spreading Factor der Signalübertragung

Abkürzungsverzeichnis

Bezeichnung	Beschreibung
ABP	Activation by Personalization
ADR	Adaptive Data Rate
CRC	Cyclic Redundancy Check
ISM	Industrial, Scientific and Medical Band
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
OTAA	Over-The-Air-Activation
SF	Spreading Factor
SNR	Signal-Rausch-Verhältnis
SRD	Short Range Device Band
TTN	The Things Network

Glossar

Activation by Personalization

Aktivierung des Node im LoRaWAN mit vorberechneten Sitzungsschlüsseln

Adaptive Data Rate

Verfahren zur Optimierung von Airtime, Energiebedarf und Reichweite bei Long Range Wide Area Network (LoRaWAN)

Airtime

Dauer, welche zum Senden einer Nachricht benötigt wird

Applikationsserver

Schnittstelle zwischen LoRaWAN und Anwendungen

Chirp

Signal steigender oder fallender Frequenz mit konstanter Amplitude

Chirp Spread Spectrum

Modulationsverfahren unter Verwendung von Chirps

Cyclic Redundancy Check

Prüfwert für Fehlererkennung oder -korrektur

Downlink

Nachricht von LoRaWAN-Anwendung via Gateway an Node

Gateway

Schnittstelle zwischen LoRa-Kommunikation und Netzwerkserver im LoRaWAN

Industrial, Scientific and Medical Band

lizenzfrei nutzbare Frequenzbereiche

Join-Server

Server für Schlüsselverwaltung und -verteilung im LoRaWAN

Long Range

proprietärer Funkstandard mit Fokus auf hoher Reichweite bei geringem Energiebedarf

Long Range Wide Area Network

auf Energiesparsamkeit bei der Datenübertragung ausgelegtes Weitverkehrsnetzwerk unter Nutzung des Funkstandards LoRa

Netzwerkserver

zentrales Element für Routing von Nachrichten zwischen Gateways und Applikationsserver im LoRaWAN

Node

Endgerät im LoRaWAN, kann per LoRa Daten senden und empfangen

Over-The-Air-Activation

Aktivierung des Node im LoRaWAN über Join-Prozess mit dynamischer Berechnung Sitzungsschlüssel

Payload

Nutzdaten zwischen verschiedenen Objekten, das heißt ohne Steuer- und Protokollinformationen

Short Range Device Band

lizenzfreies Frequenzband für Übertragungen über kurze Reichweiten bzw. geringer Leistung

Signal-Rausch-Verhältnis

Maß für die Qualität des Nutzsignals bei einer Datenübertragung

Spreading Factor

steuert Übertragunsrate und Airtime bei LoRa-Übertragung

The Things Network

weltweites, offenes und communitybasiertes LoRaWAN

Uplink

Nachricht von Node via Gateway an LoRaWAN-Anwendung

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Das Internet of Things (IoT) ist nicht nur in der IT-Branche ein aktuelles Thema sondern dringt auch immer mehr in die Welt von Otto Normalverbraucher vor. Das Einstellen der Heizkörpertemperaturen, Schalten von Steckdosen oder Protokollieren von Messwerten wie Temperatur oder Feinstaubgehalt der Luft über das Internet ist für viele Menschen bereits Normalität. Das The Things Network (TTN) bildet einen für jeden nahezu frei nutzbaren Zugang zum Internet of Things mit großer räumlicher Abdeckung.

Grundlage des TTN bildet das Ökosystem aus LoRa und LoRaWAN. LoRa ist dabei eine Funktechnologie, die zur Übertragung von Daten über große Distanzen mit wenig Energieaufwand verwendet wird. Mittels LoRaWAN können Geräte, die LoRa beherrschen, in ein Netzwerk eingebunden werden und damit Teil des Internet of Things werden. Kernelement von LoRa und LoRaWAN ist dabei ein möglichst niedriger Energiebedarf der Endgeräte.

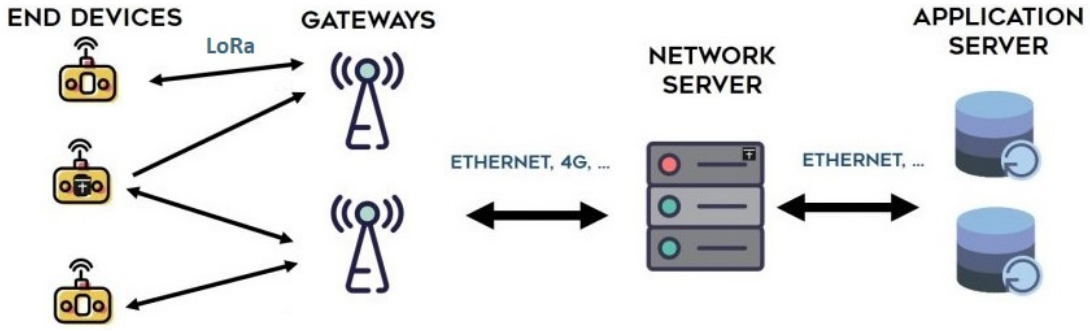

Abbildung 1.1: Architektur von LoRaWAN (vereinfacht)
Quelle: bearbeitet aus Zerynth srl,
https://www.zerynth.com/wp-content/uploads/2017/05/lorawan-architecture.jpg

Anhand von Abbildung 1.1 soll die Abgrenzung von LoRa und LoRaWAN verdeutlicht werden. Über LoRa wird lediglich zwischen den Endgeräten und den Gateways kommuniziert, den Schnittstellen zum weiteren Netzwerk. Jegliche weitere Kommunikation wird über das Internet abgewickelt. Die gesamte Abbildung stellt das LoRaWAN dar, LoRa ist nur die Funktechnologie die auf der untersten Netzebene genutzt wird.

In den folgenden Kapiteln wird zunächst näher auf LoRa als Grundlage der Kommunikation eingegangen, anschließend wird die Vernetzung der Geräte zum LoRaWAN erläutert.

2 LoRa

2.1 Grundlagen

LoRa ist ein proprietäres Übertragungsverfahren per Funk. Es wurde vom Unternehmen Semtech entwickelt, um Kommunikation mit niedrigem Energiebedarf über große Distanzen zu ermöglichen. Im Vergleich zu anderen Funktechnologien wie Bluetooth oder Mobilfunk, ist die „Bandbreite“ der Datenübertragung (Datenrate) bei LoRa nur gering. Dagegen ist die erzielbare Reichweite größer, wie Abbildung 2.1 zeigt. [Sem]

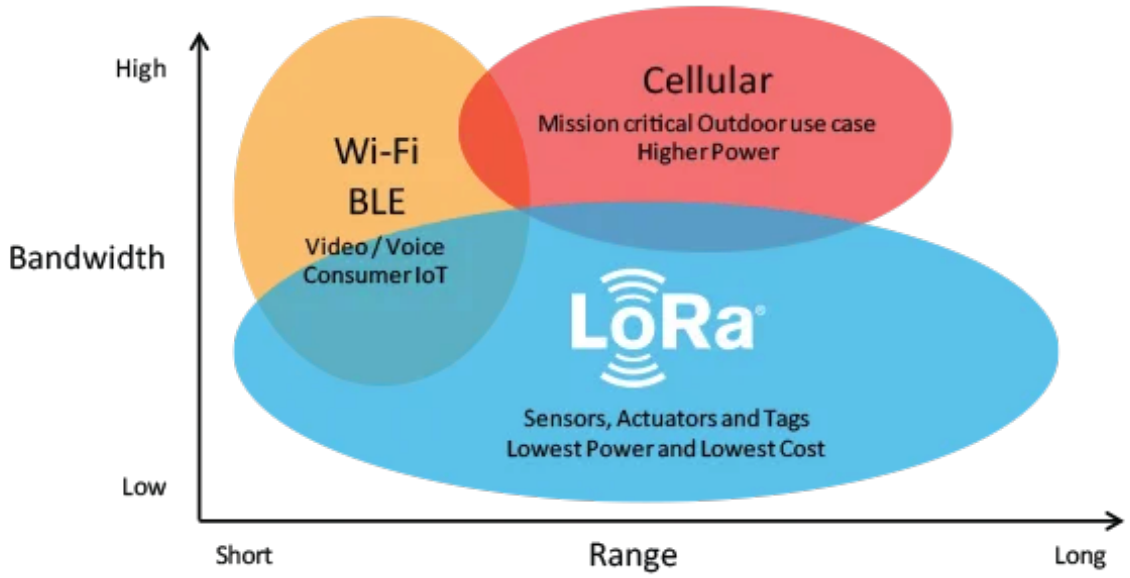

Abbildung 2.1: Bandbreite (Datenrate) und Reichweite von LoRa im Vergleich zu anderen Funktechnologien
Quelle: The Things Industries,
https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/bandwidth-vs-range.png

Für LoRa werden ortsabhängig Frequenzbereiche aus lizenzfreien Bändern genutzt (Industrial, Scientific and Medical Band (ISM), Short Range Device Band (SRD)). In Europa kommt das SRD-Band um 868 MHz zum Einsatz. LoRa nutzt hierbei mehrere Kanäle auf verschiedenen Frequenzen. [LoR21] Obwohl es sich hierbei um ein freies Frequenzband handelt, sind dennoch einige Einschränkungen zu beachten:[Eri18]

- Sendeleistung Uplink begrenzt auf 25 mW (14 dBm)
- Sendeleistung Downlink begrenzt auf 500 mW (27 dBm)
- Duty Cycle Senden pro Gerät begrenzt auf kanalabhängig 0,1% bzw. 1%

Diese Grenzen sind gesetzlich festgelegt, um eine Blockade des Bandes unter anderem durch zu häufiges Senden zu verhindern. Damit ist jedem eine faire Verwendung dieses Bandes unter Beachtung der Grenzen möglich.

Um insbesondere die Begrenzung der Sendezeit einzuhalten zu können, sollte eine Minimierung der Sendezeit (Airtime) erfolgen.

2.2 Modulation Chirp Spread Spectrum

Per LoRa gesendete Signale werden mittels des Verfahrens Chirp Spread Spectrum moduliert. Grundlage dieser Modulation sind sogenannte Chirps. Eine Anpassung der Datenrate ist über den sogenannten Spreading Factor (SF) möglich.

2.2.1 Chirps

Ein Chirp ist ein Impuls mit konstanter Amplitude und sich ändernder Frequenz. Bei steigender Frequenz wird der Chirp als Upchirp bezeichnet, bei fallender als Downchirp. In Abbildung 2.2 ist ein Upchirp mit linearem Anstieg der Frequenz veranschaulicht.

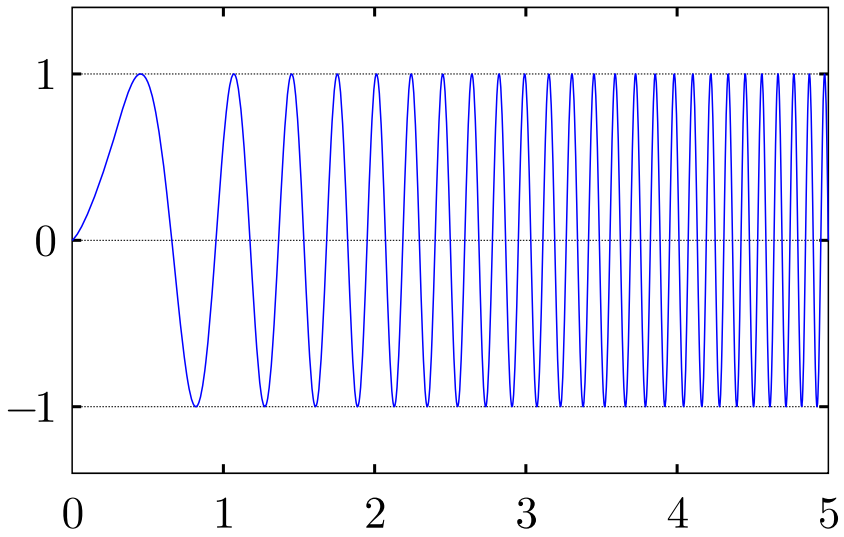

Abbildung 2.2: Upchirp mit linearem Frequenzanstieg
Quelle: Georg-Johann, CC BY-SA 3.0, via Wikimedia Commons,
https://commons.wikimedia.org/wiki/File:Linear-chirp.svg

Die Änderung der Frequenz der Chirps erfolgt nicht kontinuierlich, sondern zu diskreten Zeitpunkten. Ein einzelner Zustand heißt dabei Chip, die Anzahl an Frequenzänderungen pro Zeiteinheit wird als Chiprate R_c bezeichnet. Bei LoRa entspricht dies der von den Chirps genutzten Bandbreite B (üblicherweise 125 kHz). [Sem15, S. 10]

$$R_c = B = 125\,\mathrm{kHz} \tag{2.1}$$

2.2.2 Symbole

Zur Kodierung von Daten wird ein Chirp zeitlich verschoben und bildet damit ein sogenanntes Symbol. Die Startfrequenz des Symbols legt dabei die kodierten Daten fest. Nachdem die Frequenz des Chirps innerhalb des Symbols die Grenze der Bandbreite erreicht hat, wird der Chirp mit der Frequenz der anderen Bereichsgrenze fortgesetzt (Upchirp: Sprung von f_{max} zu f_{min}, Downchirp: Sprung von f_{min} zu f_{max}). [Ghob]

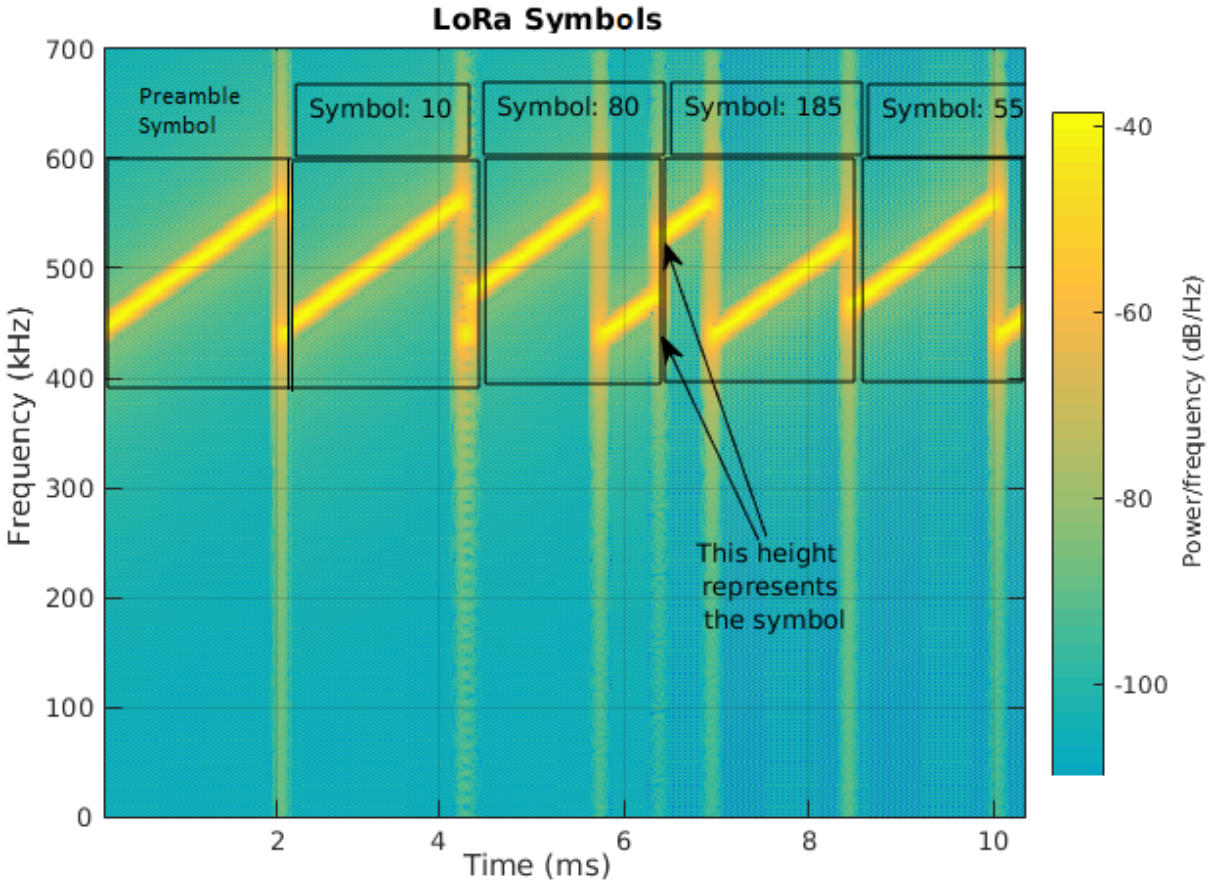

Abbildung 2.3: Spektrum verschiedener LoRa-Symbole
Quelle: bearbeitet aus Sakshama Ghoslya, https://www.sghoslya.com/p/lora_9.html

In Abbildung 2.3 ist der Frequenzgang verschiedener Symbole anhand des Spektrums veranschaulicht. Innerhalb der Symbole ist jeweils der Sprung von der maxima-

len Frequenz f_{max} zur minimalen Frequenz f_{min} und damit der Lauf über den kompletten Frequenzbereich erkennbar. Innerhalb eines Symbols wird dementsprechend immer die komplette Bandbreite genutzt, lediglich die Startfrequenz unterscheidet sich nach den kodierten Daten. Aufgrund dieser Verteilung des Signals über das Spektrum wird das Modulationsverfahren Chirp Spread Spectrum genannt.

Die Anzahl der Symbole pro Zeiteinheit wird als Symbolrate R_s bezeichnet.

2.2.3 Spreading Factor (SF)

Die Dauer und der Informationsgehalt der Symbole kann über denn sogenannten Spreading Factor SF eingestellt werden. Dieser gibt die Anzahl Bits an, die in einem Symbol kodiert werden können. Für die Symbolrate gilt die in Gleichung 2.2 dargestellte Beziehung. Da mit jedem Symbol SF Bits kodiert werden, lässt sich daraus die in Gleichung 2.3 dargestellte Bitrate R_b ableiten. [Sem15, S. 10]

$$R_s = \frac{B}{2^{SF}} = \frac{R_c}{2^{SF}} \tag{2.2}$$

$$R_b = SF * R_s = SF * \frac{B}{2^{SF}} = SF * \frac{R_c}{2^{SF}} \tag{2.3}$$

Bei Erhöhung des Spreading Factors um 1 halbiert sich damit die Symbolrate, die Dauer der Symbole verdoppelt sich. In Abbildung 2.4 ist die Verdopplung der Zeitdauer bei Erhöhung des Spreading Factors deutlich erkennbar.

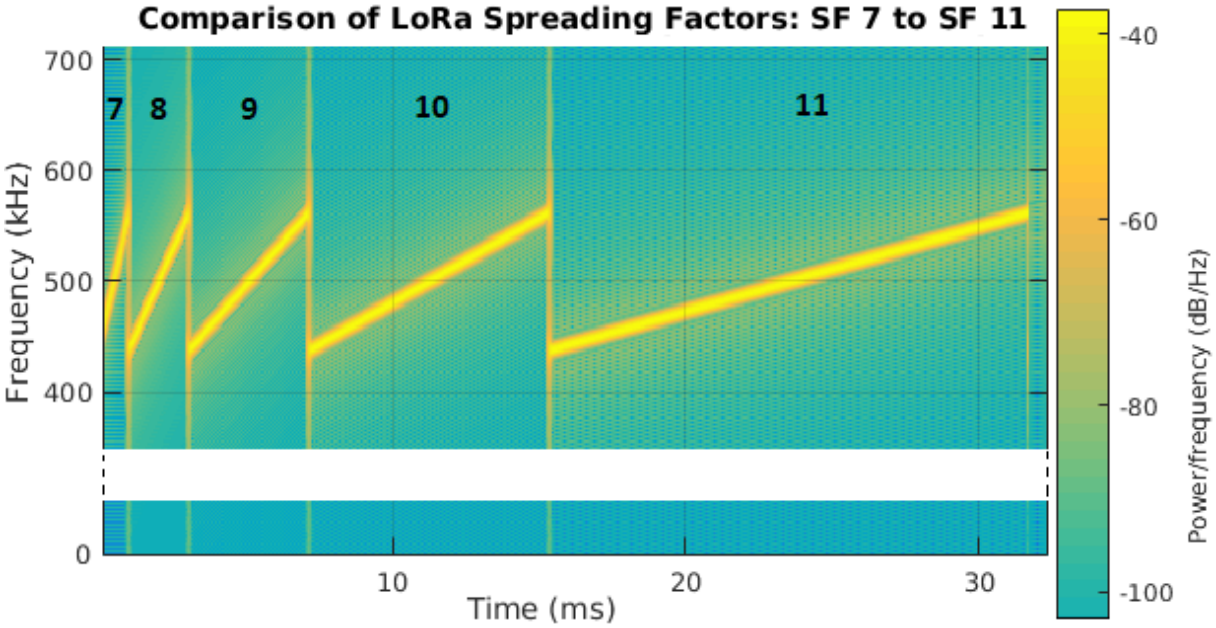

Abbildung 2.4: Spektrum verschiedener Spreading Factors
Quelle: bearbeitet aus Sakshama Ghoslya,
https://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html

LoRa-Empfänger weisen eine bessere Empfindlichkeit gegenüber Signalen mit höherem Spreading Factor auf, wie in Tabelle 2.1 dargestellt. Eine Erhöhung des Sprea-

Spreading Factor	Empfindlichkeit	Airtime
SF7	-123,0 dBm	41 ms
SF8	-126,0 dBm	72 ms
SF9	-129,0 dBm	144 ms
SF10	-132,0 dBm	288 ms
SF11	-134,5 dBm	577 ms
SF12	-137,0 dBm	991 ms

Tabelle 2.1: Empfindlichkeit und Airtime verschiedener Spreading Factors
Quelle: Semtech Corporation,
https://lora-developers.semtech.com/documentation/tech-papers-and-guides/understanding-adr

ding Factors führt damit zu folgenden Effekten:

- Airtime Sender erhöht
- Energiebedarf Sender erhöht
- Empfindlichkeit Empfänger verbessert
- Übertragungsreichweite erhöht

Für diese Werte gelten jedoch unterschiedliche Ziele: Airtime und Energiebedarf sollten minimiert werden, Empfindlichkeit und Reichweite maximiert werden.[Ade+17] Um einen bestmöglichen Kompromiss zwischen diesen Vorgaben zu schaffen, implementiert LoRaWAN die in Abschnitt 3.5 beschriebene automatische Anpassung des Spreading Factors.

2.2.4 Code Rate (CR)

Um die korrekte Dekodierung des Signals durch den Empfänger auch bei schlechtem Signalempfang oder Störungen zu gewährleisten, gibt es eine Fehlerkorrektur. Dabei werden zu je 4 Bit Nutzdaten 1 bis 4 Fehlerkorrekturbits hinzugefügt. Die Anzahl Fehlerkorrekturbits pro 4 Nutzdatenbits wird als Code Rate CR bezeichnet. Üblich sind auch die Bezeichnungen 4/5, 4/6, 4/7 und 4/8.

Durch die zusätzlichen Datenbits verringert sich die Nettodatenrate $R_{b,netto}$ entsprechend Gleichung 2.4.

$$R_{b,netto} = R_b * \frac{4}{4+CR} = SF * \frac{B}{2^{SF}} * \frac{4}{4+CR} \tag{2.4}$$

2.2.5 Orthogonalität

Um gleichzeitig störungsfrei verschiedene Nachrichten per LoRa zu übertragen, müssen die Signale orthogonal zueinander sein. Dies ist dann der Fall, wenn die Anstiege der Frequenzen (bezogen auf die Zeit) unterschiedlich sind. In Abbildung 2.4 sind beispielsweise alle Signale jeweils orthogonal zueinander, da sie verschiedene Anstiege aufweisen. Signale verschiedener Spreading Factors und gleicher Bandbreite können daher gleichzeitig störungsfrei gesendet und empfangen werden. [Ghoa]

2.3 LoRa-Nachricht

Eine per LoRa gesendete Nachricht besteht aus den folgenden Elementen:[Ade+17]

- Präambel
- Header + Cyclic Redundancy Check (CRC) für Header
- Nutzdaten
- CRC

Die Präambel dient zur Synchronisation des Empfängers auf die gesendeten Daten. Anhand der Präambel wird außerdem der Spreading Factor erkannt, mit welcher die Daten gesendet wurden. Der Header enthält unter anderem Informationen zur Länge der Nutzdaten. Im Header wird die größtmögliche Code Rate verwendet, um die Daten auch bei starken Störungen fehlerfrei dekodieren zu können. Am Ende der Nachricht folgt optional ein CRC-Wert zu Fehlerdetektion bzw. -korrektur.

3 LoRaWAN

Mittels LoRaWAN können über LoRa kommunizierende Endgeräte in ein Netzwerk eingebunden werden und bilden damit ein Wide Area Network (WAN). LoRaWAN gibt dabei die Systemarchitektur und die zur Kommunikation genutzten Protokolle vor.

3.1 Architektur

Der grundlegende Architektur von LoRaWAN ist in Abbildung 3.1 dargestellt. Die Komponenten sind von links nach rechts mit steigender Abstraktion von der eigentlichen LoRa-Kommunikation angeordnet. Eine Nachricht vom Endgerät zur Applikation hin wird als Uplink, eine Nachricht von der Applikation zum Endgerät hin als Downlink bezeichnet. [Thed]

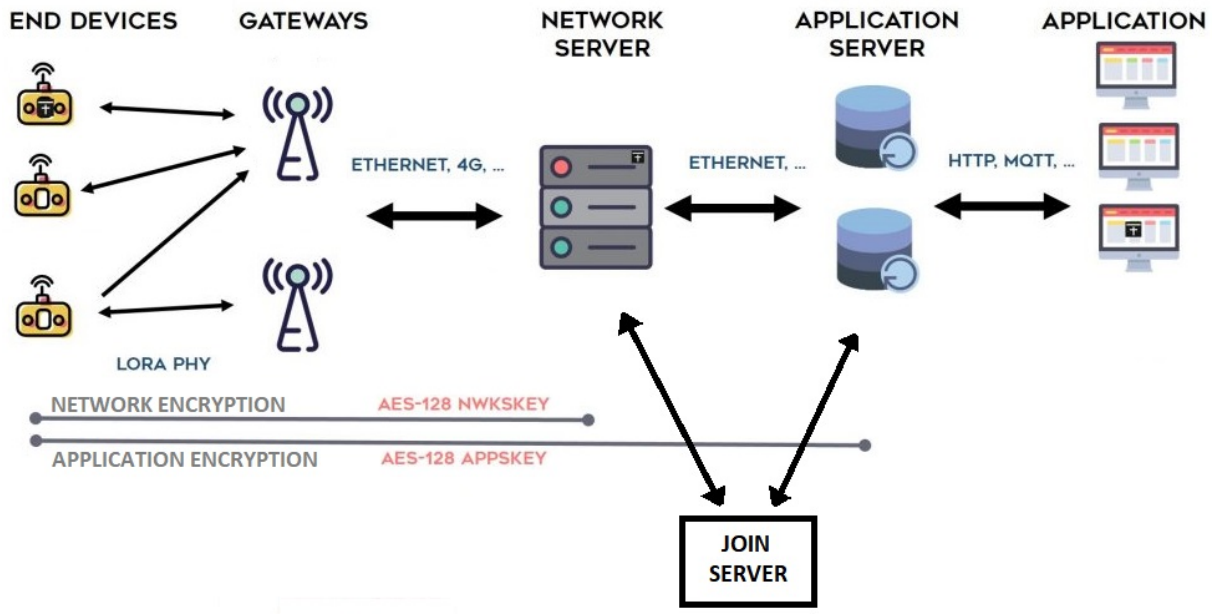

Abbildung 3.1: Systemarchitektur bei LoRaWAN
Quelle: bearbeitet aus Zerynth srl,
https://www.zerynth.com/wp-content/uploads/2017/05/lorawan-architecture.jpg

Im folgenden werden die einzelnen Komponenten von LoRaWAN näher erläutert und jeweils deren Verhalten bei einem Up- und Downlink beschrieben.

3.1.1 Endgerät

Endgeräte, auch als Nodes bezeichnet, werden über das LoRaWAN vernetzt und können Daten zur Applikation senden bzw. von dieser empfangen. Nodes kommunizieren ausschließlich über LoRa mit dem LoRaWAN, müssen also über die dafür notwendige Hardware (LoRa-Chip, Antenne) verfügen. Häufig sind Nodes auf besonders energiesparsamen Betrieb ausgelegt und batteriebetrieben. Um die in Abschnitt 2.1 beschriebenen gesetzlichen Vorgaben einzuhalten, sind die Sendeintervalle vergleichsweise hoch (Minuten bis Stunden oder Tage).

Uplink

Ein Node kann Daten per LoRa senden. Dazu wird auf die Nutzdaten (Payload) zuerst die Applikationsverschlüsselung angewendet, darauf wiederum die Netzwerkverschlüsselung. Per LoRa gesendete Pakete können von allen Nodes und Gateways im Sendebereich empfangen werden.

Downlink

Nodes können in verschiedene Geräteklassen eingeteilt werden (siehe Abschnitt 3.4) und sind davon abhängig zu unterschiedlichen Zeiten empfangsbereit. Wird während eines Empfangsfensters eine an den Node adressierte Nachricht vom Gateway empfangen, so erfolgt die Entfernung der verschiedenen Verschlüsselungsschichten und anschließend die Verarbeitung der Nutzdaten.

3.1.2 Gateway

Ein Gateway bildet die Schnittstelle zwischen der Funkkommunikation per LoRa und den restlichen Komponenten des Netzwerks. LoRa zur Datenübertragung wird somit lediglich zwischen Endgeräten und Gateways genutzt.

In einem LoRaWAN können beliebig viele Gateways genutzt werden. Durch hinzufügen von Gateways an bisher wenig nicht oder schlecht angebundenen Orten, kann auf einfache Weise die Netzabdeckung verbessert werden.

Uplink

Ein Gateway empfängt die von den Endgeräten über LoRa gesendeten Nachrichten. Außerdem werden Metadaten wie Signalstärke und Signal-Rausch-Verhältnis (SNR)

der empfangenen Signale bestimmt. Die Nutzdaten der LoRa-Nachricht und die Metadaten werden vom Gateway an den Netzwerkserver weitergeleitet, üblicherweise per Internet.

Downlink

Ebenso kann das Gateway Daten vom Netzwerkserver empfangen. Diese werden per LoRa gesendet und können von Endgeräten in Reichweite des Gateways empfangen werden.

3.1.3 Netzwerkserver

Der Netzwerkserver bildet im LoRaWAN das zentrale Element für das Routing der von Endgeräten empfangenen und an diese zu sendenden Nachrichten. Es gibt genau einen Netzwerkserver im LoRaWAN.

Uplink

Der Netzwerkserver verarbeitet die von den Gateways empfangenen Nachrichten. Wie in Abbildung 3.1 unten links dargestellt, kann die gesendete Nachricht eines Endgeräts von mehreren Gateways gleichzeitig empfangen werden. Dabei leitet jedes Gateway die Nachricht an den Netzwerkserver weiter. Durch Vergleich des (teilw. verschlüsselten) Dateninhalts der Nachricht können mehrfach empfangene Nachrichten im Netzwerkserver zu einer einzigen Nachricht zusammengefasst werden. Dies wird auch als Deduplizierung bezeichnet.

Außerdem wird für jedes Endgerät gespeichert, über welches Gateway die Signalqualität der empfangenen Daten am besten ist.

Sofern das Endgerät, von dem die Nachricht empfangen wurde, im Netzwerk aktiviert ist (siehe Abschnitt 3.3), kann die Netzwerkverschlüsselung der Nachricht entfernt werden. Die entschlüsselten Daten werden an den Applikationsserver weitergeleitet, der für dieses Endgerät festgelegt wurde.

Downlink

Ebenso kann der Netzwerkserver Downlinkpakete vom Applikationsserver empfangen. Diese werden zunächst in einer Warteschlange gespeichert (Downlink-Queue). Abhängig von der Geräteklasse des adressierten Endgeräts erfolgt die weitere Verarbeitung direkt oder durch bestimmte Auslöser (siehe Abschnitt 3.4). In der Weiterverarbeitung werden die Paketdaten zunächst der Netzwerkverschlüsselung unterzogen.

Außerdem wird für das adressierte Endgerät das Gateway bestimmt, welches aktuell wahrscheinlich die besten Übertragungsbedingungen zum Endgerät hat. Dies wird anhand der gespeicherten Daten über die Signalqualität vorheriger Uplinks durchgeführt. Anschließend werden die verschlüsselten Daten an das ermittelte Gateway weitergeleitet. Ein Paket im Downlink wird also immer nur über genau ein Gateway gesendet.

3.1.4 Applikationsserver

Ein Applikationsserver dient der Ent- bzw. Verschlüsselung der Applikationsdaten und ist die Schnittstelle des LoRaWAN zu den eigentlichen Anwendungen. Im LoRaWAN kann es beliebig viele Applikationsserver geben.

Uplink

Ein Applikationsserver empfängt vom Netzwerkserver gesendete Daten. Dabei wird zunächst die Applikationsverschlüsselung entfernt. Anschließend sind die eigentlichen vom Endgerät gesendeten Daten (Payload) im Klartext verfügbar und können beliebig verarbeitet werden. Die Metadaten der LoRa-Kommunikation, welche durch die Gateways erfasst wurden (z. B. SNR), sind ebenso Bestandteil der im Applikationsserver verfügbaren Daten. Die weitere Verarbeitung der Uplinks ist allerdings nicht mehr Bestandteil der Architektur von LoRaWAN.

Downlink

Im Applikationsserver können außerdem Downlinks gestartet werden, also Nachrichten zum Endgerät gesendet werden. Dabei werden die Daten der Applikationsverschlüsselung unterzogen und das Paket an den Netzwerkserver gesendet.

3.1.5 Join-Server

Damit eine Kommunikation mit Endgeräten im LoRaWAN möglich ist, müssen diese aktiviert werden (siehe Abschnitt 3.3). Ein Teil des Aktivierungsprozesses erfolgt dabei über den Join-Server, insbesondere die Verteilung der Sitzungsschlüssel für die Netzwerk- und Applikationsverschlüsselung. Im Join-Server wird außerdem der Root-Key für die Verschlüsselung verwaltet, aus dem die genannten Sitzungsschlüssel abgeleitet werden. Der Join-Server bildet damit ein wichtiges Element zur Sicherstellung der verschlüsselten Kommunikation. Daher ist dieser insbesondere aus dem Netzwerk-

server ausgegliedert, um ein Mitlesen der Applikationsdaten durch den Betreiber des Netzwerkserver zu verhindern.

Im LoRaWAN kann es beliebig viele Join-Server geben, die Zuordnung eines Endgeräts zu einem Join-Server muss allerdings eindeutig sein.

3.2 Verschlüsselung

Nachrichten im LoRaWAN verfügen über mehrere Schichten der Verschlüsselung, um nur denjenigen Komponenten Zugriff auf Daten zu gewähren, wie zum Betrieb des Netzwerks notwendig sind. Im folgenden sind die Schritte für einen Uplink beschrieben, im Falle eines Downlinks ist die Reihenfolge entsprechend umgekehrt und Ver- und Entschlüsselung sind vertauscht. Die Anwendungsdaten (Payload) werden mit dem 128 Bit-AES-Applikationssitzungsschlüssel im Endgerät verschlüsselt. Diese verschlüsselten Daten werden (zusammen mit weiteren für den Netzwerkserver relevanten Daten) im Endgerät mit dem 128 Bit-AES-Netzwerksitzungsschlüssel verschlüsselt und (ergänzt um zur Adressierung notwendige Daten) per LoRa gesendet. Geräte, die diese ausgesendeten Daten mithören, haben aufgrund der Verschlüsselung keinen Zugriff auf die Daten, lediglich die Geräteadresse wird unverschlüsselt übertragen. Auch Gateways können den Inhalt der durch sie weitergeleiteten Pakete nicht mitlesen. Im Netzwerkserver erfolgt die Entschlüsselung mit dem Netzwerksitzungsschlüssel und der Netzwerkserver erhält Zugriff auf die benötigten Daten. Die Anwendungsdaten sind allerdings weiterhin verschlüsselt und somit nicht durch den Netzwerkserver lesbar. Im Applikationsserver erfolgt schlussendlich die Entschlüsselung mit dem Applikationssitzungsschlüssel. Damit erhält neben dem Endgerät nur der Applikationsserver Zugriff auf die Anwendungsdaten.

3.3 Aktivierung

Damit ein Endgerät im LoRaWAN erfolgreich kommunizieren kann, muss es aktiviert sein. Die Aktivierung dient insbesondere dazu, die für die Ver- und Entschlüsselung notwendigen Sitzungsschlüssel an die zuständigen Komponenten zu verteilen und dem Endgerät eine in diesem LoRaWAN eindeutige Adresse zuzuweisen. Im folgenden werden die beiden verfügbaren Aktivierungsmethoden beschrieben. In Tabelle 3.1 sind diese zum Vergleich dargestellt. [Thec]

	Activation by Personalization (ABP)	Over-the-Air Activation (OTAA)
Sitzung	eine statische Sitzung	dynamisch, beliebig oft neu
Schlüssel	Sitzungsschlüssel fest einprogrammiert	Aushandlung für Sitzung, Ableitung aus Root-Key
Beitritt	Kommunikation direkt möglich	Beitrittsprozess nötig
Sicherheit	geringer	hoch

Tabelle 3.1: Vergleich der Methoden für die Aktivierung von Endgeräten

3.3.1 Activation by Personalization (ABP)

Bei Activation by Personalization (ABP) werden die Sitzungsschlüssel vor Inbetriebnahme des Geräts berechnet und eine freie Geräteadresse bestimmt. Diese statischen Sitzungsdaten werden zum einen fest in das Endgerät einprogrammiert und zum anderen an die zuständigen Server verteilt (Netzwerksitzungsschlüssel und Geräteadresse an Netzwerkserver, Applikationssitzungsschlüssel an Applikationsserver). Damit wurde eine Sitzung etabliert und eine Kommunikation mit diesem Gerät ist sofort möglich.

Nachteil von ABP ist die eingeschränkte Sicherheit, da bei Kompromittierung der Schlüssel keine neue Sitzung mit anderen Schlüsseln gestartet werden kann und die Verschlüsselung dann gebrochen ist. ABP wird vor allem beim Debugging während der Entwicklung von Endgeräten eingesetzt, da nach einem Neustart direkt ohne einen Aktivierungsprozess kommuniziert werden kann.

3.3.2 Over-the-Air Activation (OTAA)

Bei Over-The-Air-Activation (OTAA) erfolgen die Berechnung der Sitzungsschlüssel und die Zuweisung der Geräteadresse dynamisch. Dabei wird vor Inbetriebnahme des Geräts eine (möglichst) weltweit eindeutige ID für das Gerät (DevEUI) und ein Root-Key festgelegt. Diese Daten werden im Gerät fest einprogrammiert und im Join-Server hinterlegt. Im Gerät wird außerdem die ID des zuständigen Join-Servers (JoinEUI) hinterlegt.

Zur Aktivierung wird der in Abbildung 3.2 dargestellte Beitrittsprozess durchlaufen. Das Endgerät sendet seine Geräte-ID DevEUI und die ID des Join-Servers JoinEUI unverschlüsselt an das Netzwerk. Anhand der JoinEUI erfolgt im Netzwerkserver die Weiterleitung an den zuständigen Join-Server. Dieser wählt eine zufällige Nonce und berechnet daraus anhand des für dieses Endgerät hinterlegten Root-Keys neue Sitzungsschlüssel. Diese Sitzungsschlüssel werden vom Join-Server an die jeweils dafür zuständigen Server verteilt. Der Netzwerkserver bestimmt eine für diese Sitzung gültige Adresse für das Endgerät und leitet diese zusammen mit der Nonce des Join-Servers an das Endgerät weiter. Die Sitzungsschlüssel werden demzufolge nicht per

LoRa gesendet und können daher nicht abgehört werden. Das Endgerät berechnet die Sitzungsschlüssel anhand der Nonce und des Root-Keys über denselben Algorithmus wie der Join-Server. In der Abbildung sind die Berechnungsschritte in Schritt 4 und 9 demzufolge identisch.

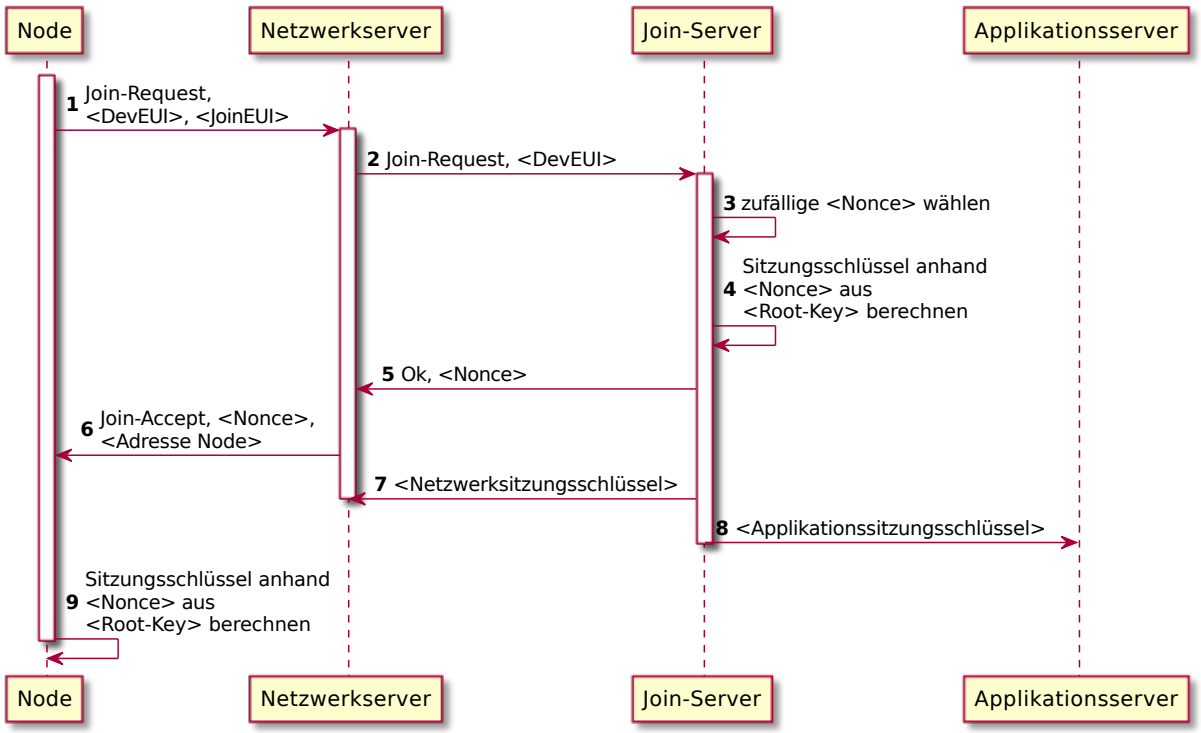

Abbildung 3.2: Beitrittsprozess Over-the-Air Activation
Quelle: eigene Darstellung

Die Sicherheit von OTAA ist höher als die von ABP, da jederzeit eine neue Sitzung mit neuen Sitzungsschlüsseln initiiert werden kann. Nachteilig bei OTAA ist die Komplexität des Beitrittsprozesses.

3.4 Geräteklassen

Endgeräten im LoRaWAN wird eine Geräteklasse zugewiesen. Anhand dieser Einstellung werden die zeitlichen Intervalle festgelegt, zu denen das Gerät empfangsbereit ist. In diesen sogenannten Empfangsfenstern kann das Endgerät einen Downlink vom Gateway empfangen, zu allen anderen Zeitpunkten ist ein Empfang durch das Gerät nicht möglich. Je nach benötigter Latenz einer Nachricht von der Anwendung zum Endgerät wird dem Endgerät die passende Klasse zugewiesen. [Theb]

In Abbildung 3.3 sind die Empfangsfenster im zeitlichen Verlauf nach einem Uplink des Endgeräts dargestellt. Allen Klassen gemein ist das Empfangsfenster „RX1“, wel-

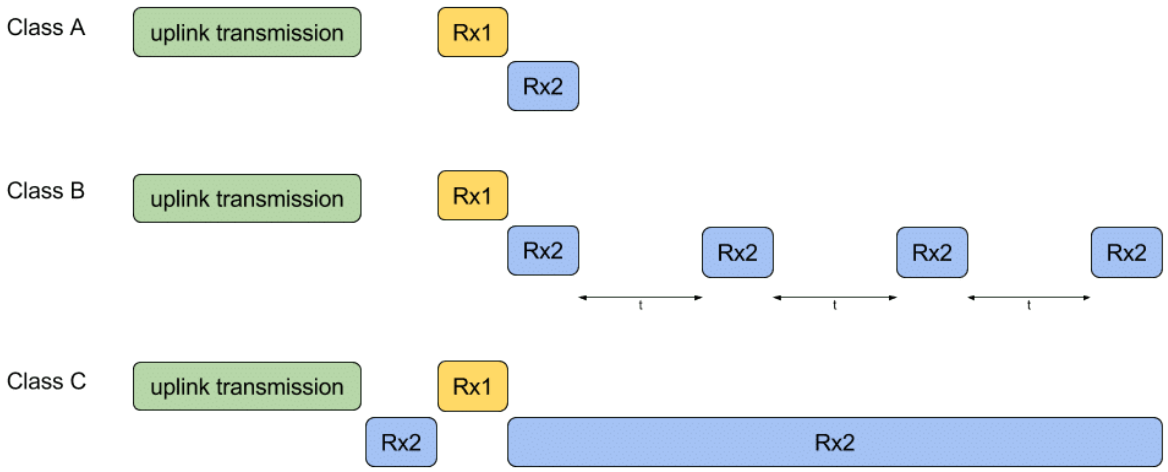

Abbildung 3.3: Empfangsfenster der Geräteklassen bei LoRaWAN
Quelle: https://witekio.com/wp-content/uploads/2018/01/Lora-wan-class.png

ches (abhängig von den Einstellungen des LoRaWAN) üblicherweise 1 Sekunde nach dem Senden einer Nachricht für kurze Zeit geöffnet wird. In Klasse A und B wird nach einer weiteren kurzen (vom Netzwerk abhängigen) Verzögerung noch das Empfangsfenster „RX2“ geöffnet. Danach ist ein Gerät der Klasse A erst wieder nach dem nächsten Uplink erreichbar, die Latenz ist entsprechend am größten und entspricht maximal der Dauer zwischen zwei Uplinks.

Geräte der Klasse B öffnen periodisch ein Empfangsfenster, welches durch vom Gateway gesendete Beacons gesteuert wird. Die maximale Latenz beträgt hierbei die eingestellte Periodendauer.

Geräte der Klasse C sind (außer wenn sie selber senden) immer empfangsbereit, es gibt entsprechend keine Latenz.

Während eines offenen Empfangsfensters wird Energie für das Betreiben des LoRa-Chips benötigt. Der Energiebedarf der Endgeräte ist also abhängig von der eingestellten Klasse. Bei Klasse C ist der Energiebedarf am höchsten, da der LoRa-Chip dauerhaft aktiviert sein muss. Der Energiebedarf ist dagegen am geringsten, wenn das Gerät in Klasse A ist, da nur während kurzer Zeitfenster Energie für den Empfang benötigt wird.

3.5 Adaptive Data Rate (ADR)

In Unterabschnitt 2.2.3 wurde die Konkurrenz zwischen Airtime, Energiebedarf und Reichweite bei Nutzung verschiedener Spreading Factors beschrieben. LoRaWAN löst

dieses Problem mittels des Verfahrens Adaptive Data Rate (ADR), welches eine Möglichkeit zur automatischen Optimierung dieser Werte bietet. Die Nutzung des Verfahrens kann durch das Endgerät gesteuert werden und sollte bei stabilen Umgebungsbedingungen (der Funkübertragung) aktiviert werden. [Thea]

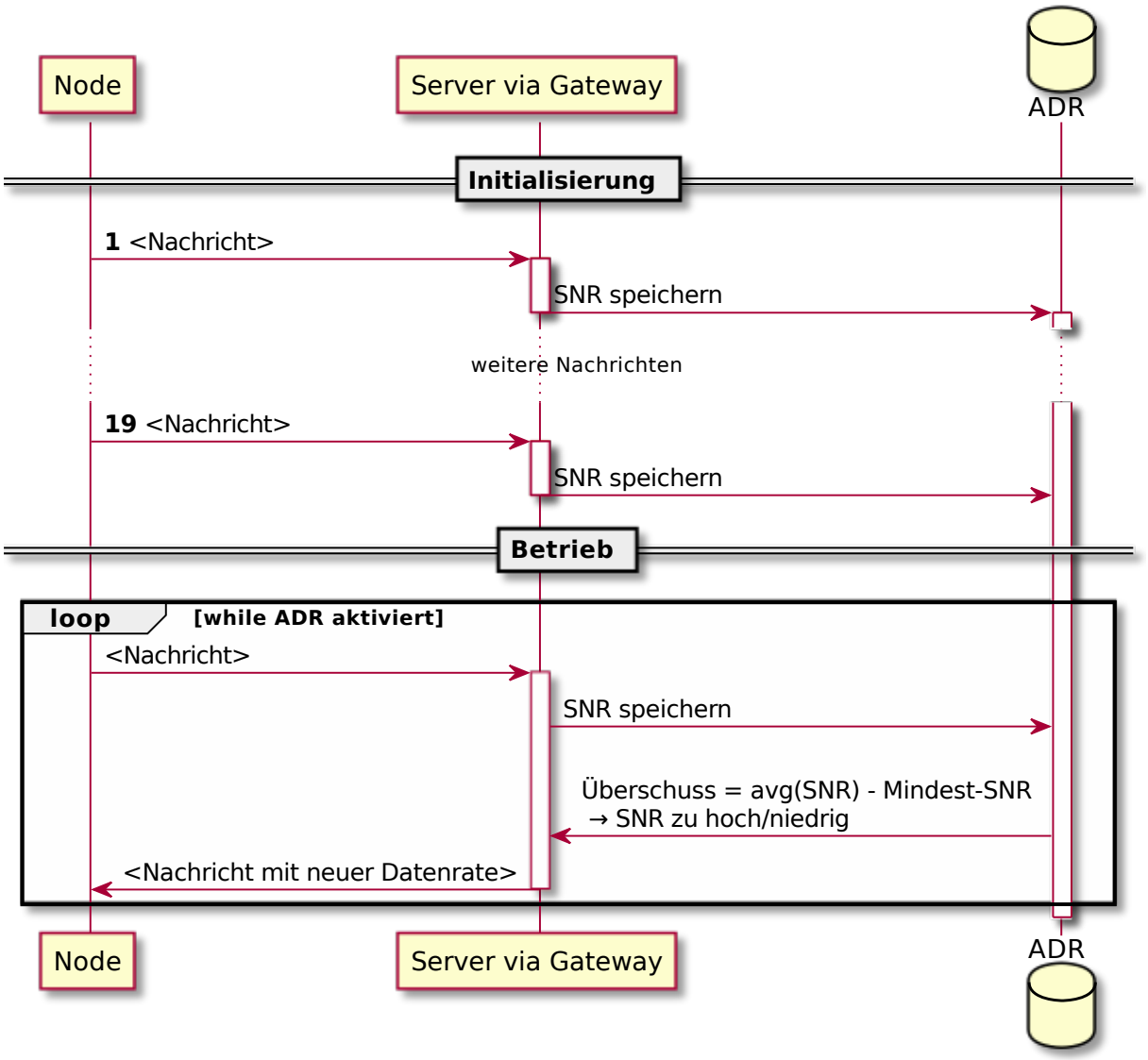

Abbildung 3.4: Ablauf ADR
Quelle: eigene Darstellung

In Abbildung 3.4 ist der Ablauf von ADR dargestellt. Nach jeder vom Endgerät empfangenen Nachricht wird das vom Gateway ermittelte Signal-Rausch-Verhältnis durch den Netzwerkserver gespeichert. Für die Initialisierung werden 20 Nachrichten benötigt. In der Betriebsphase wird nach jeder empfangenen Nachricht der Durchschnitt des SNR der letzten Nachrichten berechnet. Anschließend wird die Differenz zum mindestens nötigen SNR für erfolgreichen Empfang gebildet. Bei einer hohen Differenz gibt es einen SNR-Überschuss und das Endgerät sollte die Sendeleistung reduzieren

oder den Spreading Factor verringern (führt zu Erhöhung Datenrate und Verringerung Airtime). Bei einem SNR-Defizit sollte das Endgerät entsprechend die Sendeleistung oder den Spreading Factor erhöhen (führt zu Verringerung Datenrate und Erhöhung Airtime). Der Netzwerkserver sendet die passende Kontrollnachricht an das Gerät mit der Information, entsprechend den Spreading Factor zu verändern.

Für die Berechnung wird der Durchschnitt mehrerer Messungen verwendet, damit der Regelkreis nicht durch kurzzeitig auftretende Störungen instabil wird.

4 Anwendungsbeispiele

Im folgenden Kapitel werden kurze Beispiele zu Anwendungen von LoRa und LoRaWAN vorgestellt.

4.1 LoRa

Für den LoRa-fähigen Mikrocontroller Cubecell[1] wurde eine Software entwickelt, mit der die Kommunikation über LoRa getestet werden kann. Ein Gerät wird dabei als Client genutzt und sendet die per serieller Verbindung übergebenen Daten. Anschließend versucht das Gerät eine potentielle Antwort zu empfangen. Ein weiteres Gerät wird als Server genutzt, welcher ständig auf ankommende Pakete wartet. Wird ein Paket empfangen, so werden die in den Daten enthaltenen Buchstaben zu Großbuchstaben transformiert und per LoRa gesendet. Durch Client und Server werden die gesendeten und empfangenen Daten sowie die Signalstärke und das SNR des empfangenen Pakets jeweils auf dem Bildschirm des Mikrocontrollers dargestellt.

Das Protokoll des Clients ist in Abbildung 4.1 dargestellt. TX bezeichnet dabei die jeweils gesendeten Daten und RX die empfangenen. In der Demonstration wurde zunächst über wenige Zentimeter Abstand und mit angebrachter Antenne kommuniziert (Nachricht „Hallo Welt“ und „Moin“). Durch Entfernen der Antennen konnte gezeigt werden, dass die Signalstärke sinkt (Nachricht „1. Antenne weg“ und „...“ mit nur einer Antenne, Nachricht „Antennen weg“ komplett ohne Antennen). Außerdem wurde die Signalübertragung über mehrere Etagen in den Keller getestet. Dabei wurde festgestellt, dass ohne Antenne keine Kommunikation möglich ist (erste Nachricht „Keller?“). Mit angebrachter Antenne kann problemlos durch mehrere Wände kommuniziert werden, die Signalstärke und das SNR sinken allerdings im Vergleich zur Übertragung in über wenige Zentimeter (zweite Nachricht „Keller?“).

Der Quellcode der Software ist auf Github verfügbar.[2] Eine Live-Demonstration ist auf Youtube abrufbar.[3]

[1] https://heltec.org/project/htcc-ab02s/
[2] https://github.com/Salaml/sensor-networks/tree/main/code
[3] https://www.youtube.com/watch?v=YyFAu_R3ZoA

```
TX: "Hallo Welt!"
TX done......into RX mode
RX "HALLO WELT!" with SNR 12 and Rssi -22 , length 11

TX: "Moin"
TX done......into RX mode
RX "MOIN" with SNR 12 and Rssi -24 , length 4

TX: "1. Antenne weg"
TX done......into RX mode
RX "1. ANTENNE WEG" with SNR 11 and Rssi -62 , length 14

TX: "..."
TX done......into RX mode
RX "..." with SNR 12 and Rssi -63 , length 3

TX: "Antennen weg"
TX done......into RX mode
RX "ANTENNEN WEG" with SNR 11 and Rssi -95 , length 12

TX: "Keller?"
TX done......into RX mode


TX: "Keller?"
TX done......into RX mode
RX "KELLER?" with SNR 1 and Rssi -100 , length 7
```

Abbildung 4.1: Protokoll des Clients bei Tests der LoRa-Signalübertragung
Quelle: eigene Darstellung

4.2 LoRaWAN

In der HTW Dresden wurde ein LoRaWAN-Gateway installiert und in das freie LoRaWAN TTN eingebunden. Im folgenden wird kurz auf einige durch das Gateway bereitgestellte bzw. erfasste Statistiken eingegangen.

In Abbildung 4.2 ist der Duty Cycle des Gateways nach Kanal aufgeschlüsselt dargestellt. Es ist erkennbar, dass einige Kanäle häufiger verwendet werden als andere. Außerdem wird deutlich, dass LoRa-Übertragungen nicht dauerhaft stattfinden sondern aufgrund des gesetzlichen begrenzten Duty Cycles nur zu sporadischen Zeitpunkten.

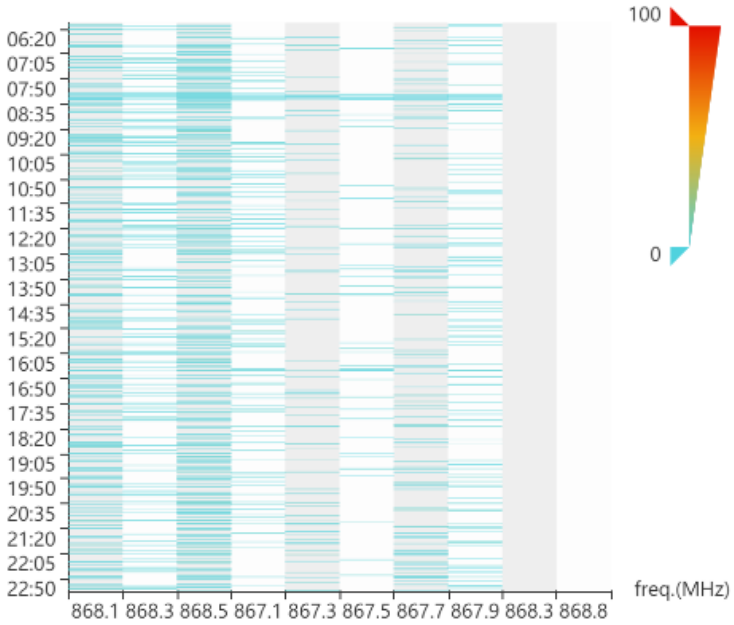

Abbildung 4.2: Duty Cycle des LoRaWAN-Gateways der HTW Dresden nach Kanal
Quelle: eigene Darstellung

In Abbildung 4.3 ist die Reichweite des Gateways erkennbar. Die Punkte sind nach der Signalstärke gefärbt, mit der eine Nachricht vom angegebenen Punkt das Gateway erreicht hat. Die Daten werden erfasst, indem ein Node periodisch (beliebige) Daten ins LoRaWAN sendet während er mit dem Kartierenden in der Umwelt bewegt wird. Die empfangenen Daten werden durch das Mobiltelefon des Kartierenden vom Applikationsserver über eine MQTT-Schnittstelle abgerufen. Das Mobiltelefon kombiniert die aus den Metadaten verfügbare Signalstärke zusammen mit der aktuellen Position und sendet diese dann an den Server des TTN-Mapper. Dort werden die Daten aufbereitet und entsprechend auf der Karte dargestellt. Dieser Workflow demonstriert perfekt den Datenfluss durch ein LoRaWAN.

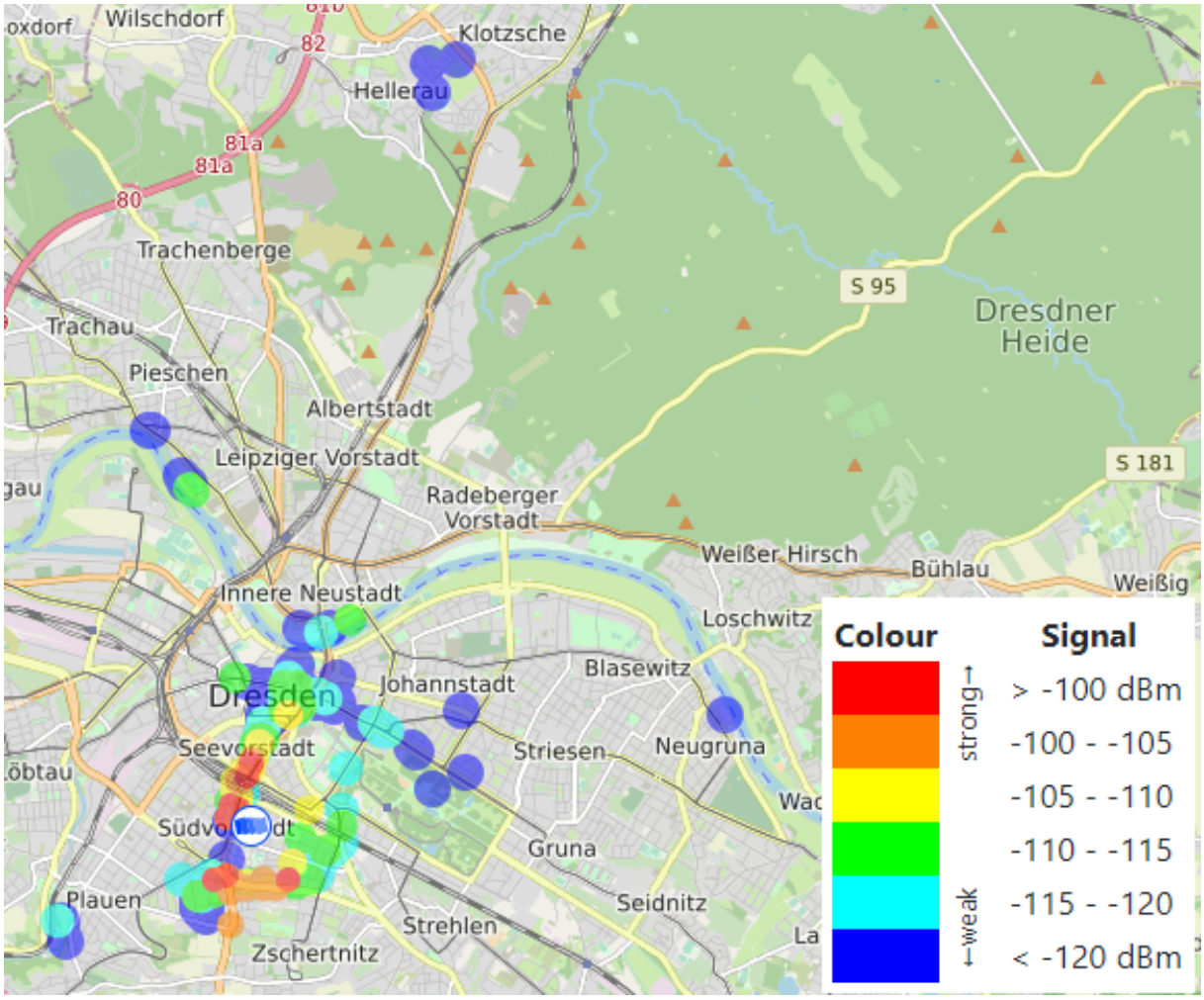

Abbildung 4.3: kartierte Signalstärke des LoRaWAN-Gateways der HTW Dresden
Quelle: TTN-Mapper, https://ttnmapper.org/heatmap/private/?gateway=htw-dresden-ttn-gw1&network=NS_TTS_V3://ttn@000013

5 Zusammenfassung

LoRa stellt als Grundlage eine solide Übertragungstechnik für die Kommunikation über hohe Reichweiten mit niedrigem Energiebedarf dar. Die Chirp Spread Spectrum Modulation ist ideal, um Signale mit geringer Leistung auch bei starkem Rauschen fehlerfrei übertragen zu können. Über verschiedene Spreading Factors lassen sich Energiebedarf und Reichweite gezielt steuern.

LoRaWAN bringt per LoRa kommunizierende Geräte zu einem einfach nutzbaren Netzwerk zusammen. Durch Verschlüsselungsmechanismen ist die Vertraulichkeit der Kommunikation gewährleistet. Durch verschiedenen Geräteklassen lässt sich ein Kompromiss zwischen Energiebedarf und Latenz der Kommunikation bilden und Verfahren wie Adaptive Data Rate ermöglichen eine automatische Optimierung von Energiebedarf und Reichweite.

LoRaWAN bildet insbesondere für Bereiche, in denen niedrige Datenraten und höhere Reaktionszeiten kein Problem sind, eine gute Grundlage für Internet of Things. Dies ist zum Beispiel für die Erfassung von Sensorwerten von räumlich weit verteilten Sensoren der Fall.

Literaturverzeichnis

[Ade+17] Ferran Adelantado u. a. „Understanding the Limits of LoRaWAN“. In: *IEEE Communications Magazine* 55.9 (2017), S. 34–40. DOI: 10.1109/MCOM.2017.1600613.

[Eri18] Eric B. *LoRa*. letzter Zugriff: 05.02.2022. 2018. URL: https://lora.readthedocs.io/en/latest.

[Ghoa] Sakshama Ghoslya. *LoRa: Orthogonality*. letzter Zugriff: 05.02.2022. URL: https://www.sghoslya.com/p/lora_6.html.

[Ghob] Sakshama Ghoslya. *LoRa: Symbol Generation*. letzter Zugriff: 05.02.2022. URL: https://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html.

[LoR21] LoRa Alliance. *RP002-1.0.3 LoRaWAN® Regional Parameters*. letzter Zugriff: 05.02.2022. 2021. URL: https://lora-alliance.org/wp-content/uploads/2021/05/RP-2-1.0.3.pdf.

[Sem] Semtech Corporation. *What Is LoRa?* letzter Zugriff: 05.02.2022. URL: https://www.semtech.com/lora/what-is-lora.

[Sem15] Semtech Corporation. *AN1200.22 LoRa Modulation Basics*. Mai 2015.

[Thea] The Things Industries. *Adaptive Data Rate*. letzter Zugriff: 05.02.2022. URL: https://www.thethingsnetwork.org/docs/lorawan/adaptive-data-rate/.

[Theb] The Things Industries. *Device Classes*. letzter Zugriff: 05.02.2022. URL: https://www.thethingsnetwork.org/docs/lorawan/classes.

[Thec] The Things Industries. *End Device Activation*. letzter Zugriff: 05.02.2022. URL: https://www.thethingsnetwork.org/docs/lorawan/end-device-activation.

[Thed] The Things Industries. *LoRaWAN Architecture*. letzter Zugriff: 06.02.2022. URL: https://www.thethingsnetwork.org/docs/lorawan/architecture.