Seminararbeit: LoRaWAN

Tobias Sigmann

25. Mai 2019

Inhaltsverzeichnis

1 Einführung in Lora

2 Aufbau eines Lora-Netzwerk

LoRa ist ideal für IoT-Geräte, da per einfachem Netzwerkaufbau Datenaustausch mit dem Internet möglicht ist. Um die von den End-Geräten gesendeten LoRa-Pakete auf IP/TCP Pakete umzusetzen wird ein Gateway als Schnittstelle benötigt, um die LoRa-Pakete in TCP/IP Pakete umzuwandeln und umgekehrt. Das Gateway implementiert aber keinerlei Logik. Hierzu ist ein Netzwerkserver zuständig der über die Gateways das Netzwerk kontrolliert und steuert. Gleichzeitig stellt er die Verbindung zu einem Applikationsserver her, in dem er die Daten weiterleitet.

Der Applikationsserver ist zuständig die gesendeten Nachrichten zu verarbeiten und sendet Daten an die Endgeräte.

Diese Architektur wurde gewählt um geringen Energieverbrauch zu ermöglichen, bei gleichzeitiger höher Endgeräteanzahl, hoher Siganlqualität und entsprechnder Netzwerksicherheit. [Tec15, S. 8 ff.]

2.1 Gateway

Die LoRa-Endgeräte werden sternförmig an die Gateways angeschlossen und stellen ein Teilnetz dar. Jedes Endgeräten kommuniziert direkt mit dem Gateway. Diese Art der Kommunikation wird "Single-Hop-Connection" genannt, da die gesendeten Daten ohne Umwege an das Gateway gesendet werden. Jedes Gateway ist mit mindestens einem Netzwerkserver verbunden.

Ein Endgerät kann gleichzeitig an mehreren Gateways senden. Der Netzwerkserver überprüft die Pakete auf Duplikate und stellt sicher, dass jedes Paket nur einmal an die Applikationsserver gesendet werden. Ein weiterer Vorteil ist das keine Endgeräteübergabe zwischen den Gateways bei Standortwechsel nötig sind. Da die Gateways mit allen in der Reichweite befindlichen Endgeräten kommunizieren müssen, wurde auf Einzelkommunikation verzichtet und auf Parallelkommunikation gesetzt. Dazu werden adaptive Datenraten und Mehrkanal-Multi-Modem-Transceiver verwendet.

Durch die genannt Eigenschaften der Gateways wird eine gute Skalierbarkeit erzielt.

Dadurch können neue Gateways die Anzahl der Endgeräte um das 6 bis 8-fach erhöhen. vgl. [Tec15, S.10]

2.2 Netzwerkserver

Der Netzwerkserver ist das "Herzstück" eines jeden Lora-Netzwerkes. Er kann mit mehreren Gateways und mehreren Applikationsserver verbunden sein.

Die wichtigste Aufgabe des Netzwerksserver ist die Steuerung des LoRa-Netzwerks. Der Server verwaltet jedes Endgerät separat indem es mit ihm den zu verwendenden Funkkanal aushandelt und die Datenrate kontrolliert wenn ADR (Adaptiv Data Rate) aktiv ist. Außerdem steuert er den Netzwerkbeitritt der Endgeräte.

Weiterhin überprüft er die empfangen Pakete auf ihre Korrektheit, Integrität und wie schon erwähnt filtert er Duplikate. Dabei ermittelt er auch das Gateway mit dem besten Empfang zum jeweiligen Endgeräten und nutzt dieses dann um Daten an das Endgerät zu senden.

Es ist nicht immer möglich Daten direkt zu senden, da die Endgeräte nicht immer empfangsbereit sind. Um die Applikationsserver zu endlasten, puffert der Netzwerkserver die Daten und sendet diese zum nächst möglichen Zeitpunkt.

Eine weitere sehr wichtige Ausgabe ist es eine Schnittstelle für den Applikationsserver bereitzustellen um eine einfache und schnelle Kommunikation zu ermöglichen.

2.3 Join-Server

Ein Join-Server wird benötigt um den Beitritt mittels OTAA zu ermöglichen. Mehr zu OTAA kann in dem Kappitel OTAA gelesen werden. Wenn ein Endgerät dem Netzwerk beitreten möchte, leitent der Netzwerkserver die Anfragen an den Join-Server weiter. Dieser führt dann die nötige Beitrittschritte aus, wie z.B. ableiten von Schlüsseln oder Senden der nötigen Einstellungen. Dafür ist der NwkKey und der AppKey notwendig, da diese zum verschlüsseln der Nachrichten benötigt werden. Aus Sicherheitsgründen dürfen diese Schlüssel nie über das LoRa-Netz übertragen werden, sondern müssen bei der Programmierung des Endgerätes vorgegeben werden. [SOR17b, S. 9 f.]

Der Join-Server kann mit mehreren Netzwerkservern verbunden werden und jeder

Netzwerkserver kann mehrere Join-Server haben.

2.4 End-Gerät

Endgeräte sind Geräte die Informationen mittels LoRa empfangen oder senden. Jedes Endgerät ist mit einem bestimmten Applikationsserver verbunden.

Jedes Endgerät muss zur korrekten Funktion mehrere wichtige Informationen haben.

- DevEUI: Globale Endgeräte_ID die eindeutig für jedes Endgerät definiert ist. Vergleichbar mit der MAC-Adresse eines TCP/IP Gerätes.
- JoinEUI: Globale Adresse des Join-Servers an den die Join-Anfrage gehen soll. Wird nur für OTAA Geräte benötigt.
- NwkKey und AppKey: Werden verwendet um spätere Schlüssel abzuleiten und die Kommunikation während der Beitrittprozedur in ein Netzwerk abzusichern. Dafür müssen sie sowohl dem Join-Server als auch dem Endgerät bekannt sein.

[SOR17c, S.47 ff.]

3 LoRaWAN Funktionsweise

Im folgenden Kapitel wird näher auf die Funktionsweise von LoRaWAN eingegangen. Speziell, liegt der Fokus auf dem Netzwerkebitritt, das verwendete Protokoll und wie die Daten physikalisch Übertragen werden.

3.1 Schichtenmodell

Das Schichtenmodell lässt sich in zwei Teile unterteilen. Der LoRa Part ist der unterste und kümmert sich um die physikalische Übertragung der Pakte. Der LoRaWAN Part ist für die Steuerung des Netzwerkes, Definition der LoRaWAN-Klassen und das Überprüfen / Verschlüsseln der Daten zuständig.

Die unterste Schicht des LoRa Parts ist für die Anwendung der richtigen Frequenzen zuständig. In Europa muss das freiverfügbare ISM-Band 868 verwendet werden, in den Vereinigten Staaten das Band 915 und in Asien das Band 430 . [Tec15, S.7]

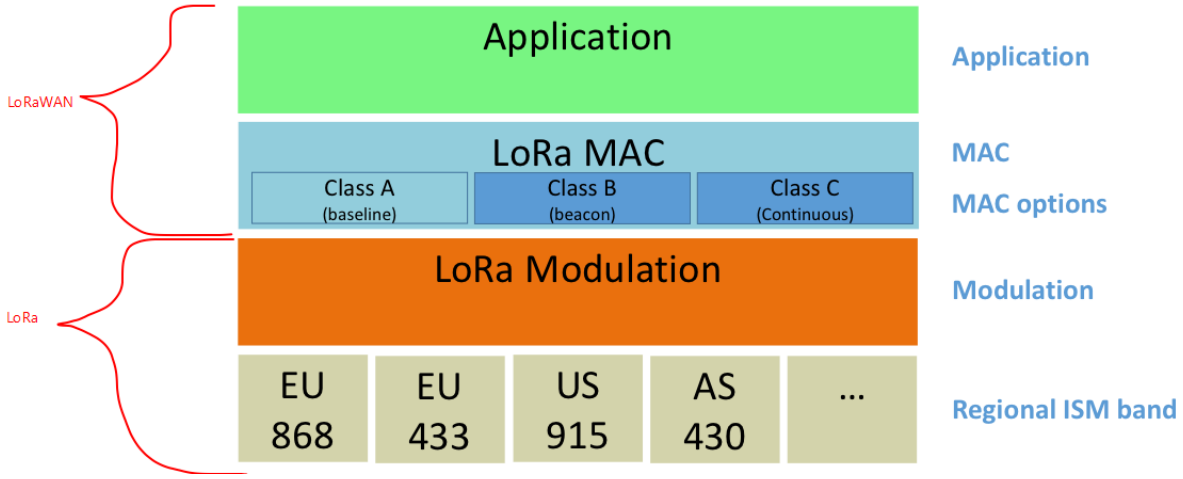

Abbildung 1: LoRaStack [Tec15, S.7]

Die darüber liegende Schicht nennt man LoRa Modulation. Sie wandelt die binären Pakete in LoRa-Signale um, so dass der Empfänger diese korrekt und effizient empfangen und wiederherstellen kann. Mehre dazu im Kapitel Übertragungsart.

Über LoRa Modulation liegt die erste LoRaWAN Schicht die LoRa MAC genannt wird. MAC steht für "Media Access Protokoll". Dieses Protokoll wird zur Steuerung des LoRa-Netz verwendet. Diese Schicht ist außerdem für die Implementierung der einzelnen Endgeräteklassen und für das Übertragen der Steuerungskommandos zuständig. Mehr zu den Endgeräteklassen kann im Kapitel Lora Geräte Klassen und im Kapitel Protokoll gelesen werden.

Die oberste Schicht nennt sich Applikationsschicht und verpackt, verschlüsselt und authentifiziert die Nutzdaten einer Nachricht.

3.2 Netzwerkbeitritt

Endgeräte sind immer einem bestimmten Netzwerk zugeordnet. Es gibt zwei Wege um ein neues Endgeräte zu einem bestehenden Netzwerk hinzuzufügen.

3.2.1 OTAA

Die sicherste aber auch aufwendigste Methode heißt OTAA "Over-the-Air Activation". Hierbei muss bei jedem Netzwerkbeitritt die Join-Prozedur ausgeführt werden. Dafür müssen folgende 4 Konstanten im Programm vorhanden sein: DevEUI, JionEUI, NwkKey

und AppKey.

Näheres zu den Konstanten kann im Kapitel End-Gerät nachgelesen werden.

Der NWKSKEY ist für die Verschlüsslung der Datenpakete bis zu Gateway zuständig. Dieser Key wird vom Netzwerkserver erzeugt und muss manuell in den Code eingetragen werden. [GAS17, S.3]

Der letzt Wert heißt APPSKEY und sichert die Kommunikation vom Endgerät zu dem Applikationsserver ab. Der Schlüssel wird genau wie der NWKSKEY vom Netzwerkserver erzeugt und verwaltet. [GAS17, S.3]

Als erstes muss das End-Gerät eine Join- oder Rejoin-Nachricht an das Gateway senden. Die Nachricht besteht aus der JoinEUI, dem DevEUI und einer DevNonce. Mit der DevNonce sollen Replayattack verhindert werden. Die Nonce stratet beim ersten Join-Request mit 0 und wird bei jedem Join-Request um eins erhöht. Die Nonce muss im einem nichtflüchtigern Speicher gespeichert werde, um den Werte unter allen Bedingungen zu Sichern. Ansonsten wäre ein manueller Reset des Zählers im Netzwerkserver erforderlich. Sendet ein Endgerät einen Join-Request mit zu kleinem DevNonce, wird die Nachricht ignoriert und es ist nicht möglich dem Netzwerk beizutreten.

Das Gateway antworted mit einer Accept-Nachricht, besteht aus einer JoinNonce, einem NetzwerkID Net_ID, einer Geräteadresse DevAddr, einem Einstellungsfeld DLSettings , einer Zeitangabe wie lange zukünftig auf eine Antwort nach dem Senden gewartet werden muss (hier RxDelay) und einer optionalen Netzwerkparameterliste CFList.

Die JoinNonce wir verwendet um Replayatacken zu verhindern und muss größer als die zuletzt gesendete sein. Ansonsten wir die Nachricht vom Endgerät ignoriert. Außerdem wir die Nonce benutz um Schlüssel wie AppSKey herzuleiten. Für jedes Endgerät wird eine eigene JoinNonce geführt, sie darf sich nicht wiederholen. Jedes Endgerät merkt sich die letzte JoinNonce und tritt auch nur bei, wenn diese größer ist als die letzte.

Die Join-Accept Nachricht wird vom Endgerät nach JOIN_ACCEPT_DELAY1 oder JOIN_ACCEPT_DELAY2 nach dem Senden des Request erwartet. Wird die Join-Accept Nachricht zu einem andern Zeitpunkt gesendet , wird diese nicht empfangen, da das Endgerät nicht empfangsbereit ist.

Mehr Informationen zu den Ableitungen der Schlüssel finden Sie in dem Kapitel Sicherheit.

3.2.2 ABP

Die einfachste Art des Beitritts heißt ABP was für "Activation by Personalization"steht. Hierbei muss lediglich vor Inbetriebnahme des Endgerätes fünf Konstanten definiert werden.

Als erstes wird die DevAdr(Geräteadresse) angegeben. Diese Adresse existiert nur einmal im Netzwerk und wird für die Indentifizierung des Endgeräts verwendet. Die Adresse wird vom Netzwerkserver erzeugt und muss im Programmcode eingetragen sein.

Die anderen vier Werte sind die verwendeten Schlüssel zur Kommunikationsverschlüsselung: FNwkSIntKey, SNwkSIntKey, NwkSEncKey und AppSKey. Damit kann die Join-Prozdeur übersprungen werden. Allerdings werden immer dieselben Schlüssel verwendet was zu einem Sicherheitsproblem werden kann.

Nach Beitritt muss das ResetInd MAC-Kommando im FOpt Feld gesendet werden. Dieses Kommando teilt dem Netzwerkserver mit, dass das Endgerät online ist und die Standardübertragungsart, -frequenz und -kanal verwendet werden. Weiter Erläuterungen folgen im nächsten Unterkapitel.

Das Netzwerk muss mit einem ResetConf-Kommando antworten. In diesem teilt es dem Endgerät die unterstützten LoRa-Versionen mit. Danach kann die Kommunikation beginnen.

3.3 Protokoll

Das LoRaWAN Protokoll ist optimiert für batteriebetrieben Endgeräte für drahtlos Kommunikation. Um energieeffizent zu sein setzt LoRa hauptsächlich auf zwei Punkte: die Modulationstechnick und Adaptive Datenrate (ADR). Auch die Öne-HopÄrchitektur trägt zur Energieeffizenz bei. Die Modulationsart wird in Kapittel Übertragungsart besschrieben. [CB+17, S,1 f]

Damit der Netzwerkserver das LoRa-Netz steuern kann, werden Mac-Kommandos eingesetzt. Mit diesen Kommandos tritt man dem Netzwerk bei, kommuniziert mit den Endgeräten und steuert Frequenzen, Kanäle und vieles mehr. Da die Kommandos nur für den Netzwerkserver und die Endgeräte von Bedeutung sind, werden diese nicht an den Applikationsserver gesendet, sondern vom Netzwerkserver herausgefiltert. Im Folgenden

wird näher auf die MAC-Kommandos und die Paketstruktur eingegangen. Ein Uplink ist ein Paket dass vom Endgerät, das bildlich gesprochen "unter" dem Gateway sitzt, an das Gateway gesendet wird. Ein Downlink ist dem entsprechend ein Paket das vom Gateway an das Endgerät gesendet wird.

3.3.1 MAC-Kommandos

MAC-Kommandos werden ausschließlich für die Steuerung und Pflege des Netzwerkes verwendet. steht für "Medium Access Control". Da der Netzwerkserver das Netzwerk steuert, werden diese Kommandos nur zwischen dem Netzwerkserver und dem Endgerät verwedet.

MAC-Kommandos werden mittels eines "Command Indentifier" (CID) gesendet. Das ist eine 8 Bit Zahl die das MAC-Kommando repräsentiert. Nach dem CID folgen mögliche Variablen die dem Kommando mitgegeben werden. Die Anzahl und Länge der Variablen ist nicht beschränkt.

Die MAC-Kommandos müssen zwingend ausgeführt werden. Die Nachrichten werden in derselben Reihenfolge wie sie angekommen bestätigt oder beantwortet. Somit weiß der Netzwerkserver welche Kommandos bereits ausgeführt wurden. Alle Kommandos die in einem Frame gesendet wurden, müssen auch in einem Frame bestätigt / beantwortet werden. Zur Speicherung der Reihenfolge wird ein Puffer für die MAC-Kommando-Antworten verwendet. Dieser Puffer wird beim nächsten Uplink mit gesendet. Sollte der Puffer zu klein sein, werden keine weiteren Antworten eingetragen. Deshalb muss der Netzwerkserver vorher die maximale Antwortgröße errechnen und die MAC-Kommandos dementsprechend in Frames aufteilen. [SOR17c, S.29 ff.]

Im Folgenden ist eine Liste aller MAC-Kommandos angegeben:

CID	Kommandoname	Funktion
0x01	ResetInd	Wird bei dem Beitritt mittels ABP vom Endgerät gesendet. Informiert das Netzwerk über den Beitritt.
0x01	ResetConf	Wird vom Gateway gesendet und bestätigt das ResetInd-Kommando.
0x02	LinkCheckReq	Wird vom Endgerät verwendet um die Verbindung zum Netzwerk zu überprüfen.

0x02	LinkCheckAns	Bestätigt das vom Endgerät gesendete LinkCheckReq-Kommando
0x03	LinkADRReq	Wird zu Steuerung der Endgeräte im ADR-Modus verwendet
0x04	DutyCycleReq	Das Gateway teilt dem Endgerät mit wie oft die Verbindung getestet werden soll
0x04	DutyCycleAns	Das Endgerät bestätigt den neuen Testzyklus
0x05	RXParamSetupReq	...
0x05	RXParamSetupAns	...
0x06	DevStatusReq	...
0x06	DevStatusAns	...
0x07	NewChannelReq	...
0x07	NewChannelAns	...
0x08	RXTimingSetupReq	...
0x08	RXTimingSetupAns	...
0x09	TxParamSetupReq	...
0x09	TxParamSetupAns	...
0x0A	DlChannelReq	...
0x0A	DlChannelAns	...
0x0B	RekeyInd	...
0x0B	RekeyConf	...
0x0C	ADRParamSetupReq	...
0x0C	ADRParamSetupAns	...
0x0D	DeviceTimeReq	...
0x0D	DeviceTimeAns	...
0x0E	ForceRejoinReq	...
0x0F	RejoinParamSetupReq	...
0x0F	RejoinParamSetupAns	...
0x10	PingSlotInfoReq	...
0x10	PingSlotInfoAns	...
0x11	PingSlotChannelReq	...

0x11	PingSlotChannelAns	...
0x12	BeaconTimingReq	...
0x12	BeaconTimingAns	...
0x13	BeaconFreqReq	...
0x13	BeaconFreqAns	...
0x20	DeviceModeInd	...
0x20	DeviceModeConf	...
0x80-0xFF	Proprietary	...

3.3.2 LoRa-Paketstruktur

Die Paketstruktur kommt wie beim ISO/OSI Schichtenmodel durch das "durchlaufen" des Stacks zustande. Die Paketstruktur wird hier Top-Down betrachtet. Als erstes werden die Felder der Modulationsschicht betrachtet.

Jedes Pakete besteht grundlegend aus zwei Felder: Präambel und PHYPalyload. Falls es sich um einen Uplink-Paket handelt wird noch ein CRC Code hinzugefügt, also Preamble, PHYPalyload, CRC. In diesem Fall spricht man von einem impliziten Paket oder vom implizitem Modus. Impliziter Modus bedeute, dass es kein Payload Header gibt. Payload Header gibt die Felderlänge und die CRC Längenangabe an. Diese sind somit zuvor fest zu definieren. Im expliziten Modus werden noch zwei Felder hinzugefügt, PHDR und PHDR_CRC. Somit sieht ein explizites Paket folgendermaßen aus: Preamble, PHDR, PHDR_CRC, PHYPalyload. Auch hier gilt, im Falle eines Uplink-Paketes wird am Ende ein CRC Feld angefügt. Somit ergibt sich dann folgende Paketstruktur: Preamble, PHDR, PHDR_CRC, PHYPalyload, CRC.

Die Preamble ist eine Startsequenz und teilt dem Empfänger mit, dass gleich Daten gesendet werden. Sie ist nur ein Signal ohne Informationen.

Da Teile des LoRaWAN Protokolls geschützt sind, findet man über die PHDR und PHDR_CRC Felder nur sehr wenig Informationen. Allerdings geht hervor, dass der PHDR die Länge des PHYPayloads und die Zieladresse beinhaltet. Mit dem PHDR_CRC Feld wird die Korrektheit der empfangenen Werte sichergestellt. Dies wird mittels des CRC Verfahrens überprüft.

Wie schon mehrfach erwähnt wird in Uplink-Nachrichten ein zusätzliches CRC Feld verwendet. CRC steht für “Cyclisch Redundanz Check” und wird zur Bestätigung der Nachrichtenkorrektheit verwendet. PHDR, PHDR_CRC und das CRC Feld werden automatisch vom dem Funktransceiver (Modul aus Empfänger und Sender) hinzugefügt.

Die LoRa MAC Ebene fügt nun das PHYPalyload Feld ein. PHYPalyload steht für Physikalische Payload. Es gibt drei mögliche PHYPayloads. Entweder wird ein MACPaylod eingefügt, Join-Rejon-Request oder aber es werden die Join-Accept Nachricht darin transportiert. Um die Daten bzw. die MAC Kommandos richtig auszuwerten und um die Korrektheit zu überprüfen, werden einige Headers und zusätzliche Felder benötigt. Deshalb lässt sich das Feld PHYPalyload in MHDR und MACPayload unterteilen. Falls der MACPaylod eine Join-Rejoin oder MACPayload Nachricht ist, wir noch ein MIC Feld hinzugefügt: MHDR, MACPayload und MIC. MIC steht für “Message Integrity Code” und mit ihr wird die Korrektheit der des MACPayloads und des MHDR ermittelt.

Das MHDR Feld definiert die Daten im MACPayload Feld. Auch dieses wird Feld in Unterfelder unterteilt: MType, RFU und Major. MType steht für “Message Type”. Das MType Feld beschreibt die Art der Nachricht, z.B. Datennachrichten oder Join-Nachrichten, ... RFU steht für “Reserved for Future Usag“. Daher kann dieses Feld in der Version 1.1 und niedriger ignoriert werden. Das Major Unterfeld wird verwendet um das LoRa-Version der Nachricht zu definieren. Momentan ist nur der Wert 0 definiert. 0 Steht für LoRaWan R1. Die restlichen Werte sind für zukünftige Updates reserviert.

Mit der Unterteilung des MACPayload springen wir in dem LoRaStack noch eine Ebene höher, in die Applikationsschicht. Im MACPayload Feld sind Frameheader FHDR, Frame-Port FPort und Frame-Payload FRMPayload enthalten. Nutzdaten befinden sich im FRMPayload Feld. Werden keine Daten gesendet, entällt das FRMPayload Feld MAC-Kommandos. In dem Feld FPorts wird angegeben an welchen Port und somit an welche Teilapplikation des Applikationsserver die Daten geleitet werden sollen. Es gibt einige fest definierte Ports. Port 0x00 ist reserviert um MAC-Kommandos im FRMPayload Feld entgegenzunehmen. Die Ports 0x01 bis 0xDF sind anwendungsspezifische Ports und Port 0xE0 ist für das LoRaWAN-Test-Layer-Protokoll reserviert. Nachrichten mit anderen Port-Adressen werden verworfen.

Auch der FHDR "Frame Header"wird in einzelne Felder unterteilt: DevAddr, FCtrl,

FCnt und Fopts. In dem Feld DevAddr (Device Address) wird die Zieladresse der Nachricht vermerkt. Im Feld FCnt (Frame Counter) wird der jeweilige Zählerwert (Counter) für die bisher gezählten Nachrichten übermittelt. Hiermit schützt man sich vor Replayattacks. Mehr zu den Counter kann im Kapitel **??** gelesen werden. Im FOpt Feld können bis zu fünf MAC Kommandos parallel zur Datenübertragung übermittelt werden. Die Anzahl kommt auf die Menge der mitgelieferten Variablen an.

Das letzte Feld das in Unterfelder unterteilt werden kann ist das FCtrl Feld. Hiermit wird das Endgeräte gesteuert und Nachrichten bestätigt. Es gibt leichte Unterschiede für Uplink und Downlink Nachrichten. Beide Nachrichtentypen haben ein ADR, ein ACK und ein FOptsLen Feld. Das ADR Feld definiert, ob im Modus Ädaptive Data Rate"Daten gesendet werden oder im Standardmodus. Siehe KapitelAdaptive Data Rate. Mit dem ACK Feld können empfangene Pakete bestätigt werden. Ob Nachrichten bestätigt werden müssen, ist im MType Feld (Confirmed Data) definiert. In dem FOptsLen Feld wird die Länge des FOpts Feldes mitsamt des Headers eingetragen. Ist das FOptsLen 0, so ist kein FOpts Feld vorhanden.

Ein Downlinkpaket hat zusätzlich ein RFU Feld das nicht verwendet wird und ein FPending Feld. In diesem Feld kann das Gateway bzw. der Netzwerkserver dem Endgerät mitteilen, dass noch mehr Daten folgen.

Dahingegen hat ein Uplink-Paket ein ClassB. Hier teilt das Endgerät dem Gateway mit, dass es auf Funktionsklasse B wechseln will. Zusätzlich hat das Uplink-Paket ein ADRACKReq Feld. Dieses Feld wird verwendet um zu überprüfen, dass das Netzwerk noch antwortet. Die genaue Funktionsweise ist im Kapitel Adaptive Data Rate erklärt.

Eine detailierte Beschreibung der LoRa-Paketstruktur findet man in der LoRaWA 1.1 Specification [SOR17c].

3.4 Übertragungsart

Um die entstandenen Pakete in Signale umzusetzen und diese effizient und gleichzeitig übertragen zu können nutzt LoRa Chrip-Spread-Spectrum (CSS). Bei dieser Frequenzmodulation wird Frequenzanstieg als Binär 1 und Frequenzabfall als Binär 0 codiert. Man spricht bei einem Bit von einem Chrip-Impuls. Durch aneinanderreihe der verschiedenen Impulse können mehrere Bits übertragen werden. Das entstandene Signal wird auch als

Sub-Chrip bezeichnet. Da verschiedene Anstiegszeiten und Abfallzeiten verwendet werden, können mehre Signale auf derselben Frequenz parallel übertragen werden. Dies nennt man auch Spreading Factor. Die Parallelität wird durch Verwendung von verschiedenen Frequenzbereiche verbessert. CSS ist besonders für große Reichweiten geeignet und ideal für LoRa. Mit dem "Spreading Factor" wird die Signaldauer entsprechend dem Endgeräteabstand zum Gateway geregelt. Damit wird auch der Energieaufwand gering gehalten. Ähnlich einer Unterhaltung auf einer lauten Party. Man spricht nicht nur lauter sonder auch besonders langsam und deutlich. [SOR17a]

Mit Spreading Factoren und Frequenzen werden Channels erzeugt. Channels können beliebig benutzt werde. Es gibt allerdings zwei Regeln zu beachtet:

1. Channels werden per Pseudozufallszahl geändert

2. Sendezeit erfüllt die regionalen Bestimmungen

Mit dem Aloha Protokoll wird festgestellt wann gesendet werden soll. Vorhandene Daten werden dann einfach gesendet. Wenn nun zwei Sender gleichzeitig auf dem selben Channel senden möchten kommt es zu einer Kollision. Dadurch kann das Gateway die empfangenen Daten nicht mehr auswerten und die Daten müssen erneut übertragen werden. Deswegen warten beide Endgeräte eine zufällige, unterschiedliche Zeit ab bis sie erneut senden.

3.4.1 Adaptive Data Rate

Adaprive Data Rate oder kurz ADR wird verwendet um die optimalste Senderate und die optimale Sendepower für das Endgerät zu finden und so die optimalste Datenübertragung zu erhalten. ADR kann nur verwendet werden wenn, im FHDR Feld des LoRa-Pakets das ADR Bit gesetzt ist, siehe Protokoll. Die Steuerung mit ADR findet durch den Netzwerkserver statt. Sobald der Netzwerkserver bereit ist, setzt er das Bit im Downlink-Paket. Ist das Endgerät auch bereit, so setzt es ebenfalls das ADR Bit und ADR kann verwendet werden. Ist ADR nicht möglich wird Standardübertragung verwendet.

Die Steuerung findet durch spezielle MAC-Kommandos statt. Standardgemäß wird die höchste Übertragungsstärke verwendet, die geringste Übertragungsrate und zufälliger Kannal. Diese Parameter werden bei Bedarf vom Netzwerkserver durch das LinkA-

DRReq MAC–Kommando angepasst. Die neuen Werte der Parameter sind in den Variablen des MAC-Kommandos codiert. Sobald die Werte geändert wurden, muss periodisch überprüft werden ob das Netzwerk die Nachrichten noch empfängt. Deshalb wird bei jedem Uplink der ADR_ACK_CNT Zähler erhöht. Wenn dieser Zähler den Schwellenwert ADR_ACK_LIMIT überschreitet, wird das ADRACKReq Bit im Uplink gesetzt. Dieses signalisiert dem Netzwerkserver eine Nachricht zu senden um die Verbindung zu bestätigen. Falls dieser Downlink nicht in ADR_ACK_DELAY Frames empfangen wird, wird zuerst die Übertragungsstärke auf das Maximum gesetzt. Gegebenenfalls wird außerdem die Datenrate verringert um die Reichweite zu erhöhen. Die Datenrate wird pro ADR_ACK_DELAY Frames schrittweise weiter bis zum minimaler Datetrate verringert. Falls diese schon minimal ist, werden alle Kanäle benutzt. Dies wird solange probiert bis eine Verbindung hergestellt werden kann. [SOR17c, S.19 f]

4 Lora Geräte Klassen

Um maximal Energie zu sparen aber trotzdem die Möglichkeit dass die Endgeräte agile Daten empfangen können wurden die Geräteklassen eingeführt. Das Hauptmerkmal der Klassen sind die unterschiedlichen Empfangsmodien. Es gibt 3 Klassen, A, B und C. Die Klasse A muss standartgemäß von jedem Endgerät implementiert werden. B und C sind Optional und müssen nicht vorhanden sein Alle Geräte die mehr als Klasse A unterstützen werden als “higher Class end-devices “ genannt. [SOR17c, S.10]

4.1 Klasse A

Klasse A wird auch (All end-Devicec) genannt, zeichnet sich durch den geringsten Stromverbrauch aus. Die Kommunikation wird von dem Endgeräte gestartet werden. Das bietet die Möglichkeit dass das Endgerät, wenn keine Daten gesendet werden müssen, in einen sehr sparsamen Schlafmodus wechselt. Um das Endgeräte nicht zum “aufwachen“ zwingen zu müssen, wurde auf einen Hardbeat oder ähnliches verzichtet. Dadurch kann das Endgerät so lange “schlafen“ wie es möchte. Klasse A erlaubt außerdem das das Endgerät andere Protokolle verwendet solange es keine LoRa Daten sendet oder empfängt. [SOR17c, S.11 ff.] Das Endgerät startet die Kommunikation in dem es Daten an das Gateway sendet.

Daraufhin hat das Gateway die Möglichkeit 2 mal Daten zum Endgeräte senden. Die Empfangsfesnter werden RX1 und RX2 genannt.

Die Empfangsfesnter RX1 und RX2 müssen mindestens solange geöffnet bleiben das sie eine beginnende Übertragung feststellen können. Falls keine Übertragung empfangen wird, wird das Empfangsfesnter wieder geschlossen. Empfangsfenster RX1 wird nach RECIEV_DELAY1 zeiteiheiten +/- 20msec nach Beendigung des Uplinks geöffnet. Es wird die selbe Frequenz und Datenrate verwendet die auch bei den Downlink verwendet wurde. Wenn festgestellt in RX1 festgestellt wurde das keine Weiteren Daten mehr empfangen werden müssen kann auf das öffnen des RX2 Fensters auch verzichtet werden.

RX2 wird wird nach RECIEV_DELAY2 Zeiteinheiten +/- 20msec nach Beendigung des Uplinks geöffnet. Allerdings ist die Datenrate und Frequenz fest. Nur mittels spezieller MAC Kommandos kann dies verändert werden.

Für die Join-Prozedur wird immer die Klasse A verwendet. Die verwendete Frequenz entspricht der Empfangsfenster RX1 oder RX2.

4.2 Klasse B

Die Klasse B (B für BEACON) bietet bidirektionale Kommunikation mit einer deterministischem Downlink Latenz. Um diese Latenz zu gewährleisten, muss die Kommunikation synchronisiert ablaufen. Außerdem muss festgestellt werden, ob das Endgerät bzw. das Gateway noch in Reichweite ist. Dies wird mittels eines periodischem Beacon ermittelt. Dieser Beacon wird regelmäßig vom Gateway gesendet und dient der Synchronisation der Endgeräte. Zeitpunkten gesendet werde realisiert. Die Latenz ist einstellbar und kann bis zu 128 Sekunden. [SOR17c, S.66 ff.]

Die Endgeräte öffnen in regelmäßigen Abständen ein Empfangsfenster das Pingslot genannt wird. Ein Downlink der in einem Pingslot gesendet wird, wird Ping genannt. Da immer das Gateway mit dem besten empfang die Daten an das Gateway sendet, muss das Endgerät selbständig feststellen wenn es einen Beacon mit einer unbekannten ID bekommt und durch eine Uplink dem Server mitteilen das es sich in einer neuen Umgebung ist. Dadurch lernt der Server wo sich das Endgerät befindet und kann das Gateway mit dem besten Empfang wählen. Obwohl das Endgerät durch die periodischen Beacon nicht “schalfe“ kann, ist die Klasse B für den Batteriebetrieb gedacht.

4.2.1 Klassenwechsel A nach B

Um einen Wechsel überhaupt zu ermöglichen muss der Netzwerkserver die Standard Pingslot Periode, die Pingslot Datenrate und den Pingslot Kanal kennen. Ale Endgeräte treten in Klasse A dem Netzwerk bei. Das wechseln in die Klasse B wird durch folgenden Prozess realisiert.

Als erstes muss das Programm des Endgerätes beim LoRaWAN Layer anfragen ob es möglich ist in Klasse B zu wechseln. Der Layer sucht nun nach einem Beacon. Wird ein Beacon entdeckt, wird die BEACON_LOCKED Serviceprimitive zurückgeliefert. Wenn kein Beaconempfangen wurde wir die BEACON_NOT_FOUND primitive zurückgegeben. Um diesen Prozess zu beschleunigen kann das DeviceTimeReq MAC-Kommando verwendet werden. Damit wird das Gateway aufgefordert einen Beacon zu senden. Nun kann das Endgerät in den Modus B wechseln.

Als Zweites setzt der MAC Layer des Endgerätes das Class B Bit im FCtrl Feld des Upliks auf 1. Der MAC Layer ist auch verantwortlich die Pingslot und für die Beacons Empfangsfenster zu offen. Dabei muss mit der größten möglichen Abweichung der internen Uhr gerechnet werden und demensprechend die Empfangsfenster angepasst werden. Diese darf pro Beacon nicht mehr als +/- 1.3msec liegen. [SOR17c, S.73]Der Inhalt des Empfangenen Beacon wird mit der Signalsterke dem Programm des Endgerätes zur weiteren Verarbeitung gesendet. Damit kann z.B. die innere Uhr nachgestellt werden oder Ortswechsel festgestellt werden.

4.2.2 Betrieb

Damit der Netzwerkserver dem Endgerät mitteilen kann dass die Pingslot Frequenz und die Datenrate geändert werden soll gibt es den PingSlotChannelReq Mac-Kommando. Die neuen Werte sind in den Argumenten enthalten.

Das Endgerät kann die Periode der Pingslot szu einer beliebigen Zeit ändern. Ist dies der Fall, so muss das Endgerät in Klasse A wechseln und mittels dem MAC-Kommando PingSlotChannelReq die geänderte Periode Mitteilen. Danach kann zurück in die Klasse B gewechselt werden.

Falls einige länger als 2 Stunden kein Beacon empfangen wird, kann die Synchroni-

sation mit dem Netzwerk verloren gehen. Dadurch funktioniert die Kommunikation in Klasse B nicht mehr und es wird in Klasse A gewechselt. Nun kann versucht werden eine Verbindung mit der Klasse A aufzubauen. Das Programm des Endgerätes kann versuchen wieder in Klasse B zu wechseln. Dieser Prozess kann sich immer wieder wiederholen.

Um auch innerhalb der minimal 2 Standen in den kein Beacon empfangen wurde einen Kommunikation zu ermöglichen wird jedes Mal wenn ein Beacon verloren geht in den Beacon-Less Modus gewechselt. Dieser Modus orientiert sich ausschließlich an der internen Uhr. Um die Abweichung auszugleichen werden die Empfangsfenster immer früher begonnen und immer später beendet. Das bedeutet einen höheren Energieverbrauch aber auch eine höhere Wahrscheinlichkeit noch Daten zu empfangen obwohl die Uhren des Gateways und des Endgerätes auseinanderlaufen.

4.2.3 Singel / Multicast

In Klasse B können die Nachrichten als Singelcast oder als Multicast Nachrichten verwendet werden. Eine Singelcast Nachricht wird an des Endgerät das im DevAfdr Feld der Nachricht codiert ist gesendet. Im Multicastmodus wird das Paket an mehrere Endgeräte gesendet. Damit dise möglich ist müssen sich die Endgeräte dieselbe Multicast Adresse und die dazugehörigen Schlüssel teilen. Durch verschiedene Multicastadresse ist es möglich sogenannte Multicastgruppen zu erzeugen die nicht alle sonder nur ein Teil aller Endgeräte beinhalten. LoRaWAN gibt allerding keine Methode vor wie die Adressen und Schlüssel verteilt werden. Diese Aufgabe muss in der Applikationsebene sprich im Programm der Endgeräte bzw. des Applikationsserver oder die Schlüssel und Adresse werden fest in den Programmcode programmiert.

In Multicastnachrichten sind keine MAC-Kommandos erlaubt. Nur Daten dürfen als Multicastnachrichten übertragen werden. Dies wurde eingeführt da Multicastnachrichten nicht dieselbe Robustheit wie Singelcastnachrichten haben. Die Nachrichten dürfen nicht bestätigt werden da sonst eine große Last für das Netzt entstehen würde. [SOR17c, S.84]

4.2.4 Beacon

Wie schon erwähnt werden der Beacons verwendet um das Endgerät mit dem Netzwerk zu synchronisieren. Deswegen werden die Beacon Periodisch gesendet. Die Zeit zwischen

zwei Beacon wir BEACKON_Period genannt. Die Endgeräte öffnen Empfangsfenster um diese Beacons zu empfangen. Ein Beacon zu übertragen dauert BEACON_RESERVED lange. Das Beacon-Empfangsfenster wird BEACKON _GUARD früher geöffnet um sicher zu stellen das Beacon auch wirklich erkannt werden kann. Außerdem wird die Beakon_GUARD benutzt um sicherzustellen dass kein Pingslot mehr geöffnet ist. Deswegen muss diese Beakon_GUARD mindestens so lang sein wie ein maximaler Pingslot. Das hat den Vorteil, dass nicht darauf gedacht werden muss wann ein Pingslot geöffnet wurde, da er im Zweifelsfall fertig ist bevor ein Beacon empfangen wird. Vergleichbar ist dies mit der Distributed Coordination die bei WLAN Anwendung findet.

Während versucht wird ein Beacon zu empfangen kann kein Pingslot geöffnet werden

Um Synchronisierungen durch die Beacon zu vermeiden, wie "alle Endgeräte wollen sofort nach den Beacon senden wollen", wird mittels zufälliger Wartezeiten und zufälliger Pingslotperiode verhindert. Durch den Zufall wird die Wahrscheinlichkeit deiner Kollision geringer.

Beacons haben ihr eigenes Paketformat. Diese Pakete sind immer gleich lang. Dadurch kann auf Header verzichtet werden was auch der Verarbeitungsgeschwindigkeit zugutekommt. Wie auch ein normales LoRa-Paket, so besteht auch das erste Feld des Beacon-Paketes aus der Preable. Danach folgt der BCNPayload. Der BCNPayload(Beacon Payload) lässt sich unterteilen in RFU, Time, CRC, GWSpecific, RFU, CRC. Die zwei CRC Felder weisen schon auf die logische Unterteilung in zwei hältern hin. Der erste Teil enthält Beacon spezifische Informationen (time und CRC). In dem Time Feld ist die Zeit seit 00:00:00, 01.01.1980 Modulo $2\hat{3}2$ enthalten. das CRC Feld wird verwendet um die Korrektheit des Zeit und des RFU Feldes zu versichern. RFU steht wieder für "Reserved for Future Usage" und wird nicht verwendet. Die andere Hälfte ist Gatewayspezifisch. Sie enthält das GwSpecific Feld und ein RFU Feld . Beide Fleder sind durch ein zweites CRC Feld abgesichert ist. Das GwSpezific Feld lässt sich unterteilen in InfoDesc und Info Felder. Das InfoDesc gibt an auf was sich das Infofeld bezieht. 0 gibt an das die GPS-Koordinaten der ersten Antenne folgen. 1 steht für die GPS-Koordinaten der zweiten Antenne und 2 steht für die GPS-Koordinaten der dritten Antenne. Die werte 3 bis127 sind noch Solange sich im Info Feld Koordinaten enthalten kann dieses unterteilt werden in Längen- und Breitengrad.

Auch Klasse A kann den Beacon nutzen, um herauszufinden von welchem Gateway es gerade Datenempfängt und um eventuelle Standortwechsel festzustellen.

In Europa werden die Beacons auf einer festen Frequenz übertragen die sich nicht ändert. Nur über das MAC-Kommando PingSlotChannelReq.

4.3 Klasse C

C steht für CONTINUOUSLY Listening. Wie der Name schon sagt ist hier dauernd ein Empfangsfenster geöffnet. Dafür wird es ermöglicht fast Latzen frei zu übertragen. Dies bedeutet aber auch das der Stromverbrauch am höchsten ist und somit die Klasse C nicht für den Batteriebetrieb geeignet.

Geräte die Klasse C implementieren sollen aus nicht die Klasse B implementieren das es sonst zu fejlern kommen kann.

Diese Klasse verwendet die Gleichen Empfangsfenster mit der gleichen Frequenz wie in Klasse A. Der große unterscheid besteht allerdings darin das RX2 immer dann geöffnet ist wenn nicht gerade Daten an das Gateway gesendet werden oder RX1 geöffnet ist.

Auch in Klasse C ist es, wie in B, möglich Multicastnachrichten zu senden. Hierbei gelten die gleichen Regeln wie bei Klasse B.

5 Sicherheit

Sicherheit in Netzwerkfähigen Systemen ist ein scher wichtiges und heiß diktiertes Thema. Da alle LoRa-Geräte über das Medium “Luft“ die Daten übertragen, sind diese auch für alle empfangbar. Deswegen ist es wichtig die Daten zu verschlüssel um zu verhindern das Dritte die Daten mitlesen. genauso wichtig die Daten zu Authentifizierung und somit zu überprüfen wer die Daten gesendet hat. Auch verschlüsselte Daten können von Dritten mitgelesen werden. Allerdings können diese nichts mit den verschlüsselten Daten anfangen. Das einzige was Dritte mit den Daten tu können ist eine sogenannte Replayattack durchzuführen in dem sie das Empfangene Datenpaket nochmal senden und so versuchen die Kommunikation zu stören oder Fehlinformationen zu streuen. Um Replayattack entgegenzuwirken, werden Zähler oder Nonce mit den Daten mitgeschikt. Im folgenden Text wird betrachtend wie LoRa diese Sicherheitsfeatures implementiert hat.

5.0.1 Schlüssel

Schon der Beitritt eines Endgerätes muss verschlüsselt sein. Dafür werden zwei verschiedene Schlüssel verwendet. Die Join-Nachricht wird mit dem JSIntKey(Joining Session Encryption Key) verschlüsselt. Der Schlüssel wird mittels dem der aes128 Verschlüsslung generiert. Speziell wird der NWkKey mit der deinem 16Byte langem Wort verschlüsselt. Das Wort besteht am anfang aus der Konstant 0x06, danach folgt die DevEUI und zum Schluss wird mit ein aufgefüllt. Die Accept-Naxhricht wird ebenfalls verschlüsselt. Allerdings wird her der JSEncKey(Joining Session Encryption Key) verwendet. Dieser wird auf die Gleiche weise erzeugt, allerdings wird bei dem Verschlüsselungswort 0x06 durch 0x05 ersetzt. JSIntKey wird außerdem verwendet um den MIC-Code in der Join-Nachricht zu berechnen.

Alle MAC-Kommandos die an Port 0 gesendet werden, werden separat verschlüsselt. Dies bietet eine Höhere Sicherheit, selbst wenn Daten entschlüsselt werden können, so bleibt es unmöglich falsche MAC-Kommandos zu verschlüsseln und zu einem Endgerät zu senden. Hierzu wird der Network session encryption key (NwkSEncKey) verwedent. Dieser wird auf die selbe weise erzeugt wie JSIntKey. Allerdings besteht hier das Schlüsselwort aus 0x04,der JoinNonce, der JoinEUI und dem DevNonce. Diese Werte werden bei dem Beitritt mittels OTAA erzeugt. Siehe: **??**.

Um die Integrität der Daten zu bestimmen werden zwei schlüssel verwedent. Der FNwkSIntKey oder lang Forwarding Network session integrity key wird benutzt um den MIC-Code für die Integritätbestimmung abzuleiten. Auch dieser Schlüssel wir wie JSIntKey abgeleitet aber das Schüsselwort besteht aus 0x01, der JoinNonce , der JoinEUI und DevNonce. Der SNwkSIntKey(Serving Network session integrity key) stellt das gegenstück da und wird verwendet den MIC-Code zu testen ab nichts verändert wurde. Hier besteht das Schlüsselwort aus 0x03, der JoinNonce, der JoinEUI und der DevNonce.

JSEncKey, JSIntKey, FNwkSIntKey, SNwkSIntKey, NwkSEncKey sind für jedes Entgerät unterschiedlich.

Momentan sind nur die MAC-Kommentare vor dem Mitlesen geschützt. Natürlich müssen auch die mitgelieferten Daten geschützt werden. Dies geschieht unter Verwunderung des AppSKeys. Der Applikaction Session Key wird von dem Applikationsserver und dem Endgerät verwendet. Dieser Schlüssel wir vom Programmierer vorgegeben, da er mit

dem Schlüssel des Applikationsserver übereinstimmen muss. [SOR17c, S.50 ff]

5.1 Zähler

Jedes Endgerät hat drei verscheidene Counter. Ein Framecounter für Uplinkframes FCntUp und zwei für Downlinkframes NFCntDown und AFCntDown.

Der FCntUp counter wird für jeden Uplink der gesendet wird erhöht. Der stand wird in das FCnt feld der Nachricht mit eingefügt. Da das Gatway den selben zähler hat, kann es erkennen ob die Nachricht schon einmal gesendet wurde in dem es nur Nachrichten mit einem gößeren FCnt Wert als der eigene FCntUp Zähler enthält.

Genau so wird mit den Downlink counter verfahren, bloß auf dem Endgerät. Im NFCntDown Zähler werden die MAC-Kommando Nachrichten gezählt. AFCntDown wird für alle anderen Nachrichten verwendet. [**?**, S.22 ff]

Literatur

[CB+17] Cheong, Phui San, Johan Bergs, , Chris Hawinkel und Jeroen Famaey: *Comparison of LoRaWAN Classes and their Power Consumption.* https://ieeexplore.ieee.org/abstract/document/8240313, November 2017. Eingesehen am 09.04.2019.

[GAS17] GEMALTO, ACTILITY und SEMTECH: *LoRaWAN™SECURITYA WHITE PAPER PREPARED FOR THE LoRa ALLIANCE™.* https://lora-alliance.org/resource-hub/lora-alliance-security-whitepaper, Februar 2017. Eingesehen am 09.04.2019.

[SOR17a] SORNIN, N. (Herausgeber): *Exploring LoRa and LoRaWAN(todo).* Lora-Alliance, https://tools.ietf.org/pdf/rfc8376.pdf, 1.1 Auflage, Oktober 2017. Eingesehen am 09.04.2019.

[SOR17b] SORNIN, N. (Herausgeber): *LoRaWAN™ 1.1 Backend(todo2.* Lora-Alliance, https://tools.ietf.org/pdf/rfc8376.pdf, 1.1 Auflage, Oktober 2017. Eingesehen am 09.04.2019.

[SOR17c] SORNIN, N. (Herausgeber): *LoRaWAN™ 1.1 Specification.* Lora-Alliance, https://tools.ietf.org/pdf/rfc8376.pdf, 1.1 Auflage, Oktober 2017. Eingesehen am 09.04.2019.

[Tec15] TechnicalMarketingWorkgroup1: *A technical overview of LoRa® and LoRaWAN™.* https://lora-alliance.org/resource-hub/what-lorawantm, November 2015. Eingesehen am 09.04.2019.