

# Seminararbeit: Lorawan

Tobias Sigmann

15. Mai 2019

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung in Lora</b>	<b>4</b>
<b>2</b>	<b>Aufbau eines Lora-Netzwerk</b>	<b>5</b>
2.1	Gateway . . . . .	5
2.2	Netzwerkserver . . . . .	7
2.3	Applicationsserver . . . . .	7
2.4	Join-Server . . . . .	8
2.5	End-Gerät . . . . .	8
<b>3</b>	<b>Lora Funktionsweise</b>	<b>8</b>
3.1	Schichtenmodell . . . . .	9
3.2	Netzwerkbeitritt . . . . .	9
3.2.1	OTAA . . . . .	9
3.2.2	ABP . . . . .	11
3.3	Protokoll . . . . .	11
3.4	Übertragungsart . . . . .	12
3.4.1	Adaptive Data Rate . . . . .	12
3.4.2	Notitz: protokoll/paket hierfor erklären . . . . .	13
<b>4</b>	<b>Lora Geräte Klassen</b>	<b>13</b>
4.1	Klasse A . . . . .	13
4.1.1	Uplink . . . . .	14
4.1.2	Downlink . . . . .	14
4.2	Klasse B . . . . .	15
4.2.1	Klassenwechsel A nach B . . . . .	16
4.2.2	Uplink . . . . .	16
4.2.3	Downlink . . . . .	16
4.3	Klasse C . . . . .	17
<b>5</b>	<b>Sicherheit</b>	<b>17</b>
<b>6</b>	<b>Live-Beispiel</b>	<b>18</b>

7	Fazit	18
8	Sonstige quellen	18

# 1 Einführung in Lora

Lora ist ein Low Power, Wide Area (LPWA) Netzwerkprotokoll und somit sehr gut für batteriebetriebene kabellose Geräte geeignet. Deswegen wird Lora auch oft im Internet of Things (IoT) Bereich verwendet. Mittels der bidirektionalen Kommunikation ist es möglich Daten und Befehle über weite Strecken zu übertragen. Leider leidet darunter die Geschwindigkeit, sodass sich Lora nicht als WLAN Ersatz eignet. Trotzdem können zwischen 0.3 und 50 kbps erreicht werden. In Europa werden 863 MHz bis 870 MHz verwendet. Allerdings variiert der Frequenzbereich für andere Kontinente. Je nach Bedingungen können so bis zu 20km entfernte Endgeräte erkannt und mit diesen kommuniziert werden. Es ist sogar möglich den Standort des Gerätes zu bestimmen.

Eine Alternative zu Lora ist Sigfox, hierauf werde ich nicht weiter eingehen. LoRaWAN 1.1

[Tec15](Optimiert für Batterie Kapazität(Teilnehmer) Reichweite, Kosten mehrjährige Batterielaufzeit, kleine Datenmengen, große Reichweite, LPWAN (Low Power WAN)

Kriterien für Lora: Netzwerk Architektur, Reichweite, Batterielaufzeit, Interferenzrobustheit, Anzahl Knoten, Sicherheit, bidirektionale Kommunikation, verschiedene Anwendungsunterstützung

Orientiert für Mobile Adressierbare Endgeräte)

[AVTP<sup>+</sup>17](alternativen: Sigfox, Ingenu, Dash7

Klassen Kompromiss zwischen Reichweite, Performance(Latenz/ Durchsatz) und Energiebedarf

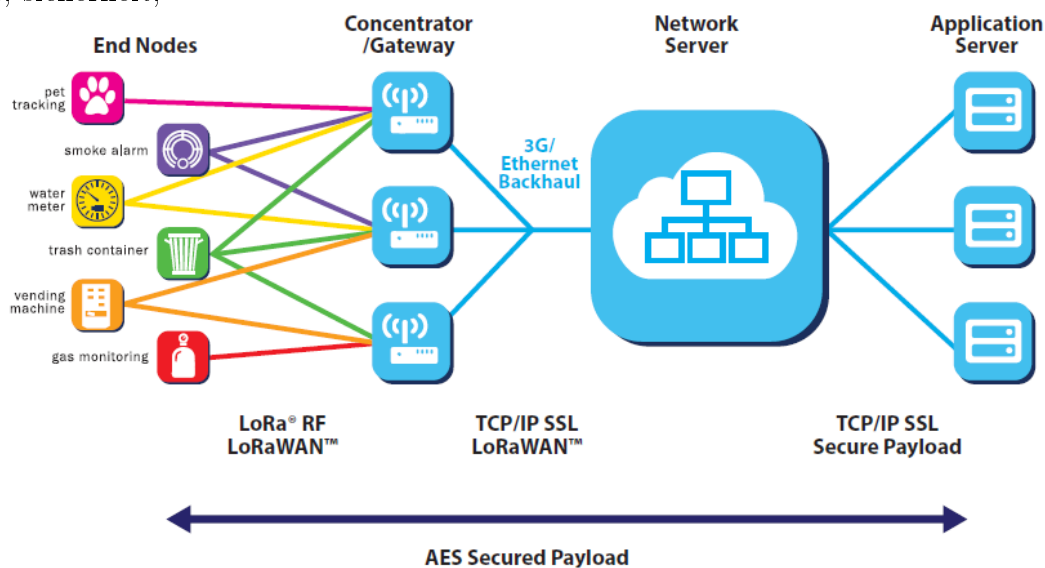
Energiesparend durch ADR (Adaptive Daten Rate) )

Es wird folgen: Was ist lora, wo und wofür wird es benutzt, wie weit kann man senden und wie schnell...

## 2 Aufbau eines Lora-Netzwerk

Lora wird auch deswegen gerne für IoT-Geräte verwendet, weil der Netzwerkaufbau ermöglicht die über Lora verwendeten Daten im Internet abzurufen und so ohne weiteres das Gerät mit dem Internet zu verbinden. Um die von den End-Geräten gesendeten LoRa Pakete auf IP/TCP Pakete umzusetzen wird ein Gateway benötigt, das auf der einen Seite LoRa pakete empfängt/sendet und auf der anderen Seite TCP/IP Pakete verwendet. Das Gateway implementiert aber keinerlei Logic. Hierzu ist ein Netzwerkservers zuständig der durch die Gateways das Netzwerk kontrolliert und steuert. Gleichzeitig stellt er die Verbindung zu einem Applicationsserver her an den er die vom Gateway empfangenen Daten sendet und von dem auch Daten an die Endgeräte, wieder über das Gateway, gesendet werden. Diese Architektur wurde gewählt um die Laufzeit der End-Geräte, Anzahl der End-Geräte, Qualität des Signals und Sicherheit des Netzwerkes möglichst hoch zu halten.

[Tec15](Architektur hat großen Einfluss auf Batterie, Anzahl Teilnehmer, Qualität, Sicherheit,



### 2.1 Gateway

Das Teilnetz, das aus dem Gateway und mehreren LoRa-End-Geräten besteht, ist sternförmig aufgebaut. Jedes End-Gerät kommuniziert direkt mit dem Gateway. Diese Art der Kommunikation wird auch (Single-Hop-Connection) zu Deutsch

(Einfacher-Sprung-verbindung) genannt, da die Gesendeten Daten ohne umwege an das Gateway gesendet werden. Jedes Gateway ist mit einem Netzwerkserverserver verbunden.

Ein Endgeräten kann gleichzeitig an mehreren Gateways senden. Der Netzwerkserverserver ist zuständig die Pakete auf Dublikate zu überprüfen und nur solche nur einmalig an die Applikation zu senden. Ein weiterer Vorteil ist das kein Handover nötig ist, da alle Gateways fähig sind die Daten des Endgeräts zu verarbeiten bzw. weiterzusenden.

Durch die Sternförmige Architektur des Netzes und die Fähigkeit von allen in der Reichweite befindlichen Endgeräten Daten zu empfangen, muss ein Gateway mit vielen End-Geräten kommuniziert. Da es nicht möglich ist mit jedem Gerät nacheinander zu kommunizieren, muss dies gleichzeitig geschehen. Hierzu werden adaptive Datenraten und Mehrkanal-Multi-Modem-Transceiver verwendet um eine hohe End-Geräteanzahl zu ermöglichen. Außerdem hängt die Anzahl der Teilnehmer davon ab wie geschickt die Kanäle gewählt wurden, welche Datenraten verwendet werden und wie lange gesendet werden muss um die Daten zu senden (man spricht auch von der "Time-On-Air").

Durch die genannten Eigenschaften der Gateways wird auch eine gute Skalierbarkeit erzielt. Dadurch kann ein neues Gateway die Anzahl der Knoten um das 6 bis 8-fach erhöhen.

[Tec15] (Meistens wird ein netzförmiges Netz aufgebaut. Knoten leiten Nachrichten weiter => größere Reichweite aber kompliziert, erlaubt weniger Teilnehmer und energieaufwändig).

Lora Sternförmig => Energie-effizient, Knoten senden direkt an Gateways. Gateways senden an Server, Server muss doppelte Pakete filtern, Sicherheitscheck, ACK über bestes Gateway senden, datenrate anpassen.

Keine Handover

Gateway müssen viele Geräte handeln da Stern. erreichen durch (adaptive Datenrate, multi channel/multi modem transceiver) mehrere Nachrichten auch verschiedenen Channels gleichzeitig empfangen

Wichtige Faktoren (anz. channels, datenrate (time on air), payload länge, Sendehäufigkeit)

Skaliert sehr gut => gemacht für große Nutzerzahlen Neues gateway kann Knoten 6-8 x verbessern ) [SOR17]( Applikation Server -> Zentraler Server(leitend Pakete weiter) -> Gateway(wandelt lorawan in ip Pakete um) -> Endgerät/Knoten )

## 2.2 Netzwerkserver

Der Netzwekserver ist das "Herzstück eines jeden Lora-Netzwerkes. Im fallen viele Aufgaben zu. Er kann mit mehreren Gatways und mehreren Applications-server verbunden sein.

Die wichtigste Aufgabe ist das Steuern des Lora-Teils des Netzwerkes. Der Server verwaltet jedes End-Gerät separat indem es mit ihm den zu verwendn Kanal aushandelt und die datenrate adaptiv kontrolliert wenn ADR(Adaptiv Data Rate) verwendet wird. Weiterhin überprüft er die empfangen Pakete auf ihre Korrektheit und Integrität und filtert Duplikate ,die druch das Empfnagen des gleichen Signales an verschiendne Gatways, verursacht wurden. Dabei ermittelt er auch das Gateway das den besten empfang zu de ENd-Gerät hat und nutzt dieses um Daten an das endgeröt zu senden. Es ist nicht immer möglich Daten direkt zu senden. Um die Appliaktion-Server zu endlasten Puffert der Netzwerkserver die Daten und sendet sie zum nächst möglichem Zeitpunkt zu senden. Desweiteren muss er die empfnagenen Pakte "bestätigen und leitet join requests an den joiserver weriter

Eine weitere sehr Wichtige Ausgabe ist es eine APi für den Applikations-server bereitzustellen um eine einfache und shnelle kommunikation zu ermöglichen.

[SOR17]( Sicherheit(zähler, ...), leited pakete weiter, filtert pakete, merher gateway via ip verbunden, kontrolliert datenrate, chanäle, adaptiv data rate api.

## 2.3 Applicationsserver

Dieser Server ist zuständig den die gesendete Nachrichten zu verarbeiten und gegebenenfalls selbst welche an die Endgeräte zu senden.

## 2.4 Join-Server

Ein Join-Server wird benötigt um den Beitritt mittels OTAA zu ermöglichen. Der Server kann an mehrere Netzwerkserver verbunden sein und jeder Netzwerkserver kann mehrere Join server haben. Wenn ein Endgerät dem Netzwerk beitreten möchte leitet der Netzwerkserver die anfragen an den JoinServer weiter. Dieser führt dann die nötigen schritte des Beitritts aus wie z.B. ableiten von Schlüsseln. Um dies zu tun muss ihm der NwkKey und der AppKey bekannt sein, da diese zum verschlüsseln der Nachrichten verwendet werden aber aus sicherheitsgründen nie über das Netz gesendet werden.

## 2.5 End-Gerät

Endgeräte sind Geräte die Informationen mittels Lora empfangen oder senden. Jedes End-Gerät ist mit einem bestimmten Applikationsserver verbunden.

Jedes Endgerät muss zur korrektur funktion mehrere wichtige Informationen Speichern.

ist das  
wichtig?

- DevEUI: Globale endgerätid die eindeutig für jedes endgerät definiert ist. (wie mac eines computers)
- JoinEUI: Globale Adresse des JoinServers an den die anfrage gehen soll. wird nur für OTAA geräte benötigt.
- NwkKey und AppKey: Werden verwendet um spätere Schlüssel abzuleiten und die kommunikation während des Joinens abzusichern. Dafür müssen sie sowohl dem Join-Server als auch dem Endgerät bekannt sein da sie nie übertragen werden.

## 3 Lora Funktionsweise

) [SOR17]( Geschwindigkeit ist kompromiss zwischen abstand/geschw. die untersch frequenzen bzw. geschwindigkeiten beeinflussen sich nicht gegenseitig => keine interferenz ) Die Datenrate ist einstellbar, jedoch wird die Reichweite bei höherer Datenrate gemindert. Ein Vorteil von Lora ist, dass die einzelnen



Datenraten nicht interferieren und so jedes Endgerät seine eigene Datenrate unabhängig von den anderen Verwenden kann. Außerdem wird die Datenrate und die Sendeleistung für jedes Gerät separat gesteuert (ADR, Adaptive Data Rate) [SOR17] [Tec15]()

### 3.1 Schichtenmodell

[Tec15](  
Application  
Lora MAC  
MacOptins(Classes)  
LoraModulation(Regionales ISB) ) Lora: Long Range ist Physikalische schicht(gibt an wie die kabellose übertragung geschieht) LoraWan:protokoll das.

### 3.2 Netzwerkbeitritt

End-Geräte sind immer bestimmten Netzwerken zugeordnet. Es gibt zwei wege um ein neue End-geräte zu einem bestehenden Netzwerk hinzuzufügen.

[SOR17](wei arten OTAA(Over the air activation), ABP(Activation by Personalization) Jedes gerät hat eine vorgegebene DevEUI (wie MAC adresse eines PCs), JoinEUI muss angegeben werden und adressiert den Join server ) Was macht

ABP steht für Activation by Personalization und bedeutet Wörtlich übersetzt Aktivierung durch Personalisierung. der? wohin

#### 3.2.1 OTAA

Die sicherste aber auch aufwendigste methode um ein End-Gerät mit einem Netzwerk zu verbinden heißt OTAA (Over-the-Air Activation). Hierbei muss jedes mal wenn einem Netzwerk beigetreten werden soll die Join-Prozedur ausgeführt werden. Hierfür müssen folgende 4 Werte Vorgegeben werden. DevEUI, JoinEUI , NwkKey, AppKey(Verschlüsselung des join requests). da- mit? umschreiben !!!!!

Als erstes muss das End-Gerät eine join- oder rejoin-Nachricht senden. Die Nachricht besteht aus der JoinEUI, dem DevEUI und einer DevNonce.

Mit der DevNonce sollen replayattacks verhindert werden. Sie ist das beim ersten Join request 0 und sollte sich bei jedem Join-Request erhöhen. Außerdem muss sie auch dann noch gespeichert werden wenn kein Strom zur Verfügung steht. Falls von dem gleichen Endgerät eine Join-Request mit einer zu kleinen DevNonce empfangen wird, wird die Nachricht ignoriert und es ist nicht möglich dem Netzwerk beizutreten.

Die Accept Nachricht besteht aus einer JoinNonce, einem NetzwerkID Net\_ID, einer Geräteadresse DevAddr, einem Einstellungsfeld DLSettings, einer Angabe wie lange auf eine Antwort nach dem Senden gewartet werden muss RxDelay und einer optionalen Liste an Netzwerkparametern CFList. Die JoinNonce wird außerdem benutzt im Schlüssel wie AppSKey, ... herzuweisen. Für jedes Endgerät wird eine eigene JoinAccept nonce geführt, sie sollte sich nicht wiederholen. Jedes Endgerät merkt sich die letzte JoinNonce und tritt auch nur bei wenn diese größer ist als die letzte empfangene.

Der NWKKEY ist für die Verschlüsselung der Datenpakete bis zu Gateway zuständig. Auch dieser Key wird vom Netzwerkserver erzeugt und muss manuell in den Code eingetragen werden.

Der letzte Wert heißt APPSKEY und sichert die Kommunikation vom Endgerät zu dem Applikationsserver ab. Der Schlüssel wird genau wie der NWKKEY vom Netzwerkserver erzeugt und verwaltet.

Mehr Informationen zu den verschiedenen Schlüsseln finden Sie in dem Kapitel Sicherheit.

Wenn der Netzwerkserver den Beitritt des Endgerätes erlaubt sendet er eine Join-Accept Nachricht zurück. Das Endgerät erwartet die Nachricht nach JOIN\_ACCEPT\_DELAY1 oder JOIN\_ACCEPT\_DELAY2 nach dem Senden des Request. Sollte die Join-Accept Nachricht zu einem anderen Zeitpunkt gesendet werden, wird diese nicht empfangen weil das Endgerät nicht empfangsbereit ist. Die Nachricht enthält Einstellungen für das Endgerät sowie die ID des Netzwerkes und die neue Adresse für das Endgerät. Um Replayataken zu verhindern enthält die Nachricht zusätzlich eine JoinNonce. Diese wird für jedes Endgerät separat geführt und muss größer sein als die zuletzt gesendete.

### 3.2.2 ABP

Die einfachste Art des Beitritts heist ABP was für Activation by Personalization zu deutsch Aktivierung durch Personalisierung steht. Hierbei muss lediglich vor inbetriebnahme des End-Gerätes 3 Konstanten definiert werden. Manche Hersteller "brennen" diese drei Werte fest in den chip ein, sodass er nicht geändert werden kann. Falls es nicht möglich ist dem hersteller die gewünschten werte zukommen zu lassen, sind solche End-Geräte nicht für den Beitritt mittels ABP geeignet.

Als erstes muss die DeviceAddress angegeben werden. Diese Adresse existiert nur einmal im Netzwerk und wird verwendet um das Endgerät zu identifizieren. Die Adresse wird vom Netzwerkserver erzeugt und muss manuell von dort kopiert werden. Die verwendete frequenz entspricht der RX1 bzw RX2 ausgehend aus dem kapitel Klasse A.

Mit hilfe dieser 3 Werte kann die Join-Request - Join-Accept prozedur übersprungen werden. Daher kann das Gerät direkt einen Lora-netz beitreten wenn es angeschaltet wird und muss nicht erst alle schlüssel neu ableiten und aushandeln. Allerdings ist diese methode deswegen weniger sicher, da immer die selben schlüssel verwendet werden.

Nach der verbindung muss das ResetInd Mac command im FOpt field gesendet werden solange bis ein ResetConf erhalten wird. Nun ist das Gerät im netzwerk und kann unter der eingestellten Adresse und mit den eingestellten schlüssel arbeiten.

Sobald dem Netzwerk erfolgreich beigetreten wurde werden ein die benötigten schlüssel aus dem vorher gesetzten Werten abgeleitet. genauers dazu in kapitel Sicherheit.

### 3.3 Protokoll

[SOR17] (Mac commands werden benutzt um geräte zu steuern => frequenzen zu ändern, ... Application wird diese nie erhalten, läuft zwischen netzwerkserver und lora gerät ab. Verschlüsselt hier oder da. aufbau: 1byte command, x byte extra data. müssen vom empfanher acknolaged werden. Reihenfolge

ist zu beachten. Alle Nachrichten in einem Frame müssen auch in einem Frame  
ack werden. => Macbuffer ermöglicht dies. Wenn buffer überleuft werden die  
ältesten ack. )

(Was  
pas-  
siert  
mit  
dem  
rest?

### 3.4 Übertragungsart

[SOR17]( Knoten können zu jeder Zeit, auf beliebigen Kanälen, beliebig schnell,  
beliebig lange senden, solange folgende Regeln befolgt werden.

- Channels werden per Pseudozufallszahl geändert
- Sendezeit erfüllt die Regionalen Bestimmungen

)

[AVTP<sup>+</sup>17]( Chirp Signal => Zeitliche Änderung in Trägerfrequenz(höhere  
Frequenz als Datenrate)(positiv chirp/negativ chirp)

Datensignal wird in Chirp Signal moduliert. Resultierende Signal ist breit-  
bandiger als Datensignal. Maximale Datenrate auch mit Rauschen erreichbar.

Durch orthogonale SSspread Factor"mehrere Signale auf einem Channel )  
[Tec15](normal FSK, schon sehr effizient. Lora "chirp spread spectrum modulation". Ist wie FSK aber größere Reichweite, robuster. Stammt aus dem Militär/raumfahrt.Lora als erstes für kommerziellen billigen Einsatz.

Spread spectrum => Signale sind Orthogonal für versch. Spreizraten, faktoriell  
koreliert mit Datenrate => verschiedene Datenraten auf einem Kanal

Nähere Geräte sind schneller => höhere Datenrate => kürzere Übertragungsdauer und lassen somit mehr Zeit für andere, => bessere Batterielaufzeit. Deswegen sind symmetrische up/downlinks nötig.) Frequenzhopping, spread spectrum, code-channels

#### 3.4.1 Adaptive Data Rate

[AVTP<sup>+</sup>17]( Datenrate und Funkfrequenz(RF) werden passend zum Abstand angepasst

nahe Knoten => hohe Datenrate => kurze Sendezeit => weniger RF-Power kann nach Bedarf geändert werden

=> immer möglichst schnelle senden => weniger Energie

)

### 3.4.2 Notitz: protokoll/paket hierfor erklären

## 4 Lora Geräte Klassen

[SOR17](GGeräte müssen mindestens A können, alle die mehr können werden auch "high class End-Devices" genannt) Vielleicht zu klein => in anderes Kapitel stopfen. Bei mehrfacher übertrageung wird nicht erhöht

Die Endgeräte sind je nach Kommunikationsart/Protokoll Art in drei Klassen (A, B und C) unterteilt.

Jede Klasse hat 3 counter FCntUP(Pro uplink ++), FCNTDown(pro downlink auser port 0 => mach), AFCntDown(port ungleich 0 dann ++) (nur beschreiben wie diese grob funktionieren) Zähler sollen nicht flüchtig sein(Batteriewechseln kein reset) bei neuverbinden müssen alle counter auf 0 gesetzt werden. counter müssen auf beiden seiten gleich gehalten werden(Synchron geführt) Wenn nachricht empfangen ist muss der darin enthaltenene counter größer sein als der eigene.

die Counter Werte sollen so weit wie möglich nur einam verwendet werden.

) [CB<sup>+</sup>17] [Tec15](Asynchrone Knoten wegen Batterie => Event/Scheduler gesteuert verwendet ALOHA

Normal Netze müssen sich synchronisieren und Nachrichten abrufen. Lora partiell nicht => laut GSMA 3 bis 5 fach effizienter)

zur besseren Anpassung/ Anpassung an Batterie

EU: 10 Kanäle (8: 250bps bis 5.5kbps) (1: FSK 50kbps) (high rate Lora 114kbps)

)

### 4.1 Klasse A

Klasse A zeichnet sich durch sehr geringer Stromverbrauch aus. Die Kommunikation kann bidirektionalen Stadtfinden, allerdings muss die Kommunikati-

on von dem Endgeräte gestartet werden. Das bietet die Möglichkeit das das Endgerät, wenn keine Daten gesendet werden müssen, in einen sehr sparsamen Schlafmodus wechselt. Um das Endgeräte nicht zum aufwachenßwingen zu müssen, wurde auf einen "Hardbeatöder ähnliches verzichtet. Das Endgerät kann so lange ßchlafen"wie es möchte. Dadurch ist die Klasse A auch die potenziell Stromsparende Endgeräteklasse.

Das Endgerät startet die Kommunikation in dem es Daten an das Gateway sendet(uplink). Daraufhin hat das Gateway die Möglichkeit 2 mal Daten zum Endgeräte senden(downlink). Da die Kommunikation asynchron Stadtfinden wartet das Endgeräte bis es beide uplinks empfangen hat.gewünscht.

Um zu ermitteln, wann gesendet werden darf, wird das ALOHA-Protokoll verwendet. Da das Gateway nicht immer Daten an die Endgeräte senden kann, muss es diese zwischenspeichern um diese bei der Nächsten Kommunikation zum senden. [SOR17](Es wird zwischen up- / downlink unterschieden)

#### 4.1.1 Uplink

[SOR17] (vom Knoten zum Gateway(1..n), Lora radio packet mode, (Preamble, PHDR, PHDR\_CRC, PHYPayload, CRC(cyklische Redundanz Prüfung))) )

#### 4.1.2 Downlink

[SOR17] ( radio packet explicit mode, vom Gateway(1) zum Knoten(1), ausgelöst vom Netzwerkservers, auch multikasts möglich, (Preamble, PHDR, PHDR\_CRC, PHYPayload) Um Nachricht kurz zu halten kein CRC am ende, nach Receiver\_Delay1 / Reciever\_Delay2 kann empfangen werden (rx1, rx2)

Fenster müssen lange genug für Preamble auf bleiben=> wenn erkannt wird empfangen wenn nicht fenster weider zu. Es darf nur gesendet werden wenn beide fenster zu sind. Es ist auch erlabut andere protokole zu sprechen wenn nicht gesendet oder gehört wird. )

**4.1.2.1 Rx1** [SOR17]( Frequenz abhängig von Uplinkfrequenz, Datenrate abhängig on Uplinkdatenrate, wird nach Reciever\_Delay 1 +/- 20 msec er-

wartet, Datenrate auch abhängig von Regionalen regeln, Standard: Datenrate = Uplinkdatenrate )

**4.1.2.2 Rx2** [SOR17]( feste Frequenz/Datenrate, nach Delay2 +/- 20 msec, Frequenz/Datenrate mittels MAC änderbar ) [SOR17]( Öffnungslänge muss für Preamble ausreichen, nach RX1 + MIC und Authentizitätscheck muss nicht zwingen RX2 geöffnet werden, Sender muss in einem der beiden Fenster stattfinden, Falls Downlink über beide Fenster => Frames müssen gleich sein. Knoten dürfen nicht während empfangen/ zwischen RX1 und RX2 senden, andere Protokolle dürfen gesprochen werden wenn gesendet werden darf )

## 4.2 Klasse B

Die Klasse B bietet bidirektionale Kommunikation mit einer deterministischen Downlink Latenz. Um diese Latenz zu gewährleisten, muss die Kommunikation Synchron ablaufen. Außerdem muss festgestellt werden, ob das Endgerät bzw. das Gateway noch in Reichweite ist. Dies wird mittels eines periodischen "beacon" zu festgelegten Zeitpunkten gesendet werden realisiert.

Die Latenz ist einstellbar und kann bis zu 128 Sekunden.

Obwohl das Endgerät durch die periodischen "beacons" nicht schlafen kann, ist die Klasse B für den Batteriebetrieb gedacht. [SOR17](wird verwendet wenn mehr Bedarf für Empfangsfenster ist. Hierzu ist ein Synchronsignal nötig => zu bestimmten Zeiten kann damit empfangen werden Gateway sendet Beacon für Synchronisation. Um Daten empfangen zu werden werden Empfangsslots => Pingslots verwendet, werden periodisch geöffnet und mittels Beacon synchronisiert. Normalerweise werden diese schnell geschlossen außer es wird etwas empfangen. Gateway dessen Beacon benutzt wird, wird nach Empfangsqualität ausgewählt. Wenn neuer/unbekannter Beacon von einem anderen Gateway empfangen wird, wird der Netzwerkservers benachrichtigt und dieser entscheidet welcher verwendet wird (passt rote an).

Das Netzwerk muss die Standard Ping-slot Periode, Datenrate und Kanal

kennen.

Um ein gerät auf klasse B zu kommen muss erst von Klasse A gewechselt werden.

Entgeräte müssen Netzwerkserver über position nformieren. Dies kann über eine leere nachricht passieren oder eine normale(uplink).

Das beacon und die enthaltenen daten werden an die applikation geschiht. Der server kann den beacon auswerten. ziwischen beacon und uplink wird random time verwendet um kolisionen zu verhindern . änderungen an pingslot- periode .. muss mitgeteilt werden. Hierzu ist klasse A nötig => wechel zu A, wechel zu B.

Beacon wird genutzt um clockdrivt auszugleichen. Wenn kein beacon empfanen wird => Bacenless mode. Dieser wird bis zu 2 stunden beibehalten. Reines verlassen auf interne Uhr. Wenn beacon empfagne wird, wird zeit zurückgesetzt. )

#### 4.2.1 Klassenwechsel A nach B

[SOR17]( Endgerät fart LoRaWAN layer an. Layer sucht beacon. Mac command DeviceTlmeReq um schneller bacon zu bekommen nutzen. Danach wird das ClassB feld auf 1 gesetzt. Bei den geöffneten fenstern wrd der maximal mögliche clockdrift berücksichtigt. Downlink läuft wie bei A ab.

)

#### 4.2.2 Uplink

[SOR17](Wie bei)

#### 4.2.3 Downlink

[SOR17](wie bei A, frequenzplan kann sich unterschieden. AUch Multikasts möglich,)

##### 4.2.3.1 Singelcast [SOR17]()



**4.2.3.2 Multicast** [SOR17]( separate Adresse für Multicast Festgelegt durch layer oder manuell für gruppenmulticast Nicht führ MAC geeignet, )

## 4.3 Klasse C

Um eine möglichst geringe/keine Latzen zu erzielen ist die Klasse C gemacht. Dies bedeutet aber auch das der Stromverbrauch am höchsten ist und somit nicht für den Batteriebetrieb geeignet. Das Gateway kann immer Daten senden außer wenn das Endgerät gerade Daten sendet. Hier sind Geschwindigkeit von bis zu 50mb möglich.

Es ist auch möglich während des Betriebes eines Endgerätes die Klasse zu wechseln. Dies wird am häufigste zwischen A und B getan/ ist nur zwischen A und B möglich. [SOR17]( öffnet RX1 und RX2 fenster wie in Klasse A. Immer wenn nicht gesendet wird oder RX1 offen ist, ist RX2 offen. Multicast ist auch möglich. )

## 5 Sicherheit

Lora bietet die end-to-end Sicherheit an, indem es die Signale zweimal verschlüsselt.

Die erste Verschlüsselung dient dazu die gesendeten Daten vor eventuellen Mithörern zu verschlüsseln. Die Verschlüsselung geschieht mit einem 128-bit Network-Session-Key.

Die zweite Verschlüsselung wird bis zur endgültigen Weiterverarbeitung der Daten auf z.B. einen Server verwendet und ist ein 128 bit Application-Session-Key.

Das zur Verschlüsselung verwendete Protokoll ist AES. Auch zu Authentifizierung und zur Überprüfung der Integrität wir AES verwendet. [GAS17] [Tec15](Applikationsverschlüsselung(schutz der Daten for mitlesen) Netzwerk(Autentiizierung der Knoten) AFS, Key Exnage IEEE EU164) [SOR17](symetrischer Schlüssel => nur einer benötigt, Sessionkey ist abgeleited von Knoten-rootkey. JoinServer setllt verbindung der Keys her. )

## 6 Live-Beispiel

wenn vorhanden.

## 7 Fazit

## 8 Sonstige quellen

<https://lora-alliance.org/resource-hub> QuickStart für ein kleines Projekt:  
<https://www.thethingsnetwork.org/docs/devices/node/quick-start.html#setup-arduino-ide>

Weitere Infos [http://www.multitech.com/documents/publications/marketing-guides/lora\\_device\\_dev\\_guide\\_orange.pdf](http://www.multitech.com/documents/publications/marketing-guides/lora_device_dev_guide_orange.pdf)

# Literatur

- [AVTP<sup>+</sup>17] ADELANTADO, FERRAN, XAVIER VILAJOSANA, PERE TUSET-PEIRO, BORJA MARTINEZ, JOAN MELIÀ-SEGUÍ und THOMAS WATTEYNE: *Understanding the Limits of LoRaWAN*. <https://ieeexplore.ieee.org/abstract/document/8030482>, September 2017. Eingesehen am 09.04.2019.
- [CB<sup>+</sup>17] CHEONG, PHUI SAN, JOHAN BERGS, , CHRIS HAWINKEL und JEROEN FAMAHEY: *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<sup>TM</sup> SECURITY WHITE PAPER PREPARED FOR THE LoRa ALLIANCE<sup>TM</sup>*. <https://lora-alliance.org/resource-hub/lora-alliance-security-whitepaper>, Februar 2017. Eingesehen am 09.04.2019.
- [SOR17] SORNIN, N. (Herausgeber): *LoRaWAN<sup>TM</sup> 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<sup>TM</sup>*. <https://lora-alliance.org/resource-hub/what-lorawantm>, November 2015. Eingesehen am 09.04.2019.