Seminararbeit: Lorawan

Tobias Sigmann

22. Mai 2019

Inhaltsverzeichnis

1 Einführung in Lora

Lora ist ein Low Power, Wide Area (LPWA) Netzwerkprotokoll und somit sehr gut für batteriebetriebene kabellose Geräte geeignet. Deswegen wir Lora auch of 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, sodas 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, hierrauf 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, Interreferenzrobustheit, Anzahl Konten, Sicherheit, bidirektionale Kommunikation, verschiedene Anwendungsunterstützung

Orientiert für Mobile Adressierbare Endgeräte)
[AVTP+17](alternativen: Sigfox, Ingneu, Dash7

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

Energiesparend durch ADR (Adaptive Daten Rate))

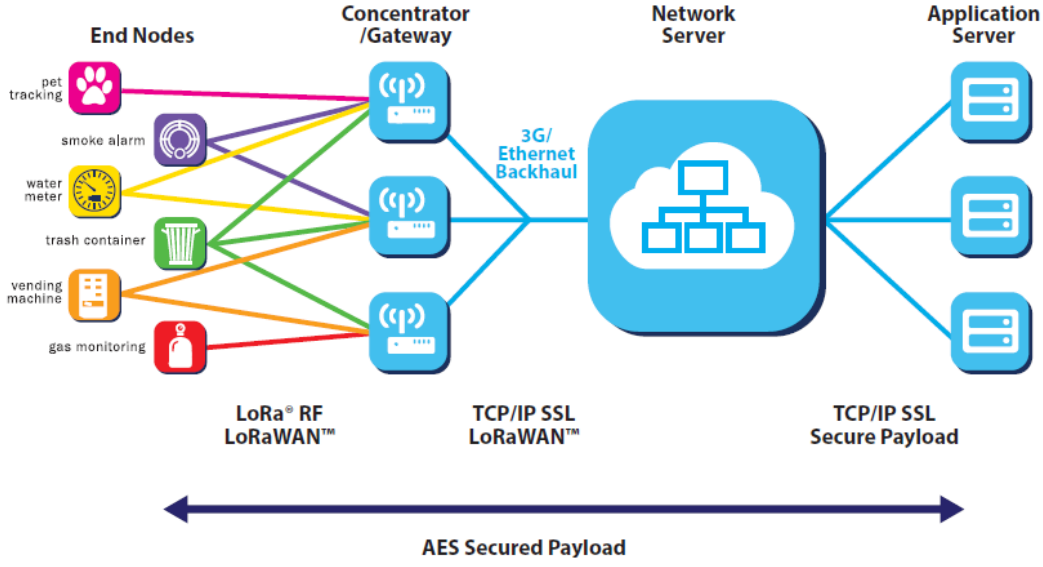
Es wird folgen: Was ist lora, wo und wofür wird es benutzt, wie weit kann man senden und wie schnell...

2 Aufbau eines Lora-Netzwerk

schreib

Lora wird auch Deswegen gerne für IoT-Geräte verwendet, weil der Netzwe- viel-
kaufbau ermöglicht die über Lora verwendeten Daten im Internet abzurufen leicht
und so ohne weiteres das Gerät mit dem Internet zu verbinden. Um die von den noch
End-Geräten gesendeten LoRa Pakete auf IP/TCP Pakete umzusetzen wird hinzu
ein Gateway benötigt, das auf der einen Seite LoRa pakete empfängt/sendet das
und auf der anderen Seite TCP/IP Pakete verwendet. Das Gateway implemen- die
tiert aber keinerlei Logic. Hierzu ist ein Netzwerkserver zuständig der druch geräte
die Gateways das Netzwerk kontrolliert und seuert. Gleichzeitig stellt er die auch
verbindung zu einem Applicationsserver her an den er die vondem Gateway unter-
empfangenen Daten sendet und von dem auch Daten an die entgeräte, wie- ein-
der über das Gateway, gesendet werden. Diese Architektur wurde gewählt um ander
die laufzeit der End-Gerät, Anzahl der End-Geräte, Qualität des Signals und fer-
SIcherheit des Netzwerkes möglichst hoch zu halten. gnüpft

[Tec15](Architektur hat größen Einfluss auf Batterie, anz Teilnehmer, qua- sein
lität, sicherheit, kön-



en

2.1 Gateway

Das Teilnetz das aus dem Gateway und meheren LoRa-End-Geräten besteht ist Sternförmig aufbau. Jedes End-Gerät kommuniziert diret mit dem Gateway. Diese Atrt 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 Gatwy ist mit einem Netzwerkserver verbunden.

Ein Endgeräte kann gleichzeitig an mehren Gateways senden. Der Netzwerkserver ist zuständig die Pakete auf Dublikate zu überprüfen und nur solche nur einmalig an die Appliaktion 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 Sernförmige Architektur des Netzes und die fähigkeit von allen in der Reichweite befindlichen Endgeräte Daten zu empfnagen, muss ein Gatway mit vielen End-Gerätn kommuniziert. Da es nicht möglich ist mit jedem Gerät nacheinander zu kommuniziern, muss dies gelichzeitig 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 genannt Eigenschaften der Gateways wird auch eine gute Skallierbarkeit erziehl. Dadurch kann ein neues Gateway die anzahl der Knoten um das 6 bis 8-fach erhöhen.

[Tec15](Meistens wird ein Netzförmiges Netzt 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 chanel/multi modem transive) mehrere Nachrichten auch verschieden Chanels gleichzeitig empfangen

Wichtige Faktoren(anz. chanels, datenrate(time on air), paylod länge, Sendehäufigkeit)

Dabei sind die Endgeräte in Multicast Gruppen unterteilt.

realy?

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 "Herzstückëines jeden Lora-Netzwerkes. Im fallen viele AUfgaben zu. Er kann mit meheren Gatways und meheren Applicationsserver verbunden sein.

Die wichtigste Aufgabe ist das Steuern des Lora-Teils des Netzwerkes. Der Server verwalted jedes End-Gerät seperat indem es mit ihm den zu verwendendn Kanal aushanelt 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 nächt möglichem Zeitpunkten zu senden. Desweiteren muss er die empfnagenen Pakte "bestätegenünd leitet join requests an den joiserver weriter

Eine weitere sehr Wichtige Ausgabe ist es eine APi für den Applikationsserver bereitzustellen um eine einfache und shnelle kommunikation zu ermöglischen.

[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 gegebenenfals sebst 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 seinund jeder Netzwerkserver kann mehrer Join server haben. Wenn ein Endgerät dem Netzwerk beitreten möchte leited der Netzwerkserver die anfragen an den JoinServer weiter. Diser führt dann die nötige 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 NAchichten verwendet werdan aber aus sicherheitsgründen nie über das Netzt 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 korrektion funktion mehere wichtige Informationen Speichern.

ist das wichtig?

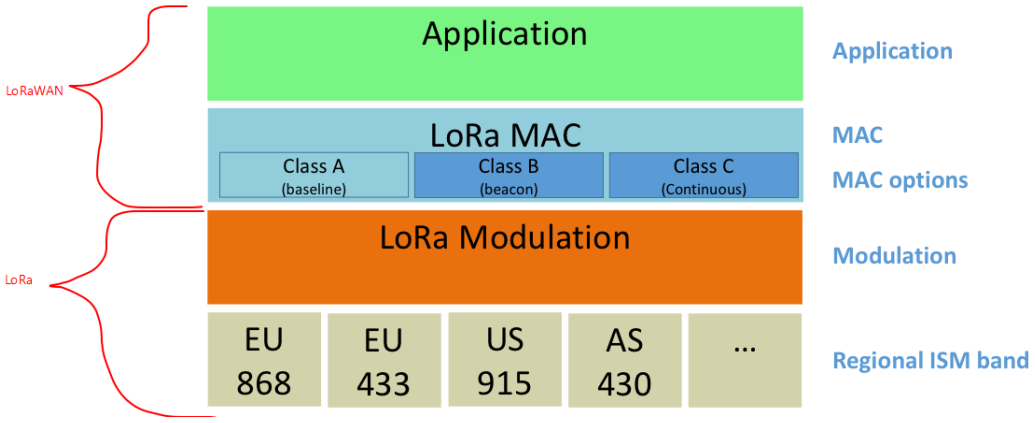
- DevEUI: Globale endgerätid die eindeutig für jedes endgerät definiert ist. (wie mac eines compueters)
- JoinEUI: Globale Adresse des JoinServers an den die anfrage gehen soll. wird nur für OTAA geräte benötigt.
- NwkKey und AppKey: Werden verwendet um spätere Schlüssel abzuleiten und die kommunikation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

3 LoraWan Funktionsweise

Im felgenen Kapittel wird näher auf die funktionsweise von LoRaWAN eingegangen. Spezell, liegt der fokus auf dem Netzwerkebitritt, das verwendete Protokoll und wie die Daten physikalisch Übertragen werden. [SOR17](Geschwindigkeit ist kompromiss zwischen abstand/geschw. die untersch freuen-

zen bze. geschwindigkeiten beinflussen sich nicht gegeseitig => keine inteferenz Die Datenrate ist einstellbar, jedoch wird die Reichweite bei höherer Datenrate gemindert. Ein Vorteil von Lora ist, das 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, Adaprive Data Rate))

3.1 Schichtenmodell



Das Schichtenmodell lässt sich in zwei Teile unterteilen. Der LoRa Teil ist der unterste und kümmert sich um die Physikalsche übertragung der Pakte und er LoRaWAN teil des Modells ist für die Stuerung des NEtzwerkes, implementierung der LoRaWAN-Klassen und das Überprüfen udn verschlüsseln der Daten zuständig.

Die Unterste Schicht des LoRa Teils moduliert die verwendeten Frequenzen. In Europa muss das ISM-Band 868 verwendet werden in den Verienigten Staaten wird das BAnd 915 verwendet.

Die darüberliegende Schicht heißt LoRa Modulation und kümmert sich darum das die Pakete so in die frequenz "moduliert"werden, dass der empfänger diese korrekt und effizent empfangen kann. Meher dazu im kapittel Übertragungsart

Über der LoRa Modulations schicht liegt die erste LoRaWan schicht, LoRa MAC. Diese sicht ist für die Implementierung der einenel Endgeräteklassen und für das Übertragen der Steuerkomanndos zuständig. Mehr zu den Klassen kann im kapittel Lora Geräte Klassen und im kapittel Protokoll gelesen werden.

Die oberste schiecht nennt sich Applikationsschicht und ist dafür zuständig die Nutzdaten einer NAchricht passend zu verpacken zu verschlüsseln und zu authentfizieren.

[Tec15](Application, Lora MAC, MacOptins(Classes), LoraModialtion(Regionales ISB))

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 der? wohin damit? umshreiben !!!!!

ABP steht für Äctivation by Personalizationünd bedeutet Wörtlich übersetzt Aktivierung durch Personalisierung.

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 folgene 4 Werte Vorgegeben werden. DevEUI, JionEUI , NwkKey, AppKey(Verschlüsselung des join requests).

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 replayattacs 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 speht. Falls von dem gelichen endgerät eine Join-Reguest mit einer zu kleinen DevNonce empfagen wir, wird die NAchricht ignoriert und es ist nocht möglich dem Netzwerk beizutreten.

Die Accept Nachricht besteht aus eier JoinNonce, einem NetzwerkID Net_ID,

einer Geräteadresse DevAddr, einer einstellungsfeld DLSettings , einer angabe wie lange auf eine antwort nach dem senden gerwarted werden muss RxDelay und eriner optionalen liste an Netzwerkparamerter CFList. Die JoinNonce wir außerdem benutz im schlüssel wie AppSKey, ... herzuleiten. 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 großer ist als die letzte empfangene.

welche noch, wo beschriebe ich wie? realy? überprüfe die komplette aussage

Der NWKSKEY ist für die verschlüsselung der Datenpakete bis zu Gateway zustendig . Auch dieser Key wird vom Netzwerkserver erzeugt und muss manuell in den code eingetragen werden.

Der letzt Wert heißt APPSKEY und sichert die kommunikation vom End-Gerät zu dem Applikationsserver ab. Der Schlüssel wird genau wie der NWKSKEY vom Netzwerkserver erzeugt und verwalted.

Mehr Infomationen zu den vonkioinsweise der Schlüssel finden Sie in dem Kapittel Sicherheit.

Wenn der Netzwerkserver den Beitritt des Endgerätes erlaubt sendet er eine Join-Accept nachricht zurück. Das Endgerät erwarted die nachrichten nach JOIN_ACCEPT_DELAY1 oder JOIN_ACCEPT_DELAY2 nach dem Senden des Request. Sollte die Join-Accept nachricht zu einem andern zeitpunkt gesendet werden, wird diese nicht empfnagen weil das Endgerät nict empfangsbereit ist. Die Nachricht enthält einstellungen für das Endgerät sowei die Id des Netzwerkes und die neue Adresse Für das Endgerät. Um replayatacken zu verhindern enthält die nachricht zusätzlich eine JoinNonce. Diese weitd für jedes endgerät seperat geführt und muss größer sein als die zuletzt gesendete.

3.2.2 ABP

Die einfachste Art des Beitritts heist ABP was für Äctivation by Personalizationßu deutsch Äktivierung durch Personalisierungßteht. Hierbei muss lediglich vor inbetribnhme des End-Gerätes 3 Konstanden definiert Werden. Manche Hersteller "brennen"diese drei Werte fest in den chip ein, sodas er nicht geändert werden kann. Flls es nicht möglich ist dem hersteller die gewünschten

werte zukommen zu lasse, sind solche End-Geräte nicht für den Beitritt mittels ABP geeignet.

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

Mit hilfer dieser 3 Werte kann die Join-Request - Join-Accept prozedur übersprungen werden. Daher kann das Gerät direkt einen Loranetz beitreten wenn es angeschalten 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 verwbindung muss das ResetInd Mac command im FOpt feld gesendet werden gesendet werden solange bis ein ResetConf erhalten wird. NUn ist das Gerät im netzwerk und kann unter der eingestellten Adresse und mit den eigestellten schlüssel arbeiten.

Sobal dem Netzwerk erfolreich beigetreten wurde werden ein die benötigten schlüssel aud dem vorher gesetzetn Werten abgeleited. genauers dazu in kapitel Sicherheit.

gehe ich zu weit?

hab noch nci

von mac ge- spro- chen

3.3 Protokoll

Das LoRaWAN Protokoll ist obtimiert für Batteriebetrieben Endgeräte die draahtlos kommunizieren möchten. Um energieeffizent zu sein setzt LoRa hauptsächlich auf zwei Punkte. Die Modulationstechnick und eine Adaptive Dtanenrate (ADR). Auch die Öne-Hopärchitektur trät zur energieeffizenz bei. Die Art wie LoRa siganle Moduliert wird in kapittel Übertragungsart besprochen. Um die gannannten Eigenschaften und das Lora Netzwes zu steuern werden sogenannte MAC commands verwendet. Diese werden von Dem Netzwerkserver oder von einem Endgerät gesendet. MAC steht hierbei für "Media Access Protokollünd bietet die möglichkeit die kommunikation mit den endgeräten, frequenzen, kanäle und vieles mehr zu stuern. Da die kommandos nur für den

doppeltgemoppelt

Netzwerkserver und die Endgeräte von bedeutung sind, werden diese nicht an den Applikationsserver gesendet sonder om Netzwerkserver herausgefiltert. Im folgenen wird näher auf die MAC komanndos und die Paketstruktur eingegangen.

Jedes Pakete besteht aus grundlegend aus 2 Felder (Preamble, PHYPalyload). Falls es ich um einen Uplinkpaket handelt wird noch ein CRC code hinzugefügt (Preamble, PHYPalyload, CRC). In diesem fall spricht man von einem implizit Paket oder von dem implezitem modus. Implizit modus bedeute das das es kein payload, codirungsrate und der CRC längenangebe gibt und diese somit eine feste zuvor definierte länge haben. Im expliziten modus werden noch 2 Felder hinzugefügt, PHDR und PHDR_CRC. SOmit sihet ein explizitest paket folgernermasen aus(Preamble,PHDR, PHDR_CRC, PHYPalyload). AUch hier gilt, im alle eines Uplinkpaketes wird am ende ein CRC felad angefügt => (Preamble,PHDR, PHDR_CRC, PHYPalyload, CRC).

erkläre up und downlink erkläre crc

Die Preamble ist dafür gedacht dem Empfänger mitzuteilen das gleich Datengesendet werden. Deswegen wird hier nur ein Signal gesendet das ohne Informationen ist, aber von dem Empfänder wargenommen wird.

Da Tiele des LoraWAn protokols geschützt sind, finden sich über die PHDR und PHDR_CRC felder kaum informationan . ALlerdings geht herfor das der PHDR die länge des PHYPayloads und die Zieladresse beinhalten sollte. Das PHDR_CRC Feld wird benutzt um sicherzustellen dass bie empfangenen Werte korekt sind mittels ddes CRC verfahrens .

hier das strikt einfügen

Wie schon merhfach erwähnt wird in Uplinknachrichten ein zustätzliches CRC feld verwendet. CRC steht für Cyclic Redundancy Check und wird verwendet um die korrektheit der NAchricht zu bestätigen. PHDR, PHDR_CRC und das CRC FLed werdenautomatisch vom dem Funktransceiver (modul asu empfänger und sender) hinzugefügt.

erkläre CRC

Die bis jetzt ebhandelten Felder des LoRa Paketes wurden alle von der LoRa Modulationsebene erstellt.

Die Darüberliegende Ebende "LoRa Mac"fügt nun das PHYPalyload Fled ein. PHYPalyload setht für Physikalische Payload. Es gibt 3 Mögliche PHY Payloads . Entweder wird ein MACPaylod eingefügt oder es werden join-rejon-

was heist PHYPalyoad?

request oder aber es wird die join accept nachricht darin transportiert. Um die Daten bzw die MAC kommandos richtig auswerten zu können und um die korrektheit überprüfen zu können werden einige Headders und zusätzliche felder benötigt. Deswegen lässt sich das Feld weiter unterteilen in (MHDR, MACPayload). Für den Fall das der MACPaylod keine join-rejoin oder MAcPayload nachricht ist, wir noch ein MIC feld hinzugefügt (MHDR, MACPayload, MIC). MIC steht für Message Integrity Code und wird verwendet um die korrektheit der Unterfelder MHDR | FHDR | FPort | FRMPayload festzustellen. DIese unbekannen felder werde im laufe des kapittels noch behandelt.

Das MHDR Feld beschribt wie die Daten im MACPayload Feld zu deuten sind. Wieder wird dieses Feld in Unterfelder Unterteilt. MTYpe, RFU und Major heisen die Unterfelder. Das MType feld beschreibt die Art der Nachricht. z.B: kann hier angegebn werden ob es sich um Datennachrichten, Join-Nachrichten, ... handelt. RFU steht für "Reserved for Future Usageßu Deutsch "für zukünftige verwendeung reserviert". Daher kann dieses Feld in der version 1.1 und niedriger ignoriert werden. Im Major Unterfeld wird ferwendet um das Format der Nachricht zu definieren. Momentan ist nur der wert 0 Definiert. 0 Steht für loRaWan R1. Die restlichen werde sind für zukünftige updates reserviert.

Mit der Unterteilung des MACPayload springen wir din dem LoRaStack noch eine ebene höher in die Applickationsschicht. Enthalten im MAcPayload feld sind der Frameheader (FHDR), der Frame Port (FPort) und der Frame payload (FRMPayload). Daten die gesendet werden sollen befinden sich in dem FRMPayload Feld. Wenn keine Datengesendet werden, kann das FRMPayload Feld auch MAC kommandos enthalten. IN dem Feld FPorts wird angegeben an welchen port und somit an welche teilapplikation die Daten geleidet werden. Es gib einige feste Ports. z.B. Port 0 Zeit an das das FRMPayload Feld MAC commands endthällt, 0x01 bis 0xDF sind Anwendungsspeziefische Ports und Port 244 ist für das LoRaWan Test LAyer protokoll reserviert. Falls ein andere Port als die geraden genannten angegeben wird, wird die nachricht verweorfen.Erneut kann der FHDR "Frame Headerïn einzelne Felder unterteilt werden (DevAddr, FCtrl, FCnt, Fopts).

was ist wie verschlüsselt? wirklich richtig?

hier tabelle

zahlenbasen anpassen

In dem feld DevAddr wird die Zieladresse der NAchricht vermerkt. Im feld FCnt (Frame counter) wird der jeweilige counterwert für die bisher gezählten Nachrichten übermittelt.Hamit schützt man sich vor replay Attacken. Im FOpt feld können bis zu 5 MAC kommandos parallel zu Dtaen übermittelt werden. DIe Anzahl kommt auf die mege der mitgelieferten variablen an . Das Letzte feld das in Unterfelder unterilt wird ist das FCTRL feld. Hier wird das verhalten des Gerätes gestuert sowie nachrichten acknoleged. Es gibt leichte unterschiede für ein Up-Link und für Down-link Nachrichten. Beide NAchrichtentüpen haben ein ADR, ein ACK und ein FOptsLen feld. Im ADR wird definiert ob der snedende bereit ist im Modus Ädaptive Data Rate"Daten zu senden, siehe Adaptive Data Rate. Mit dem Ack Feld können empfangene nachrichten makiert werden. Ob NAchrichte bestätigt werden müssen steht im MType feld. In dem FOptsLen feld wird die länge des FOpts feldes mitsamt des Headers eingetragen .

Ein Downlinkpaket hat zusätzlich ein RFU feld das nicht verwednet wird und eun FPending feld. In diesem fled kann das Gateway bzw der Netzwerkserver dem Endgerät mitteilen, dass noch mehr Dtanen zu senden sind und mehr empfangsfenster geöffnet werden müssen.

Dahingegen hat ein Uplinkpaket ein ClassB feld indem das endgerät dem Gateway mitteilt, dass es gerne auf Funktionsklasse B wechseln würde und ien ADRACKReq feld. Dieses feld wird verwendet um zu überprüfen ob das NEtzwerk noch antworted. .

[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 empfancher acknolaged werden. Reihenfolge ist zu be<chten. Alle nahrichten in einem farme müssen auch in einem frame ack werden. => Macbuffer ermöglicht dies. Wenn buffer überleuft werden die ältesten ack.

CRC usw wurden fon sender erstellt und eingefügt.)

[CB+17](Um energieeffizent zu sein setzt LoRa hauptsächlich auf zwei Punkte. Die Modulationstechnick und eine Adaptive Dtanenrate (ADR))

couter in gerät einführen und fileicht erklären wie das mit den counter geht ,länge reinschreiben? udn erklärn das mac varialen haben können da steht noch was von port und

3.4 Übertragungsart

Um die Enstandenen Pakete in Signale umzusezenun didese effizent und gleichzeitg übertragen zu können nutzt LoRa Chirp Spread Spectrum (CSS). Hierbei werden die Frequenz über eine gewisse Zeit hinweg veränder. Durch erkennen in welche richtig, ansetigen oder Abfalleb, die frequenz verändert wird, können 1 und 0 Codiert werden. Man spricht bei einem Bit von einem Chrip-Impuls. Durch aneinanderreihe der verschiedenen impulse ist es möglich mehere Bits nacheinander zu übertragen. Das entstandene Signal wird auch al Sub-Chrip bezeichnet. Durch verwenden von Unterschiedlichen anstiegs und abfalszeiten ist es möglich mehere Signale auf der Selben frequenz zu übertragen ohne das die Signale sich gegenseitig stören. DIes nennt man Spread Factor. Auserdem kann die Paralelität durch verschiedene Frequenzbereiche verbessert werden. CSS ist besonders für große reichweiten geegnet und somit auch bestens für Lora. Am besten ist das Signal wenn das endgerät nahe am Gateway ist. Je weiter es entfert desto schlechter wird das sgnal. Um die kommunikation trozdem zu ermöglichen wird der ßpredding Factorërhöht. Dies hat auch den Vorteil dass der Energieaufwand gering gehalten wird. Analog wie Menschen auf einer Party nicht immer versuchen lauter zu sprechen, sonder auch versuchen besonders langsam und deutlich zu scprecehn.

nachprüfen

Mann sichbrcht auch von Channels. CHannels können beliebeig benutzt werde. es gibt alerdings zwei regeln zu beachtn.

1. Channels werden per Pseudozufallszahl geändert
2. Sendezeit erfüllt die Regionalen Bestimmungen

Das Aloha Protokoll wird verwendet um festzustellen wann gesendet werden soll. Dabei wird einfach gesendet wenn Daten zum senden vorhanden sind. Wenn nun zwei Sender gleichzeitig auf der selbern Frequenz senden möchten kommt es zu einer kollision. Dadurch kann das Gateway die empfangenen Dtane nicht mehr auswerden. Deswegen warten beide Endgeräte eine zufällige, unterschiedliche Zeit abe bist sie erneut senden.

[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+17](Chrip Signal => Zeitliche Änderung in Trägerfrequenz(höhere Frequenz als Datenrate)(positiv chrip/negativ chrip)

Datensignal wird in Chrip Signal moduliert. Resultierende Signal ist breitbandiger als Datensignal. Maximale Datenrate auch mit Rauschen erreichbar.

Durch orthogonale SSpread Factor"mehrere Signale auf einem Chanel) [Tec15](normal FSK, schon sehr efficent. Lora "chirp spread spectrum odulation". Ist wie FSk aber größere Rechiweite, robuster. Stammt aus dem Militär/raumfahrt.Lora als erstes für kommerziellen billigen Einsatz.

Spread spectrum => signale sind Ortohonal für versch. spreizraten, fakto koreliert mit datenrate => verschiedene Datenraten auf einem Kanal

Nähere Geräte sind schneller => höhere Datenrate => kürzee übertrgungsdauer und lassen somit merh zeit für andere, => bessere Batterielaufzeit. Deswegen sidn symetrische up/downlinks nötig.) Frequenzhopping, spread spectrum, code-chanels

soll ich verhältniss zwischen datarat sf und energie reinmachen? warum?

3.4.1 Adaptive Data Rate

Adaprive Data Rate oder kurz ADR wird verwedent um immer die optimalste senderate und die optimale sendepower für das Endgerät zu finden und so schnellstmöglich die Daten zu senden. ADR kann nur verwendet werden wenn im FHDR feld des LoraPaketes das ADR Bit gesetzt ist, siehe Protokoll. Die Steuerung duch ADR findet durch den Netzwerkserver statt. Sobald der NEtzwerkserver bereit ist, stzt er das bit im downlink. IST das endgerät ebenfalls bereit setzt es ebenfalls das bit und ADR kann verwendet werden. Flass es nicht möglich sein sollte ADR zu verwenen sollte es durch das Applikaionslayer gesteuret werden.

Die Steuerung dfindet durch spezielle MAC kommandos statt. Standartgemäs wird die höchset übertragunsstäreke verwedent allerdings auch die gerings-

te Übertragunsrate. Flass diese gedrosselt werde soll wird vom Netzwerkserver das **LinkADRReq** MAC command benutzt. mIt diesem wird das Endgerät informiert, dass es die data rate, transmit power, repetition rate or channel ändern soll. Was auf welchen wert geändert werden soll wird in die Parameter codiert. Sobald die Werte geändert wurden, muss periodisch überprüft werden ob das Netzwerk die NAchrichten noch bekommt. Deswegen wird jedes mal wenn der uplinkframecounet erhöht wird, wird der ADR_ACK_CNT counter verwedent. Wenn dieser counter ein gewissen schwellenwert (ADR_ACK_Limit) überschreited, iwrd das ADRACKReq bit gesezt. DIeses signalisiert den NEtzwersverer das er mit einem Uplink ein Downlonk senden muss um die Verbindung zu bestätigen. Falls dieser Downlink nicht in ADR_ACK_Delay frames empfangen wird, wird zuerst die übertragusstärke auf max gesetzt. Flass möglich wird auserdem die Datenrate veringert um die Reichweite zu erhöhen. DIe Datenrate wird solange weiter jede ADR_ACK_Delay frames veringert bis diese minimal ist. Falls siese schon minimal ist müssen alle chanles wiederverswenet werden. DIes wird solange probiert biss eine verwbindung hergestellt werden kann.

hab ich das?

[AVTP+17](Datenrate und Funkfrequenz(RF) werde passend zum Abstand angepasst

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

=> immer möglichst schnelle senden => weniger Energie

) [CB+17](crip signal)

4 Lora Geräte Klassen

Um maximal energie zu sparen aber trozdem die möglichkeit dass die endgeräte agiel 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 A können werden als "high class

Joinen nur in A beschrieben?

End-Devices"genannt. wohin

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

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 nich flüchtig sein(Batteriewechseln kein reset) bei neuverbinden müssen alle counter auf uf 0 gesetzt werden. counter müssen auf beiden seiten glich gehalten werden(Synchron geführt) Wenn nachricht empfagen ist muss der darin enthaltenene counter größer sein als der eigene.

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

) [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 wird auch (All end-Devicec) gennnt undzeichnet sich durch sehr geringer Stromverbrauch aus. Die Kommunikation kann bidirektionalen Stadtfinden, allerdings muss die Kommunikation von dem Endgeräte gestartet werden. Das bieted die möglichkeit das das Endgerät, wenn keine Daten gesendet werden müssen, in einen sehr sparsamen Schlafmodus wechselt. Um das Endgeräte nicht zum äufwachenżwingen zu müssen, wurde auf einen Hardbeat oder ähnliches verzichtet. Dadurch kann das Endgerät so lange ßchlafen"wie es möchte.

Somit ist die Klasse A auch die potenziell Stromsparende Endgeräteklasse. Die Klasse A erlaubpt auserdem das das Endgerät andere Protokolle schickt solange es keine LoRa Daten sendet oder empfängt.

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). Die Downlinkfenster werden RX1 und RX2 genannt. Da die Kommunikation asynchron Stadtfinden, muss das endgerät wartet bis die uplinkphase abgeschlossen ist.

Die empfangsfenserr RX1 und RX2 mussen mindestens solange geöffnet bleiben das sie eine beginnende Übertrgung feststellen können. Flass keine übertragung epfangen wird, wird das fenseter weider geschlossen. Anderenfalls werden die Dtaen empfangen. Das Empfangsfenster RX1 wird nach RECIEV_DELAY1 zeiteiheiten +/- 20msec nach beendigung des Upliks geöffnet. Es wird die selbe freuqenz und Datenrate verwendet die auch be den uplik verwendet wurde. Wenn festgestellt in RX1 festgestellt wurde das keine Weiteren Daten mehr epfangen werden müssen kann auf das öffnen des RX2 fensters auch verzichted werden. RX2 wird wird nach RECIEV_DELAY2 zeiteiheiten +/- 20msec nach beendigung des Upliks geöffnet. Allerdings ist die Datenrate und freuenz fest. Nur Mittels spezieller MAC commands kann dies verändert werden.

Für alle join / rejoin aktivitäten wird immer die Klasse A verdendet . Schon [SOR17](radio packet explicit mode, vom Gateway(1) zum Knoten(1), erklärt ausgelöst vom Netzwerkserver, auch multikasts möglich, (Preamble, PHDR, oder PHDR_CRC, PHYPayload) Um Nachricht kurz zu halten kein CRC am ende, woannach Reciever_Delay1 / Reciever_Delay2 kann empfangen werden (rx1, rx2) ders

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 ncht gesendet oder gehört wird.<==) [SOR17](Frequenz abhänig von Uplinkfrequenz, Datenrate abhängig on Uplinkdatenrate, wird nach Reciever_Delay 1 +/- 20 msec erwarted, Datenrate auch abhänig von Regionalen regeln, Standart: Datenrate = Uplinkdatenrate) [SOR17](feste Fre-

quenz/Dtanetnrate, nach Delay2 +/- 20 msec, Frequenz/Datenrate mittels MAC änderbar) [SOR17](Öffnungslänge muss für Preamble ausreichen, nach RX1 + MIC und autentigitätscheck muss nicht zwingen RX2 geöffnet werden, Sender muss in einem der beiden Fenster stattfinden, Falls Downlink über beide Fenster => feames müsen gleich sein. Knoten dürfen nich während empfangen/ zwischen RX1 und RX2 senden, ender Protokolle dürfen gesprochen werden wenn gesendet werden darr)

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 Synchron ablaufen. Außerdem muss festgestellt werden, ob das Endgerät bzw das Gateway noch in Reichweite ist. Dies wird mittels einens periodischem "beacon"die zu festgelegten. DIeser BAcon wird regelmäßig vom GAteway gesendet und dint der syncronisation der Endgeräte. Zeitpunkten gesendet werde realisiert. Die Latenz ist einstellbar und kann bis zu 128 Sekunden. Die Endgeräte öffnen in regälmasigen ubständen ein empfangsfenster das pingslot genannt wird. Ein Downlink der in einem Pingslor gesendet wird wird ping genannt. Da dimmer Das gateway mit dem besten empfang die Daten an das GAteway sendet, muss das Endgerät selbständig feststellen wenn es einen Bacon mit einer unbekannten ID bekommt und durhch eien uplink dem server mitteilen das es in ierne neuen Umgebung ist. Dadurch lernt der seerver wo sich das Entgerät befindet und kann das Gatewa mit dem besten empfang wählen.

Obwohl das Endgerät durch die periodischen "beacons"nicht ßchalfen"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 sended Beacon für synchrinsation. Um daten empfangen zu werden werden empfangsslots => pingslots verwendet, werden periodisch geöffneto und mittels beacon synchronisiert. Normalerweise werde diese schnell

geschlossen außer es wird etwas empfagne. Gateway dessen beacon benutzt wird, wird nach empfangsqualität ausgewählt. Wenn neuer/unbekanter Beachon von einem anderen GAteway empfangen wird, wird der netzwerkserver benachrichted und dieser entscheidet welcher verwendet wird()passt rozte an).

Das Netzwerk muss die standart ping-slot periode Datenrate und kanal kennen.

Um ein gerät auf klasse B zu kommen muss erst von Klasse A gewächselt 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. ziwschen beacon und uplink wird random time verwendet um kolisionen zu verhindern . änderungen an pingslotperiode .. muss mitgeteilt werden. Hierzu ist klasse A nötig => wechel zu A, wechel zu B.

Nachschuen wie genau

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.)

das funktioniert

4.2.1 Klassenwechsel A nach B

Um einen Wechel überhaupt zu ermöglichen muss der Netzwerkserber die devault ping-slot periodem die pingslot datenrate und den Pingslot channel kennen.

Ale endgeräte treten in Klasse A dem Netzwerk bei. Das wecheln in die klasse B wird durch folgenden Prozess realisiet.

Als erstes muss das Programm des ENdgerätes beim LoRaWAN layer anfrogen ob es möglich ist in klasse B zu wecheln. Der LAyer sucht nun nach einem baecon. Wird ein backen entdeckt, wird die BEACON_LOCKED Servisprimitive zurückgeliefert. Wenn kein BAckoun empfangen wurde wir die BEACON_NOT_FOUND primitive zurückgegeben. Um diesen proess zu be-

erklären

schleinigen kann das DeviceTimeReq MAC kommando verwendet werden. Damit wird das GAteway aufgefordert eien bAcon zu senden. Nun kann das endgerät in den modus B wächseln.

Als Zeites setzt der MAC Layer des engerätes das Class B BIt im FCtrl feld Des Upliks auf 1. Dadurch ist er auch verandwortlich die Ping slots und für die Beacons zu öffen. Dabei muss mit der größt möglichen abweiching der Internen Uhr gerechnet werden und demensprechend die Epfangsfenster angepasst werden. DIese darf pro Beacon nicht mehr als +/- 1.3msec liegen. Der Inhalt der Empfangenenen Beacons wird mit der Signalsterke and das Programm des Endgerätes zur weiteren Verarbeitung gesendet. Dmait kann z.B. dem LoRaWan layer angewiesen werden die Uhr nachzustellen.

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

)

4.2.2 Betrieb

Damit der NEtzwerkserver dem Endgerät mittielen kann dass die pingslots frequen und/oder die Datnerate geändert werden soll gibt es den PingSlotChannelReq Mac kommando. DIe werden sind in den argumenten enthalten.

Das Endgerät kann die Periode der Pingslots zu einer beliebigen Ziet ändern. Ist dies der Fall, so muss das ENdgerät in Köasse A wechseln mit mittels dem MAc kommando PingSlotChannelReq die geämderte periode MItteilen . wird
Danach kann zuück in Kalsse B gewechselt werden. andere

Falls einige länger als 2 Stunden kein Beacon empfangen wird, kann die gespeisyncronistion mit de Netzwerk verloren gehen. Dadruch funktoiniert die Kom- cher
munikation in Klasse B noicht merh und es wird in Klasse A gewechselt. Da 1/s
sich nun die Kommunikationsstrategie verändet muss mit einem Uplink in dem => hz
das CLassB Fled 0 ist, der Netzwerkserver informiert werden. Nun kann versucht werden eine verbindung mit der Klasse A aufzubauen. Das Programm

des Endgeätes kann versuchen wieder in Klasse B zu wecheln. DIeser prozess kann sich immer weider wiederholen.

Um auch innerhalb der maimal 2 Stnden in den kein Beacon empfangen wurde einen kommunikatio zu ermöglichen wird jedes mal wen ein Beacon verloren geht in den beacon-less modus gewechselt. Dieser Modus orierntiert sich ausschlieslich an der internetn Uhr. Um den Drift auszugleichen werden die EMpfangsfenter immer früher begonnen und immer später beendet. Das bedeutet einen höheren Energieverbracuh aber auch eine höhere Warschelinlichkeit noich Daten zu empfangen obwohl die Uhren des GAtways und des ENdgerätes auseinanderlaufen. drift?

4.2.3 Singel / Multicast

Die Downlink der Klasse B unterschidene sich nicht von denen der Klasse B. allerding kann sich derFreqenzplan untersdchedien.

In Klasse B können die NAchrichten als Singelcast oder als Multicast nachrichten verwendet werden. Eine Singelcast nachricht wird an des geröt das im DevAffr fled der NAhcricht codiert ist gesendet. Im Multicastmodus wird das paket an alle ENdgeräte gesendet. Damit die möglich ist müssen sich die geräte die selbe multicas Adresse und die dazugehörigen schlüssel teilen. Durch verschiedene Multicstadressen ist es möglich soganannte multicas gruppen zu erzeugen die nciht alle sonder nur ein Teil aller entgeräte beinhalten. LoRaWan git allerding keine Methode vor wie die adressen und Schlüssel verteilt werden. Diese Aufgabe muss laso in der Applikationsebene sprich im Programm der ENtgeräte oder Direkt bei der Personlaisierung (Programerung) erledigt werden.

In Mlticastadressen sind keine MAc kommandows erlaubt. Nur Daten dürfen als Multicastbnachricht übertragen weden. DIes wurde eingeführt da Multicastnachrichten nicht die selbe robutheit wie SIngelcastnachrichten haben. Die NAchrichten dürfen nicht acknloged werden . Das Fpending zeigt an das mehr unconfirmed Multicasnachrichten zu senden sind. [SOR17](sepearate Adresse für Multicast / con-Festgelegt durch layer oder manuell für gruppenmulticast Nicht führ MAC firmed

geeignet,)

4.2.4 Beacon

Wie schon erwähnt wird der Beackon verwendet um das ENdgerät mit dem Netzwerek zu synchronsisiern. Deswegen wird dieser Periodisch gesendet. Die Zeit zwischen zwei Beackons wir BEACKON_Period genannt. Die Endgeräte öffnen Enmpfangsfenster um diese Beacons zu empfangen. Ein BAcok zu übertragen dauert BEACON_RESERVED lange. Das beaon wird Beakon_GUARD früher geöfnnet um sicher zu stellen das BEac auch wirklich zu empfangen. Während versucht wird ein Beacon zu empfangen kann kein pingslot geöffnet werden. Auserdem wird die Beakon_GUARD benutzt um sicherzustellen das kein Ping slott mehr geöffnet ist. Deswegen muss diese Beakon_GUARD mindestens so lang sein wie ein maximaler pingslot. Ein weiterer vorteil ist, dass nicht daraf geachth werden muss wann ein pingslot geöffnet wird, da er soweiso im zweifelsfall fertig ist befor ein beakon empfangen wird. vorlesungsbezug?

Um snychronsisierungen druch die beacons zu vermeiden, wie alle entgeräde wollen sofort nach den beakon senden wollen, wird mittels zufälliger warte, pingslot zeiten und zufälliger pingslotanzahlen verhindert.

Beacons haben ihr eigenes Paketformat. DIese PAkete sind immer gleich lang. Dadurch kann auf header verzichted werden was auch der Geschiwndigkeit der verarbetug zu gute kommt. Wie auch ein Normales LoRaPaket, so besteht auch das erste Feld des Beakonpaketes aus der Preable nur das die des Beakonpaketes länger dauert was ein bemerken der übertragung warscheinlicher macht. Danach folgt nur noch der BCNPayload. Der BCNPayload lässt sich untertielen in RFU, Time, CRC, GWSpecific, RFU, CRC. DIe zwei CRC Felder weisen schon auf die logische unterteilung in zwei hälten hin. Der erste Teil enthält beacon speziische informationen (time und CRC). In dem Timefeld ist die zeit seit 00:00:00, Sunday 6th of January 1980 (start of the GPS epoch) modulo 2$\hat{3}$2 enthalten. das CRC feld wird verwendet um die korrektheut des Zeit und des RFU Fledes zu versichern. DIe andere hälfte ist GAtewayspezifisch. Sie enthält das GwSpecific fled und ein RFU fled das auch dirch 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 GPS coordinate of the gateway first antenna 1 GPS coordinate of the gateway second antenna 2 GPS coordinate of the gateway third antenna 3:127 RFU 128:255 Reserved for custom network specific broadcasts. Sonlage sich im infofled coordinaten enthalten kann dieses unterteilt werden in Längen unt breitengrad.

Auch Klasse A kann den beacon somit nutzen um herauszufinden von welchem gateway es gerde Datenempfängt und um somit eventuelle standortwechel festzustellen.

In Europa werden die Beacons auf einer festen frewuen übetragen die sich nicht endert auser über das MAC kommando PingSlotChannelReq. Auf anderen Kontinenten kann es sein das frequenzyhopping angewendet wird.

regionale parameter erwähnt?

4.3 Klasse C

C steht für CONTINUOUSLY Listening. Wie der Name schon sagt wird hier unaufhörlich ein empfängssender geöffnet. Dadur wird es ermöglist fast Latzenfrei zu übertragen. 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.

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 den gleichen Funktione wie in Klasse A. Der große unterscheid besteht allerdings darin das RX2 immer dan geöffnet ist wenn nicht gerade daten an das Gatway gesendet werden oder RX1 geöggnet ist. Also auch Während . Auserdem stehen die gleichan MAC kommandus und zwei zusätzzliche zu verfügubng .

suche normal net?

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

[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.)

4.3.1 Wechsel von A nach C

Da es kein ClassC Fled in einem LoRapaket gibt, wurde für das umschalten in ClassC mode MAc kommandos eingeführt. Das endgerät sendet das DeviceModeInd commando. ALs parameter kann es 0 für Klasse A und 2 Für klasse C angeben. Der Netzerkserver kann mit DeviceModeConf welches den wert der klasse enthät indas gewächselt wurde.

5 Sicherheit

SIcherheit in netzwerkfägigen Systemen ist ein sher wichtiges und heiß dikutiertes thema. Da LoRa daten Üver die Lpft überträgt, ist es extrem wichtig sich und die Dtaen zu schützen. Da Luft als Medium benutzt wird könnten alle in der Nähe befindlichen geräte die gesendeten Daten mithören. Aber genauso kann ein Endgerät sich als ein andres ausgeben und in seinem Namen Daten an ein Fremden Server send. Um zu verhindern das Gesnedene Daten mitgelsen werden müssen diese verschlüsselt werde. Um zu verhindern das jemand anderst so tut als wäre er das engerät mussen die Dtane Autentifiziert werden. Slest jetz könnten z.B. Join-request mitgeschnitten werden und von dem (bößen) endgerät wiederholt werden um das (gut) endgerät daran zu hindern aktiv dem Netzwerk beizutreten. Deswegen wurden zähler eingebaut. Im folgenden wird sich nächer damit beschäftigt welche mechanismen es gibt die gennten probleme zu umgehen.

Oberflächlich gesehen bietet Lora eine end-to-end Sicherheit an, indem es die Signale zweimal verschlüsselt. Die erste Verschlüsselung dient dazu die gesendeten Daten vor eventuellen Mithörern zu verschlüsseln, also pm Endgerät bis zu Gateway zu verschlüsslen. 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.

Nächer betrachtd benutzt Lore eine ganze Reihe an Schlüssel und Zähler

verwendet um die Kommunikation abzusichern. Da die verwendeten Schlüssel bei OTAA-Aktivation variieren wird hier eine viel höhere Sicherit geboten als bei ABP-Activation wo alle Schlüssel von anfangan vorgegeben werden. Infolgedessen wird im folgenden Text auf die SIcherheit unter verwendung von OTAA bezogen.

Jesed enggerät hat seine eigenen NwkKey (Netzwerkschlüssel) und App-Key (applikation schlüssel). Sobald einem Netzwerk begetreten wurde wird aus dem NwkKeay der FNwkSIntKey , SNwkSIntKey und NwkSEncKey abgeleited. AUs dem AppKey iwrd zusätzlich der AppSKey abgeleited. Die schlüssel müssen so gespeichert werden, dass es nicht mölgich ist diese auf irgendeiener weise aus dem Speicher zu holen außer für das endgerät selber. Zusätzlich werden Join-Keys abgeleited. JSInitKEy und JSEncKey.

Der FNwkSIntKey ist einzigartig für ein Endgerät und heist Forwarding Network session integrity key. Der Schlüssel wird verwendet um ganze oder Teile der MIC felder in den LoRapaketen zu berechen . mic

Serving Network session integrity key heißt abgekützt SNwkSIntKey. Dieser Schlüssel wird verwedent um die Integrität des MIC codes zu überprüfen. Zusätzlich wird er auch verwendet um Teile des MIC codes zu berechen. Dieser Schlüssel ist spezifisch für ein entgerät.

NwkSEncKey oder lang Network session encryption key, ist für jede Netzwerksitzung einzigartig und wurd verwendet um empfnagen order gesendete Mac kommandos zu ent- oder verschlüsseln.

Der AppSKey wird auch Application session key und wird einem Endgerät zugeordent. Er wird vom Gateway und vom Endgerät verwendet um Daten die zum Applikationsserver geschickt werden sollen zu verschlüsseln.

pad fügt do viele 0en das die länge an vielfaches von 16 ist AppSKey = aes128_encrypt(NwkKey, 0x02 | JoinNonce | NetID | DevNonce | pad16) FNwkSIntKey = aes128_encrypt(NwkKey, 0x01 | JoinNonce | NetID | DevNonce | pad16) SNwkSIntKey = NwkSEncKey = FNwkSIntKey.

Jedes Gerät hat 3 verscheidene Frame counter um die Anzahl der gesendeten und empfangenen Frams mitzuzählen der FCntUP counter zählt die

uplikframes, der NFCNTDown zählt die MAC-downlinkframes und der AFCntDown welcher alle downlinkframes zählt die Nutzdaen enthalten.

Wenn ein gerät dem Netzwerk beitritt, werden zuerst die Counter auf 0 gesetzt. Beide seiten einer Kommunikation halten die zähler gleich. Beim senden wird der Aktulle counterwert in das FCnt feld eingetragen. Werden übertragungen wiederholt so wird der counter nicht erhöht weiderholung

Durch das verwerfen von NAchrichten mit zu kleinem Counterwert, wird schon verhindert das Pakete von einem Angreifer aufgenommen und zu einem späteren Zeitpunkt wiederabgespielt werden. drin?

Jauch bei den Join oder Accept NAchrichten besteht die gefahr eine Replayattac. Da hier dem Netzwerk noch nicht begetreten wurde, können die zähler niht verwendet werden. Hier wird eine Nonce in die Join-Pakete coderit . DIese Nonce zählt auf die gleiche weise hoch wie die counter. Die gegnerische Seiter der Kommunkikation muss die Nonce tracken und darf nur pakete mint einer Nonce akzeptieren die höher ist als die letzt Nonce. wie sieht paket aus.

[GAS17](Netzwerkserver hat AppKey daraus werden AppSKeay und NwkSkey erzeugt) [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.) frequncyhopping

6 Live-Beispiel

wenn vorhanden.

7 Ausblick

Literatur

[AVTP+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+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.

[SOR17] 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.