LoRaWAN Security

VOOR IOT SECURITY

Beveiliging in het LoRaWAN protocol.

V1.0, Mei 2022

Bavo Debraekeleer & Birk Tamm

ARTESIS PLANTIJN
HOGESCHOOL ANTWERPEN

Inhoud

1. Introductie

Internet of Things (IoT) toepassingen zijn volop in de opmars en kent een snelle groei die in de toekomst enkel zal toenemen. Het is het onderdeel van informatie technologie dat het geheel is van toestellen, of dingen (things), die met elkaar verbonden zijn. Vaak enkel tussen apparaten zonder de tussenkomst van personen, of Machine-to-Machine (M2M) communicatie. Het is een wereld van sensors, actuatoren en ingebedde informatieverwerking. Sommige IoT toestellen zijn rechtstreeks verbonden met het internet. Andere gebruiken draadloze communicatie. Toepassingen die slechts over korte afstand moeten kunnen communiceren of waar real time data vereist is gaan eerder GHz-gebaseerde protocollen gebruiken zoals WiFi, Bluetooth of Zigbee. Als het gaat over lange afstanden of toepassingen waar de focus ligt op laag energie verbruik, bijvoorbeeld een sensor op batterij, en waar real time data niet vereist is, zal er eerder gegaan worden voor MHz-gebaseerde protocollen. De zogenaamde Low-Power Wide-Area Network (LPWAN) netwerken zijn hiervoor uiterst geschikt. Dit zijn bijvoorbeeld SigFox, Narrow Band-Internet of Things (NB-IoT) of Long Range (LoRa en LoRaWAN) om een aantal te noemen.

IoT toestellen duiken overal op. Bij consumenten thuis, in industrie, kantoorgebouwen, en in Smart City toepassingen zoals parkeerplaats monitoring, slimme verlichting, park onderhoud, vuilnisophalen. Deze snelle groei van nieuwe toestellen en protocollen als ook de soorten toepassingen brengen echter gevaarlijke veiligheidsrisico's met zich mee. Het gaat hier over vrij nieuwe protocollen die nog volop in ontwikkeling zijn en waar regelmatig nieuwe zwakheden in gevonden worden. Al deze technologieën gebruiken daarboven ook radio golven. Deze kunnen door iedereen, met de juiste ontvanger, opgevangen worden. Hierdoor is het mogelijk dat de data gelezen kan worden door derden, maar de data kan ook aangepast en heruitgezonden worden. Een transmissie kan ook opgenomen worden en heruitgezonden worden op een ander moment (replay attack). Of een transmissie kan opzettelijk verstoord worden (jamming attack). En dan gaat het nog maar enkel over het draadloze aspect van de communicatie. Er is ook nog de verbinding met internetdie de toestellen blootstelt aan nog andere aanvallen.

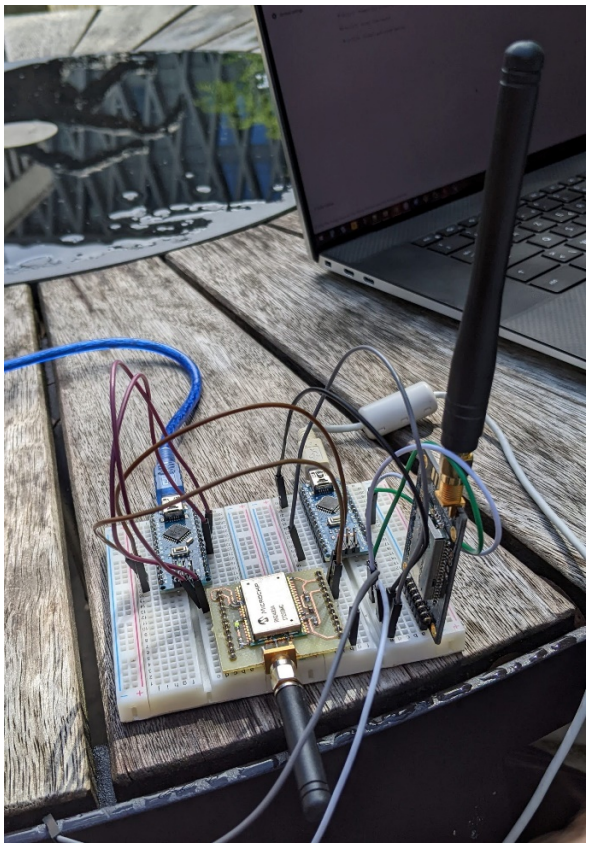
Het onderdeel waar bij IoT specifiek ook extra aandacht aan gegeven moet worden is het hardware aspect. Toestellen in industriële en Smart City toepassingen kunnen overal geplaatst worden en zijn dus potentieel toegankelijk voor derden. Door de radio golven is lokalisatie ook heel eenvoudig dus ze zijn ook niet moeilijk vindbaar. Eens een aanvaller een toestel in handen heeft is het belangrijk dat deze bescherming tegen het uitlezen van data heeft (side-channel attack), als ook tegen herprogrammering of aanpassen van de firmware. Een correcte implementatie met focus op beveiliging is hier uiterst belangrijk.

Veroudering is ook een belangrijk veiligheidsrisico. Toestellen worden vaak geproduceerd en geplaatst om jaren mee te gaan. Zwakheden die gevonden worden en waar eventuele oplossingen voor kunnen komen in de specificaties van het protocol kunnen mogelijk opgelost worden door firmware updates, maar kunnen ook hardware aanpassingen vereisen. Firmware updates moeten ook eerst nog door de producent gemaakt worden, wat niet altijd mogelijk is. En dan moeten deze ook nog op een veilige manier tot bij de te updaten toestellen geraken.

Er moet bij een veiligheidsanalyse ook steeds gekeken worden naar het gehele netwerk. Niet enkel de IoT toestellen zelf.

In deze analyse wordt er gekeken naar hoe LoRa werkt en hoe LoRaWAN omgaan met beveiliging. Hoe deze gespecifieerd zijn, de zwakheden en mogelijke aanvallen. Er zijn ook enkele praktische tests uitgevoerd om een replay en jamming attack in de praktijk te testen met actuele hardware die iedereen vrij kan kopen. Twee LoRa radio modules in combinatie met een

Arduino Nano als end device, en een Raspberry Pi met LoRa concentrator HAT als gateway. Als Server backend maken we gebruik van The Things Network's The Things Stack.



Figuur 1 Arduino Nano's met LoRa modules

Figuur 2 Raspberry Pi als LoRaWAN TTN gateway

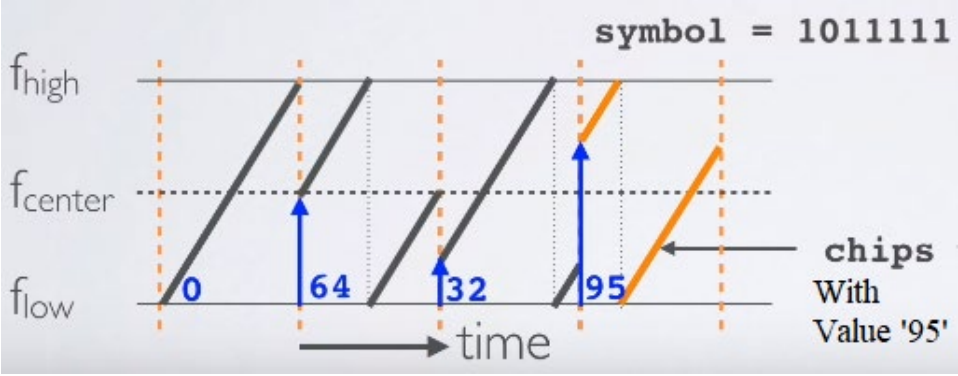
2. LoRa Communicatie

LoRa staat voor Long Range en is een fysische radio modulatie techniek. Samen met het LoRaWAN protocol, beschreven in het volgende hoofdstuk, vormen ze een Low-Power Wide-Area Network (LPWAN) waarbij de focus ligt op een zo groot mogelijk bereik samen met een zo laag mogelijk energieverbruik. Het is geschikt voor toepassingen waarbij data verzonden kan worden in kleine stukken en met lage bit rates.

LoRa, ook wel LoRa PHY genaamd, is enkel voor de fysische (physical) en data link laag in het OSI model. Het bevat geen beveiliging, maar het is voor veiligheidsmaatregelen rond het draadloos verzenden van informatie wel belangrijk om te begrijpen hoe het werkt.

2.1 LoRa Modulatie

LoRa modulatie is afgeleid van Chirp Spread Spectrum (CSS) technologie. De te verzenden informatie wordt gemoduleerd aan de hand van chirps. Deze chirps, ook wel symbols genoemd, zijn de dragers van de data. Het zijn lineaire frequentie verhogingen of verlagingen ten opzichte van de tijd tussen bepaalde frequenties in. Het kan gevisualiseerd worden in schuine strepen. De periode waarin er van de laagste tot de hoogste frequentie kan gegaan worden is de chirp (de oranje stippellijnen in onderstaande figuur). Elk afzonderlijk streepje is een chip. Deze techniek zorgt voor de goede bestendigheid tegen storingen van het LoRa netwerk.



Figuur 3. LoRa modulatie. (n.d.). [Graph]. RF Wireless World. https://www.rfwireless-world.com/Terminology/What-is-difference-between-Chip-and-Chirp-in-LoRaWAN.html

Naar beveiliging toe maakt dit de transmissies echter gevoelig voor patroon herkenning. Een LoRa pakket is bijvoorbeeld voorzien van een preamble om het begin van het pakket aan te geven. Dit is dan steeds hetzelfde en dus herkenbaar door aanvallers. Meer hierover onder Spreading Factor.

2.2 Carrier Frequency (CF)

LoRa transmissie kan technisch gebruik maken de license free sub-gigahertz banden met frequenties van 137 MHz tot 1020 MHz, maar ook 2.4 GHz is mogelijk. Deze laatste laat toehogere data rates te bekomen ten kosten van bereik (range). Er moet echter ook rekening gehouden worden met de lokale wetgevingen. De license free sub-gigahertz radio frequentie band is EU868 (863–870/873 MHz) in Europe; AU915/AS923-1 (915–928 MHz) in Zuid-Amerika; US915 (902–928 MHz) in Noord-Amerika; IN865 (865–867 MHz) in India; en AS923 (915–928

MHz) in Azië. De 2.4 GHz frequentie valt in ISM banden en wordt internationaal gereserveerd voor industriële, medische en wetenschappelijke toepassingen.

Aanvallers weten dus ook perfect op welke frequenties ze waar in de wereld moeten luisteren.

2.3 Coding Rate (CR)

Een LoRa modem gebruikt de Coding Rate voor bescherming tegen interferentie pieken. Dit is gedefinieerd door de Forward Error Correction Rate dat volgende CR waarden accepteert: 4/5, 4/6, 4/7 of 4/8. Hoe hoger de CR waarde hoe langer de transmissie lengte (packet time-on-air), maar hoe sterker de interferentie bescherming. De CR beïnvloed met andere woorden de lengte van een uplink pakket.

Uplink betekend dat het pakket van end device, de zender, naar een gateway verzonden wordt, de ontvanger. Het omgekeerde noemt downlink waarbij de gateway de verzender is en het end device de ontvanger.

2.4 Spreading Factor (SF)

De Spreading Factor geeft de chirp rate aan en bepaald dus de snelheid van de data transmissie. Hogere SF betekend snellere chirps en een snellere data transmissie. Elke verhoging in SF halveert de chirp sweet rate en ook de data transmissie rate. Lagere SF verkleint dan weer het bereik van de LoRa transmissie.

De SF wordt ook gebruikt om congestie van het netwerk tegen te gaan. Signalen gemoduleerd met verschillende SF op hetzelfde frequentie kanaal (channel) en uitgezonden op hetzelfde moment interfereren niet met elkaar.

Een lagere SF heeft de hoogste bit rate en de hoogste SF heeft de beste range en minste kans op fouten in het pakket. Hoe hoger de SF echter ook hoe langer de radio actief moet zijn en dus een groter energieverbruik.

Voor een aanvaller die een jamming attack wilt uitvoeren is het hier dus belangrijk dezelfde Spreading Factor te gebruiken. Dit gebeurd namelijk door gelijktijdig met de te jammen transmissie ook een transmissie uit te zenden met een grotere signaal sterkte, maar dus ook dezelfde SF. Zo zal er een botsing plaatsvinden. Om de juiste SF te vinden helpt de wetgeving hier weer. Afhankelijk van de regio zijn er bepaalde SF beschikbaar voor gebruik. In EU868 gaat dit van SF7 tot SF12 en een bandbreedte van 125 kHz. Aan de hand van het Channel Activity Detection (CAD) mechanisme kan geluisterd worden op een bepaald kanaal en SF naar de preamble van een LoRa pakket om zo te detecteren wanneer er een trannsmissie begint en op welke channel en met welke SF.

2.5 Bandbreedte (Bandwidth, BW)

De bandbreedte is de frequentie breedte van een LoRa transmissie frequentie band. Doordat dit te tijd beïnvloed betekend een hogere bandbreedte ook een hogere chip rate en dus data rate. De BW kan binnen LoRa gaan van 7.8 kHz tot 500 kHz. In het LoRaWAN protocol wordt echter enkel gebruik gemaakt van 125, 250 en 500 kHz.

In de praktijk zijn de standaardwaarden van LoRa modules meestal 125 kHz en SF12. Deze kunnen aangepast worden, maar dit is dus afhankelijk van implementatie. Voor aanvallers is dit dan ook vaak het startpunt.

2.6 Duty Cycle

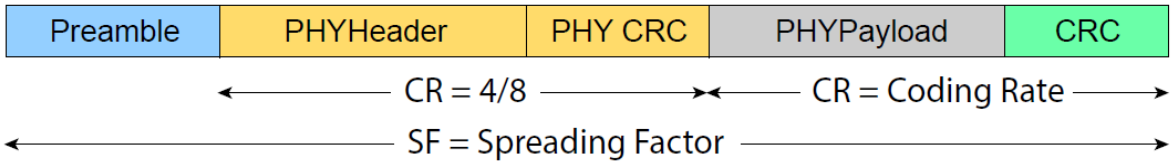
De duty cycle is een percentage dat aangeeft hoelang een toestel een specifiek kanaal mag gebruiken binnen een bepaalde tijd. Ook dit is afhankelijk van lokale wetgevingen. Meestal is dit 1%. Door gebruik van een duty cycle wordt de kans op collisions sterk verminderd.

2.7 Frame Formats

Frame formats bepalen wat de onderdelen zijn van een transmissie. Er zijn twee frame formats die door LoRa worden ondersteund.

De impliciete frame format bevat enkel de preamble en de payload. Deze preamble dient voor de synchronisatie met de ontvanger. Het kan een lengte hebben van 6 tot 65535 chirps of symbols die door de LoRa modem gecombineerd worden een extra 4.25 symbols om tot een synchronisatie word te komen. De payload is de informatie die verzonden wordt.

Het expliciete frame format bevat naast de preamble en de payload ook een header en optionele Cyclic Redundancy Check (CRC). Deze header bevat informatie over de lengte van de payload, de gebruikte CR en of er een CRC gebruikt wordt of niet.



Figuur 4 LoRa uplink pakket structuur [Graph] Perković, T., Rudeš, H., Damjanović, S., & Nakić, A. (2021). Low-Cost Implementation of Reactive Jammer on LoRaWAN Network. Electronics, 10(7), 864. https://doi.org/10.3390/electronics10070864

In LoRaWAN is de preamble steeds zes symbols. Gevolgd door de header met een CR van 4/8, en vervolgens de payload die in grote kan variëren van 1 tot 255 bytes.

Zoals reeds verteld is het voor aanvallers mogelijk om deze preamble te herkennen en hier gebruik van de te maken voor aanvallen.

3. Het LoRaWAN Protocol

LoRaWAN is een Media Access Control (MAC) laag protocol bovenop LoRa modulatie. Het is een software laag die specifieert hoe toestellen de LoRa hardware moeten gebruiken.

Het protocol wordt ontwikkeld en onderhouden door de LoRa Alliance die de eerste specificatie uitbracht in januari 2015. Sinds dien is het protocol verder ontwikkelt (zie onderstaande tijdlijn) met voornamelijk aandacht voor beveiliging en schaalbaarheid.

Figuur 5 The Things Network Global Team. (2021, June 7). An overview of LoRaWAN specifications [Timeline]. The Things Network. https://www.thethingsnetwork.org/article/whats-new-in-LoRaWAN-104-1#:~:text=designated%20%E2%80%9CLoRaWAN%20Certified%E2%80%9D-,The%20L

In 2017 kwam een belangrijke stap voor betere beveiliging met versie 1.1 van het protocol. De industrie volgde echter niet en bleef verder toestellen produceren volgens versie reeks 1.0.x. aangezien deze al in ontwikkeling waren en v1.1 niet backwards compatible is en andere hardware vereisten heeft. De LoRa Alliance is daardoor de 1.0.x reeks verder gaan ontwikkelen om deze ook te blijven verbeter, tot versie 1.0.4 in 2020. Nu hun marktaandeel groot genoeg is geworden is de focus terug naar versie 1.1 zodat deze verder verbeterd kan worden.

De voornaamste verandering voor beveiliging zijn:

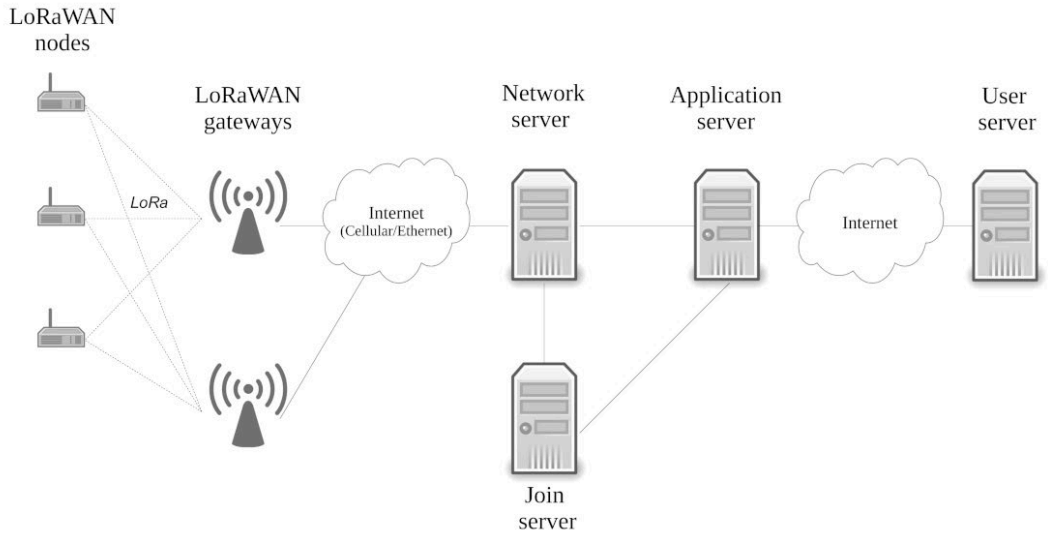
- Versie 1.0.2
  - FCntUp geëncrypteerd en bijgevoegd in de ACK downlink als beveiliging tegen Replay Attacks.
- Versie 1.1
  - Laat netwerk en server decompositie toe. De belangrijkste is hier dat de Join Server door een derde partij kan gehost worden of door applicatie beheerder zelf, afzonderlijk van de Netwerk en Applicatie servers.
  - MAC commando's zijn altijd geëncrytpeerd.
  - Sessie beveiliging opgesplitst tussen Netwerk Server en Application Server.
  - Frame counters kunnen niet worden gereset.
  - DevNonce is nu incrementeel in plaats van random als beveiliging tegen forced keystream reuse attacks.
  - Rejoin requests mogelijkheid om sessie context te verversen waardoor ook de frame counters ververst worden om uitputting hiervan tegen te gaan. Het kan ook gebruikt worden om communicatie door te geven aan een ander netwerk voor roaming.

    - Verbeterde Availability:
        - Betere bescherming tegen active denial of service attacks.
        - End device herconfigureerbaar tijdens roaming (handover roaming).
        - Geen time drifts meer voor klasse B end devices.
    - Verbeterde Confidentiality door het vermijden van keystream reuse.
    - Verbeterde Authentication en Confidentiality door de mogelijkheid om de Join Server bij een derde partij te hosten of het zelf te hosten.
- Versie 1.0.3
    - Unicast en Multicast ondersteuning voor klasse B end devices.
    - Tijd synchronisatie voor klasse B end devices.
- Versie 1.0.4
    - 32-bit en persistente FCnt
    - Monotonische incrementatie van de DevNonce tegen replay attacks

Verder voorziet de LoRa Alliance ook end device certificering om betrouwbaarheid te verhogen door na te gaan of deze toestellen voldoen aan de specificaties.

3.1 Netwerk Topologie

LoRaWAN netwerken hebben een star-of-stars topologie. End devices, ook wel nodes genoemd, zijn via meerdere gateways verbonden met een centrale Network Server (NS) waarmee ook een Application Server (AS) en Join Server (JS) verbonden zijn. Deze Join Server is pas gespecifieerd in LoRaWAN 1.1. In 1.0.x is dit niet deel van het protocol, maar kan wel gedaan worden.



Figuur 6 Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). Overview of the LoRaWAN network architecture [Illustration] LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. Sensors, 22(9), 3127. https://doi.org/10.3390/s22093127

In de LoRaWAN specificatie v1.1, LoRaWAN Backend Interfaces v1.0, wordt de Netwerk Server verder opgedeeld in Home, Serving en Forwarding om Roaming met Handover Roaming uit te breiden. Deze onderdelen kunnen op éénzelfde NS staan, maar ook elk op afzonderlijke servers.

3.2 Medium Access Control (MAC) Klassen

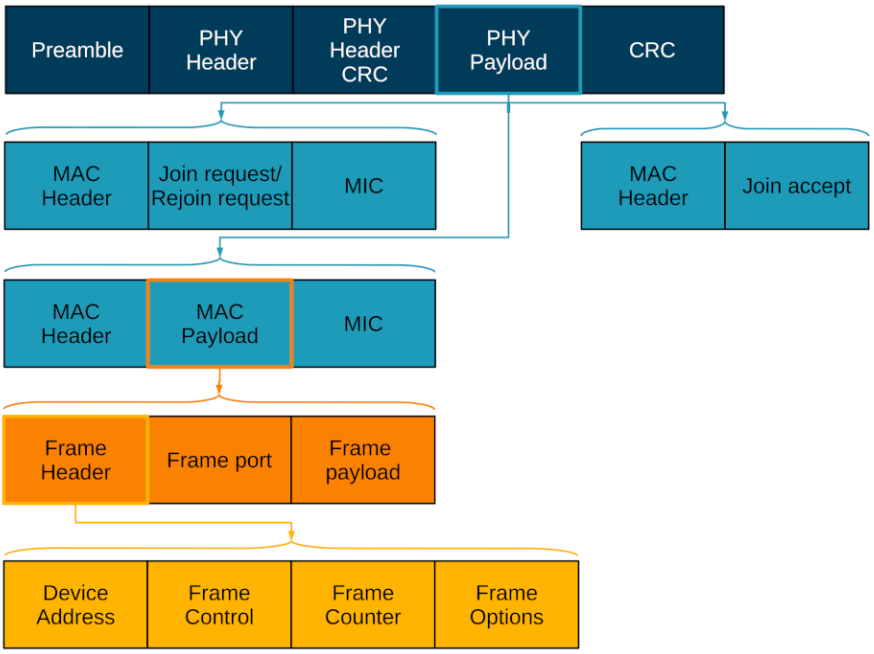
LoRaWAN specifieert drie klassen in MAC laag operaties.

- Klasse A: voor low power. Deze zenden uplink data volgens hoe ze gepropgrammeerd zijn. Er wordt naar een gateway gestuurd zonder eerst na te gaan of het kannaal vrij is. Vervolgens wordt gewacht op een bevestiging (ACK) van de gateway, en eventuele MAC commands, in twee geplande momenten 1 en 2 seconden na het verzenden, genaamd RX1 en RX2. In de tussentijd kunnen de microcontroller en LoRa module in slaap modus om energie te besparen.
- Klasse B: voor verminderde latency. Deze voorziet een vast gepland tijdsluik waarin continu bi directionele data uitwisseling nodig is. End devices synchroniseren zich hiervoor met het broadcast synchronization beacon message. Deze klasse was voor v1.1 enkel experimenteel en is aangeraden enkel te gebruiken bij end devices met versie 1.1 of 1.0.4 van het LoRaWAN protocol.
- Klasse C: voor hoge data beschikbaarheid. Deze luisteren continu naar downlink messages die om data kunnen vragen waardoor data direct opvraagbaar is. Dit brengt wel een veel hogere energieverbruik met zich mee waardoor dit eerder geschikt is voor niet batterij gevoede end devices.

Verder specifieert LoRaWAN ook een hele boel MAC commando's om info op te vragen of instellingen aan te passen.

3.3 Pakket Structuur

In het LoRa hoofdstuk werd de pakket structuur op de fysische laag reeds bekeken. In onderstaande figuur is een overzicht van de lagen binnen het LoRaWAN protocol.



Figuur 7 Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). Overview of the LoRaWAN packet structure [Illustration] LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. Sensors, 22(9), 3127. https://doi.org/10.3390/s22093127

Het donker blauwe gedeelte is de fysische laag. De PHY Payload bevat de informatie voor de MAC laag, waarbij de MAC Payload verdere informatie over de frame bevat. Indien de end device nog moet geactiveerd worden zal de PHY Payload geen MAC Payload bevatten, maar in de plaats de Join of Rejoin Request. Tot slot bevat de Frame Payload de informatie voor de LoRaWAN applicatie laag.

3.4 Beveiligingen

3.4.1 Geheime sleutels en Identifiers

Elke LoRaWAN end device heeft een unieke 128-bits AES geheime sleutel, de AppKey, en een globally unique identifier dat EUI-64-based is genaam de DevEUI. Beide worden gebruikt tijdens het device authenticatie proces. Voor het aanmaken van een EUI-64 moet de toekenner beschikken over een Organizationally Unique Indetifier (OUI) van de IEEE Registration Authority.

LoRaWAN netwerken zijn gelijkaardig identificeerbaar aan de hand van een 24-bit globally uniqe identiefier toegekend door de LoRa Alliance.

In LoRaWAN versie 1.1 wordt er ook nog gebruik gemaakt van een unieke 128-bits AES geheime netwerk sleutel, de NwkKey.

3.4.2 Encryptie en Sessies

Omdat bij radio eender wie transmissies kan ontvangen en opslaan wodrt er gebruik gemaakt van encryptie. Als encryptie methode wordt de Advanced Ecnryption Standard (AES) gebruikt met 128-bit symmetrische sleutels en algoritmes. LoRaWAN gebruikt de AES cryptographic primitive gecombineerd met enkele modes of operation afhankelijk van de te genereren sleutel. CMAC voor integrity, CTR voor encryptie, en ECB en CCM voor vertrouwelijkheid (Confidentiality).

Deze encrypties zorgen voor sessies. Een sessie start wanneer de end device geactiveerd wordt via de Join procedure. Hierbij worden symmetrische sessie sleutels aangemaakt gebaseerd op de symmetrische geheime sleutels.

- Network session: onderhouden door de end device en de Network Server (NS)
    - DevAddr (device address)
    - NwkSKey (network session key v1.0.x)
    - FNwkSIntKey, SNwkSIntKey, NwkSEncKey (zie overzicht, v1.1)
    - FCntUp, (N)FCntDwn (frame counter uplink, (network) frame counter downlink)
    - MAC state (channels, data rates, …)
- Application session: onderhouden door de end device en de Application Server (AS)
    - AppSKey (application session key)
    - FCntUp, (AFCntDwn) (frame counter uplink, application frame counter downlink)

Gedurende de LoRaWAN sessie veranderen de sessie sleutels niet

De AppSKey wordt gebruikt om de MAC Payload, die de data voor de Application Server bevat, te encrypteren aan de hand van AES-CTR. Zo wordt deze enkel leesbaar door wie over de AppSKey beschikt, dus ook niet door de Network Server (tegen spoofing, Authentication).

De NwkSKey wordt gebruikt om de Message Integrity Code (MIC) te berekenen aan de hand van AES-CMAC. Dit om aanpassingen van derden of beschadiging van de data door storingen tegen te gaan voor transmissies tussen end devices en de Newtork Server (Integrity).

3.4.3 Frame Counters

Om heruitzendingen van berichten (replay attacks) te kunnen detecteren en blokkeren wordt er gebruik gemaakt van Frame Counters. Bij activering van een end device worden de Frame Counters op nul gezet. Gedurende de LoRaWAN sessie worden ze verhoogd (incremented) en

nooit hergebruikt. Als een bericht ontvangen wordt dat een lagere Frame Counter heeft dan het vorige bericht wordt deze genegeerd.

Bij LoRaWAN versie reeks 1.0.x is er enkel spraken van een FCntUp voor uplink messages van end device naar de Network Server, en een FCntDwn voor downlink messages van Network Server naar end device.

Bij LoRaWAN versie 1.1 wordt de FCntDwn verder opgedeeld in een NFCntDwn voor downlink messages van de Network Server, en een AFCntDwn voor downlink messages van de Application Server.

Belangrijk om te weten is dat bij gebruik van ABP statische activatie (zie hoofdstuk 3.5 End Device Activatie en Join Procedure) de Frame Counters zullen resetten bij heropstart, zoals na firmware flashing of bij stroomverlies, als er geen persistent geheugen (NVM) aanwezig is. De FCntUp moet dan ook gereset worden aan de server zijde. Anders zullen alle berichten geblokkeerd worden tot de FCntUp weer hoger is geworden dan het laatste bericht ontvangen voor de reset van het end device. Bij The Things Network (TTN) vereist dit een her-registratie van het end device in de applicatie.

Bij gebruik van OTAA dynamische activatie worden de Frame Counters gerest bij elke nieuwe sessie. Dit dus zowel bij een Join of Rejoin.

3.4.4 Nonces

Een nonce (number once) is een willekeurig getal dat slechts eenmalig kan gebruikt worden met dezelfde sleutel in cryptografische communicatie.

In LoRaWAN worden twee nonces gebruikt:

- DevNonce
- AppNonce of JoinNonce

3.4.4.1 DevNonce

In LoRaWAN v1.1 en 1.0.4 is de DevNonce een 16-bit counter die start op nul en die verhoogd wordt telkens het end device een Join Request doet met hetzelfde JoinEUI. Deze mag niet herbruikt worden. Het word dus vereist dat de DevNonce persistent is en wordt bijgehouden in (secure tamper-proof) non-volatile memory (NVM) op het end device. Zo blijft deze behouden tijdens stroomverlies of power-cycling. Anders zal de Join Server met dat JoinEUI, die een aantal DevNonce ook bijhoud, de Join Request negeren.

In LoRaWAN v1.0 tot 1.0.3 is de DevNonce een random waarde en opgevolgd door de Network Server, mits er geen Join Server gespecifieerd is in deze versies van het protocol.

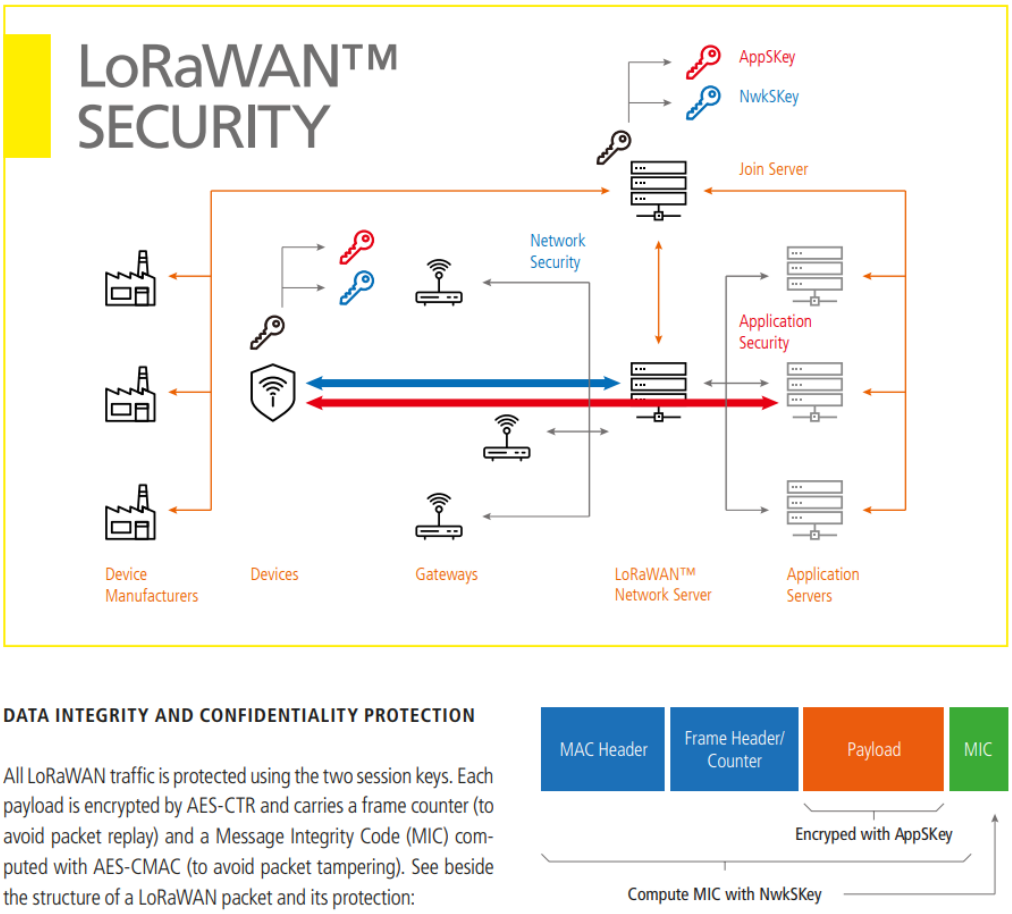
3.4.4.2 AppNonce of JoinNonce

Deze Nonce noemt in LoRaWAN v1.0 tot 1.0.3, AppNonce. Vanaf v1.1 en 1.0.4 werd deze hernoemt naar JoinNonce, samen met de henroeming van AppEUI naar JoinEUI.

De AppNonce of JoinNonce is een 24-bit counter waarde meegegeven in een Join Accept downlink message. Het end device dat de Join Request stuurde kan hieruit de sessie sleutels afleiden. Bij LoRaWAN 1.0.x end devices gebeurt dit aan de hand van de AppKey, en bij 1.1 aan de hand van de NwkKey.

3.4.5 Overzicht

- DevEUI Device Glabally Unique Identifier (Identification)
- AppEUI Application Unique Identifier (v1.0 tot 1.0.2) (Identification)
- JoinEUI Join Server Unique Identifier (vanaf v1.1 en 1.0.3) (Identification)
- AppKey Application (Secret Root) Key (Authentication)
- NwkKey Network (Secret) Key (Authentication)
- AppSKey Application Session Key (End-to-end Encryption)
- NwkSKey Network Session Key (v1.0.x) (End-to-end Encryption)
- SNwkSIntKey Serving Network Session Integrity Key (v1.1) (Integrity)
- FNwkSIntKey Forwarding Network Session Integrity Key (v1.1) (Integrity)
- NwkSEncKey Network Session Encryption Key (v1.1) (End-to-end Encryption)
- DevAddr Device Address (Identification APB activation)
- DevNonce Device Nonce value (tegen replay attacks)
- AppNonce Application Nonce value (voor afleiding sessie sleutels)
- NetID Network ID (unieke netwerk 1006 identifier, Identification)
- FCntUp Frame Counter Uplink messages (van device naar netwerk)
- FCntDwn Frame Counter Downlink messages (van netwerk naar device, v1.0.x)
- NFCntDwn Network Frame Counter Downlink messages (van netwerk naar device, v1.1)
- AFCntDwn Application Frame Counter Downlink messages (van applicatie naar device, v1.1)
- MIC Message Integrity Check (Integrity LoRaWAN message)



Figuur 8 Gemalto, Actility and Semtech. (2017, February). LoRaWAN Security [Graph] LoRaWAN Security Whitepaper. LoRa Alliance. https://LoRa-alliance.org/wp-content/uploads/2020/11/LoRaWAN_security_whitepaper.pdf

3.5 End Device Activatie en Join Procedure

Het LoRaWAN protocol voorziet allerlei methoden voor belangrijke beveiligingen zoals end device authenticatie (authentication), data integriteit (message integrity) en confidentialiteit (confidentiality). Deze fundamentel beveiligings aspecten worden geïnitialiseerd bij de end device activatie fase wanneer het toestel het LoRaWAN netwerk joined of rejoined.

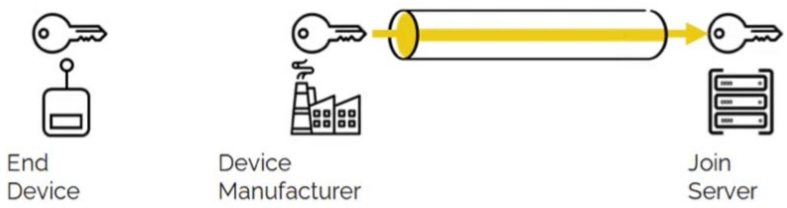
Er zijn twee methoden om een end device te activeren:

- Over-The-Air Activation (OTAA): dynamische join procedure waarbij het end device en het network bewijzen dat ze de AppKey kennen. Het ondersteund ook rejoin en rekey.
- Activation By Personalization (ABP): hardcoded voor één enkel netwerk, en persistent geheugen nodig voor het opslagen van de sleutels. Anders kunnen deze niet bijgehouden worden bij heropstart.

Op vlak van veiligheid wordt sterk aangeraden OTAA te gebruiken. Doordat ABP een vaste sessie heeft is de encryptie steeds hetzelfde. Wanneer deze gekraakt wordt is zo ineens alle voorgaande en toekomstige data ook leesbaar. Terwijl bij OTAA bij elke Join een nieuwe sessie wordt gecreëerd met nieuwe sleutels. In LoRaWAN 1.1 is er daarbovenop ook de mogelijkheid tot Rejoinen. Een Rejoin request kan om een bepaalde tijd met andere data mee verzonden worden om zo de sessie sleutels te vernieuwen waardoor de encryptie veranderd.

Bij OTAA is het echter ook belangrijk te beseffen dat de JoinEUI/AppEUI en de DevEUI als plain tekst verzonden wordt en dus publiek zichtbaar is. Aan de hand van de JoinEUI kan zo achterhaalt worden op welke server de geheime sleutels bewaard worden. Beveiliging van deze server is dus uiterst belangrijk. Liefst aan de hand van een Hardware Security Modules (HSM). Aan de hand van de DevEUI kan dan weer het type module en LoRaWAN versie achterhaalt worden.

Bij beide manieren moeten de geheime sleutels op een server bewaard worden. Hier gaat het om een trust relationship met de uitbater van deze server(s). Idealiter worden de sleutels rechtsreeks van de fabrikant overgedragen naar de Join Server met een HSM op een beveiligde manier.



Figuur 9 LoRaWAN Security in 5 Minutes. (2022, February 22). YouTube. https://www.youtube.com/watch?v=UIu-2zTs8dM

Afhankelijk van de LoRaWAN protocol versie van het end device en de backend zal de Join procedure op een andere manier gebeuren. We onderscheiden hier de versie reeksen 1.0.x en 1.1 van het protocol.

3.5.1 LoRaWAN v1.0.x Join Procedure

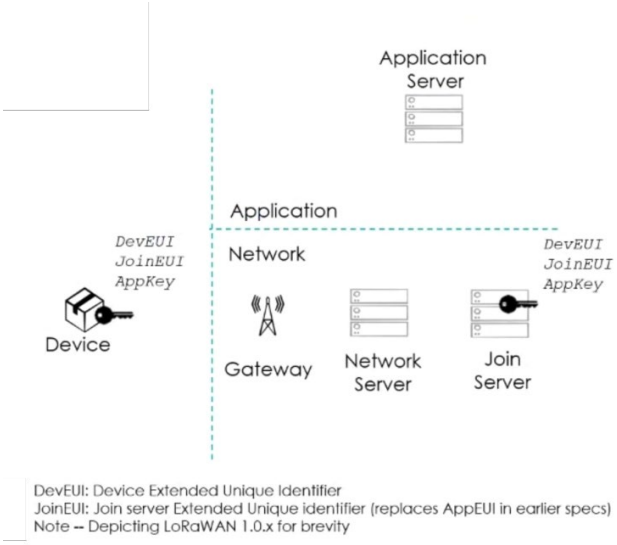
3.5.1.1 LoRaWAN 1.0.x OTAA

Deze versie vereist een DevEUI, AppEUI/JoinEUI, en AppKey.
(De JoinEUI is de hernaming van de AppEUI voor versie 1.1 en later ook 1.0.3.)

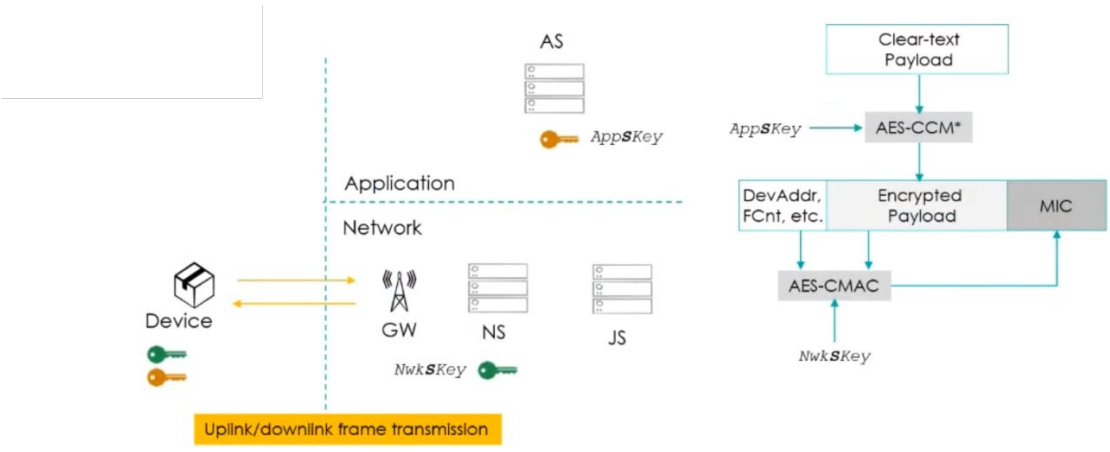
Voor elke sessie wordt een AppSKey en een NwkSKey aangemaakt.

De procedure is als volgt:

1) De DevEUI, AppEUI en AppKey worden opgeslagen in zowel het end device als het netwerk waarmee gejoined wilt worden.
2) Het end device maakt een join request uplink message aan met de AppEUI, DevEUI, DevNonce en een Message Integrity Code (MIC). De MIC wordt berekend aan de hand van de AppKey en het join request message.
3) Wanneer het join request ontvangen wordt en toegelaten zal het netwerk de sessie sleutels AppSKey en NwkSKey genereren en een join accept downlink message terugsturen. Deze bevat de random nonce AppNonce, NetID, DevAddr en parameters voor de fysische laag als ook de MIC. Deze is geëncrypteerd met de AppKey.
4) Bij aankomst terug bij het end device worden aan de hand van de AppNonce en AppKey, de AppSKey en NwkSKey afgeleid.
5) Om end-to-end encryptie op te kunnen zetten, behound de Network Server de NwkSKey en geeft de AppSKey aan de Application Server.



Figuur 10 LoRaWAN security webinar. (2019, January 16). Symmetric keys storage [Illustration] Actility. YouTube. https://www.youtube.com/watch?v=S6nJzSc4iy4



Figuur 11 LoRaWAN security webinar. (2019, January 16). Transmission encryption [Illustration] Actility. YouTube. https://www.youtube.com/watch?v=S6nJzSc4iy4

3.5.1.2 LoRaWAN 1.0.x ABP

Bij ABP worden enkel de DevAddr, AppSKey en NwkSKey gebruikt. Deze worden op voorhand geprogrammeerd in het end device, de Netwerk Server en de Application server.

3.5.2 LoRaWAN v1.1 Join Procedure

3.5.2.1 LoRaWAN 1.1 OTAA

Deze versie vereist een DevEUI, JoinEUI, AppKey en NwkKey
De AppEUI is hernoemd naar JoinEUI omdat hier het gebruik van een Join Server gespecifieerd wordt en de JoinEUI wordt specifiek gebruikt om deze JS te identificeren. Het gebruik van een Join Server laat in deze versie toe om de te gebruiken Network Server te herconfigureren voor roaming of eigenaar overdracht. De segmentatie van servers zorgt er hier ook voor dat de Network Server de geheime sleutels niet kent en dus ook niet kan blootstellen.

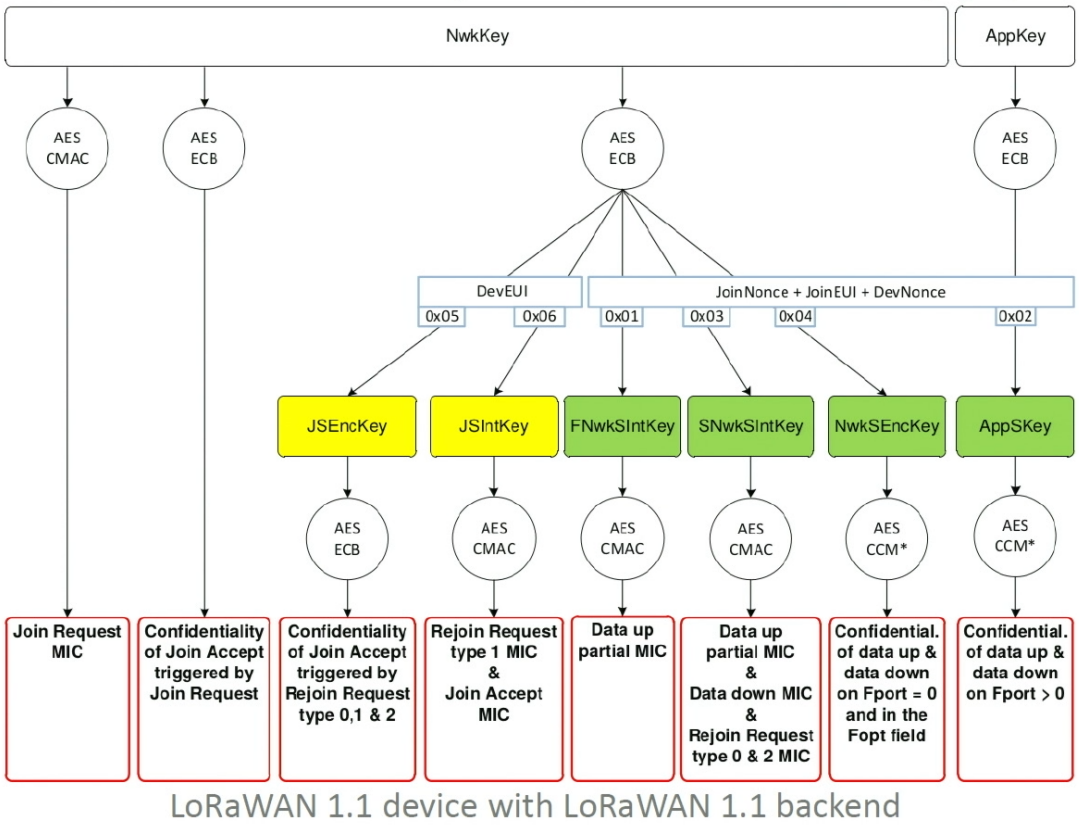
Voor elke sessie wordt een AppSKey, en de netwerk sessie wordt opgedeeld in SNwkSIntKey, FNwkSIntKey en NwkSEncKey.

De procedure is als volgt:

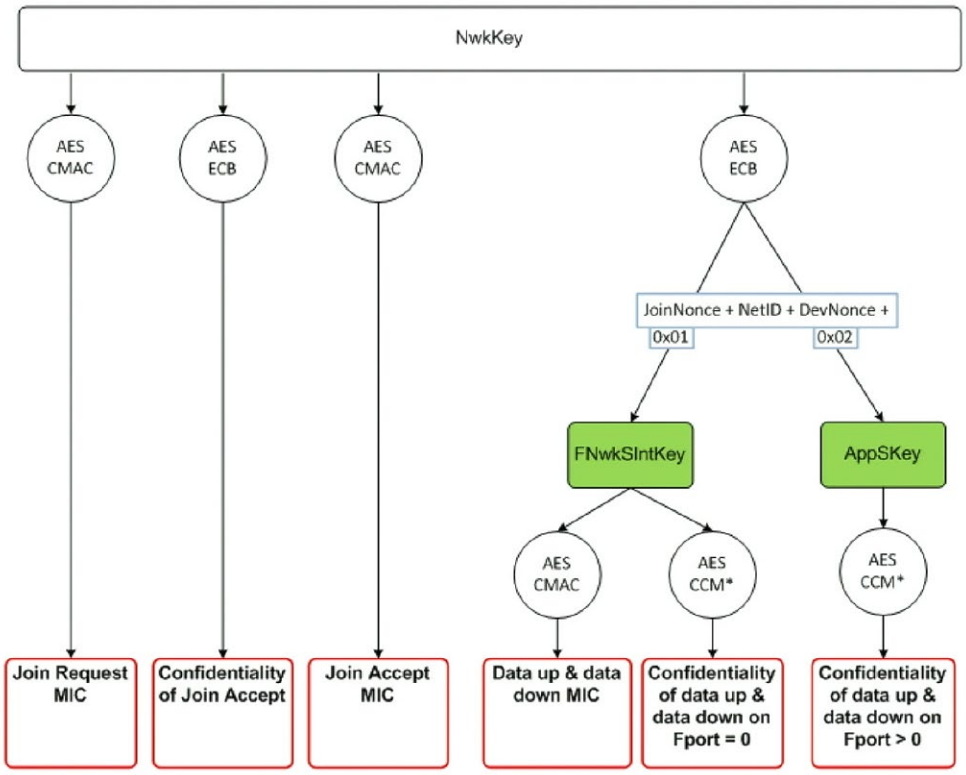
1) De DevEUI, JoinEUI, AppKey en NwkKey worden opgeslagen in het end device. De DevEUI, AppKey en NwkKey worden ook opgeslagen in de Join Server.
2) Het end device maakt een join request uplink message aan. Deze bevat De DevEUI, JoinEUI, DevNonceen MIC. Hier wordt de MIC berekend met de NwkKey (ipv de AppKey bij 1.0.x).
3) Bij ontvangst en acceptatie van de join request uplink message gaat de Network Server de Join Server identificeren aan de hand van de JoinEUI en DNS.
4) Een JoinReq message wordt naar de Join Server gestuurd. De bevat het originele join request uplink message als ook device relevante parameters.
5) Bij ontvangst van de Join Server zal deze de netwerk sessie sleutels aanmaken, namelijk SNwkSIntKey, FNwkSIntKey en NwkSEncKey, als ook de AppSKey (gebruikt voor Integrity en Confidentiality checks op de MAC commands en payload data).
6) De sessie sleutels samen met het join accept downnlink message worden vervolgens door de Join Server geëncrypteerd aan de hand van de NwkKey en ingesloten in het JoinAns message (Join Answer) dat teruggestuurd wordt naar de Network Server.
7) Bij ontvangst en verificatie zal de Network Server het join accept downlink message forwarden naar het end device.
8) Het end device leidt de sessie sleutels af uit het join accept downlink message aan de hand van de AppKey en NwkKey.
9) De Application Server ontvangt vervolgens ook de AppSKey van de Network Server bij het eerste uplink message van het end device.

Onderstaande diagrammen geven een uitgebreid overzicht welke geheime sleutel voor wat gebruikt wordt en welke algoritmes hiervoor gebruikt worden.

Het is hier ook belangrijk te vermelden dat een LoRaWAN netwerk met versie 1.1 van het LoRaWAN protocol niet backwards compatible is met end devices die versie reeks 1.0.x. De meeste providers, zoals The Things Network (TTN), voorzien dit en hebben twee versies aanwezig in hun The Things Stack V3. End devices met versie 1.1 kunnen echter wel werken met netwerken die op versie reeks 1.0.x werken. Bij deze wordt dan echter de NwkKey gebruikt voor authenticatie in plaats van de AppKey zoals in v1.0.x het geval is, zoals u kan zien in de tweede onderstaande diagram.



Figuur 12 From LoRaWAN 1.0 to 1.1: Security Enhancements - Renaud Lifchitz - The Things Conference 2019. (2019, February 11). LoRaWAN 1.1 Keys. [Diagram] The Things Network. YouTube.



Figuur 13 From LoRaWAN 1.0 to 1.1: Security Enhancements - Renaud Lifchitz - The Things Conference 2019. (2019, February 11). LoRaWAN 1.0 Keys. [Diagram] The Things Network. YouTube.

3.5.2.2 LoRaWAN 1.1 PBA

PBA werkt bij versie 1.1 nagenoeg hetzelfde als bij 1.0.x.

De sessie sleutels en de DevAddr worden voorgeprogrammeerd in zowel het end device als de Network Server en Application Server.

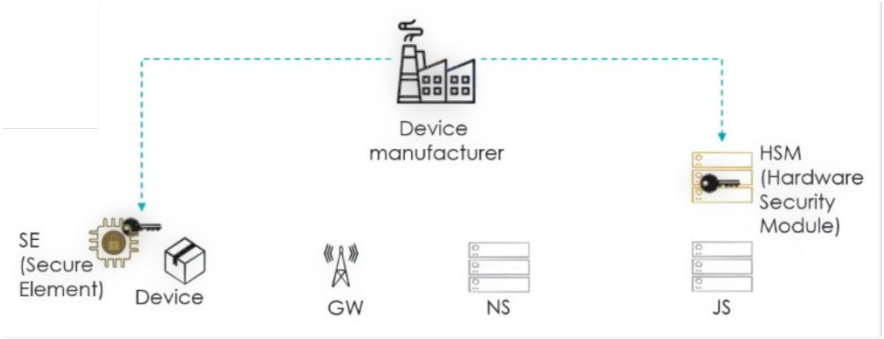
3.6 LoRaWAN Is Secure (but Implementation Matters)

Het belangrijkste aspect bij het ontwikkelen en gebruiken van IoT toestellen, als het aankomt op beveiliging, is een correcte en goede implementatie. LoRaWAN heeft een uitgebreide beveiliging, maar als er zwakheden zijn buiten het bereik van het protocol valt heel de beveiliging in elkaar.

Implementation Matters zijn aanbevelingen en industry best practices voor implementatie gegeven door de LoRa Alliance en security specialisten.

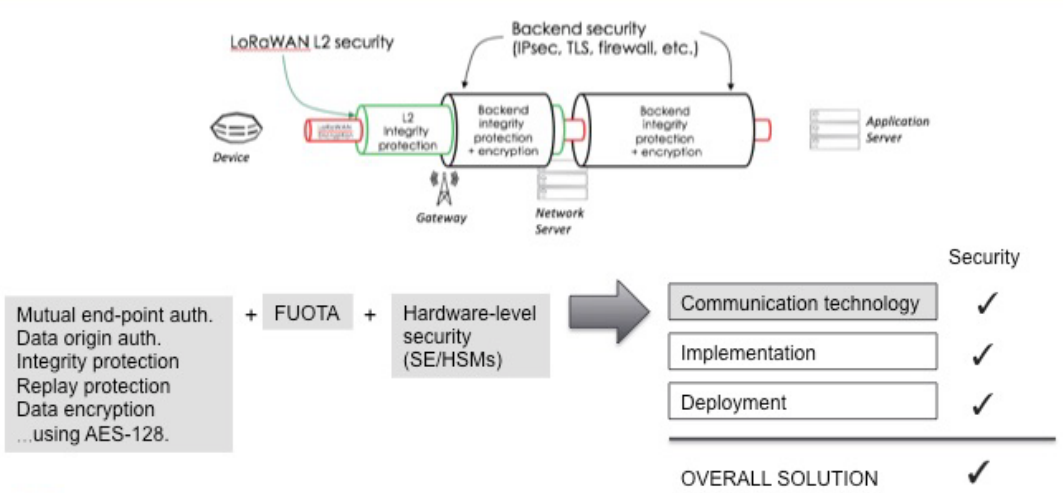
Enkele voorbeelden:

- Het gebruik van Secure Elements in end devices en Hardware Security Modules (HSM) in servers voor het bijhouden van geheime sleutels en het uitvoeren van cryptografie. De sleutels mogen zeker nergens hardcoded zijn of verzonden worden als plain text in email.



Figuur 14 LoRaWAN security webinar. (2019, January 16). Hardware Security [Illustration] Actility. YouTube. https://www.youtube.com/watch?v=S6nJzSc4iy4

- Het gebruik van een cryptografisch protocol als Transport Layer Security (TLS) in de backend communicatie tussen de Network Server en de Application Server.



Figuur 15 LoRa Alliance. (n.d.). LoRaWAN® Is Secure (but Implementation Matters) [Illustration]. LoRa Alliance. https://LoRa-alliance.org/resource_hub/LoRaWAN-is-secure-but-implementation-matters/

- Bij voorkeur OTAA gebruiken in plaats van ABP join mode.
- Gebruik constante lengte messages met padding. De cipher tekst heeft dezelfde lengte als de plain tekst. Hieruit kan afgeleid worden over welke verschillende data het gaat en deze onderscheiden van elkaar.
- Gebruik een afzonderlijke Join Server (JS).
- Hergebruik geen sleutels op verschillende end devices.
- Gebruik geen end devices waarbij private sleutels kunnen uitgelezen worden aan de hand van ingebouwde commando's of een debug mode.
- Pas de duty cycle toe.
- Gebruik binaire messages in plaats van JSON.
- Voor private netwerken, monitor actief de gateways op actieve aanvallen.
- Geheime sleutels moeten random aangemaakt worden per toestel.
- Gebruik geen willekeurige DevEUI's, maar respecteer IEEE OUI's.
- Gebruik geen willekeurige DevAddrs, maar respecteer de LoRa Alliance NetID/NwkID allocations.
- Gebruik geen willekeurige JoinEUI/AppEUI. Deze moet naar een echte JS wijzen met legitieme IEEE OUI.
- Update toestellen met software/firmware pacthes via Firmware Update Over The Air (FUOTA) enkel met ondertekende firmware van de fabrikant. Gebruik makend van integrity-protected multicast delivery (met group key) of integrity-protected unicast commands (met device key).
- Secure boot: end devices zouden bij opstarten moeten nagaan of de firmware ondertekend is door de fabrikant.
- Firmware update verification: binnenkomende firmware updates zouden moeten nagegaan worden dat deze ondertekend is door de fabrikant.
- Hergebruik nooit nonces voor end device activatie en frame counters.
- Geef voorkeur aan een Join Server te gebruiken bij een vertrouwde derde partij.

4. Mogelijke Aanvallen

In deze sectie worden de meest relevante mogelijke aanvallen (attacks) overlopen en welke effecten op C.I.A ze hebben. Dit is voornamelijk een samenvatting van de informatie beschikbaar in referentie [19].

C.I.A staat voor:

- Confidentiality of vertrouwelijkheid: De informatie is enkel toegankelijk voor rechthebbende. Dit kan aan de hand van encryptie, geheime sleutels, passwoorden.
- Integrity of integriteit: De correctheid van de informatie. Of deze niet beschadigd is door storingen of aangepast door derden. Dit kan met gebruik van hashes, AES-CMAC, MIC.
- Availability of beschikbaarheid: De informatie is beschikbaar voor rechthebbende. De informatie zelf of de toegang ertoe kan op één of andere wijze worden geblokkeerd. Dit kan verholpen worden door backup, redundante servers, firewalls, load balancers.

De meest relevante mogelijke aanvallen bij LoRaWAN zijn:

- Sniffing → Confidentiality
- Covert Channels → Confidentiality en Integrity
- Jamming Attacks → Availability
- Key Extraction Attack → Confidentiality en Integrity
- Wormhole Attack → Availability
- Energy Attack → Availability

4.1 Sniffing

Sniffing is een vorm van eavesdropping. LoRaWAN berichten zijn radio dus deze kunnen vrij ontvangen worden. Zonder de juiste sleutels is het echter niet mogelijk deze te lezen. Een sniffer is echter niet uit op het lezen van deze berichten maar puur de detectie ervan. Bij LoRaWAN beginnen berichten bijvoorbeeld telkens met een bepaalde preamble dat het begin van een bericht duidelijk maakt. Op zich niets gevaarlijk, maar het kan gebruikt worden om meer geavanceerde aanvallen uit te voeren zoals man-in-the-middle attack of als detectie wanneer een transmissie start om deze te verstoren met een jamming attack. Dit kan zeer eenvoudig met een LoRa module en Arduino of een Software Defined Radio (SDR).

4.2 Covert Channels

Covert channels is een manier voor aanvallers om gevoelige data te verzenden vanuit een toestel zonder detectie van het slachtoffer. Bij LoRaWAN kan er bij een typisch pakket een extra 38-bits mee worden gestuurd aan de hand van amplitude modulatie bovenop de physical LoRa payload. Zo kan bijvoorbeeld de AppKey of AppSKey verkregen worden uit een end device in slechts vijf LoRaWAN pakketjes. Deze methode is wel beperkt tot een bereik van 250m.

4.3 Jamming Attacks

Een Jamming Attack is een vorm van Denial-of-Service (DoS) aanval door opzettelijke interferentie, of verstoring, op een draadloze fysische laag.

Jamming kan op verschillende manieren:

- Continuous Jamming

- Reactive/Selective Jamming
- DevNonce randomness manipulation

4.3.1 Continuous Jamming

Continuous Jamming is de continue verstoring van een bepaald draadloos kanaal door het continu uitsuren van een sterk RF signaal.

4.3.2 Reactive/Selective Jamming

Met gebruik van een sniffer word gedetecteerd wanneer een transmissie begint en eventueel door wie. Hiermee kan er enkel op de juiste momenten jamming plaats vinden om bijvoorbeeld slecht een bepaalde zender te verstoren. Deze manier maakt detectie veel moeilijker omdat interferentie ook onopzettelijk kan plaats vinden.

4.3.3 DevNonce randomness manipulation

Bij LoRaWAN v1.0 tot 1.0.3 is de DevNonce, die Replay Attacks op Join Request detecteerd, telkens een random waarde. Bij bepaalde LoRa modems gebruikt in end devices werkt de randomness generator voor de DevNonce aan de hand van RSSI sampling van de LoRa ontvanger. Door een bepaalde of continu dezelfde golfvorm naar deze ontvanger te sturen zal de randomness generator telkens dezelfde waarde genereren. Doordat de DevNonce nu altijd hetzelfde blijft worden Join en Rejoin Requests genegeerd en kan het end device dus niet meer in het netwerk geraken.

4.4 Key Extraction Attack

In de LoRaWAN cryptografie is het van uitermate belang dat de geheime sleutels confidentieel blijven. Het protocol specifieert echter geen hardware, maar enkel aanbevelingen hoe best om te gaan met de sleutels en hoe ze op te slaan. Het hangt dus af van de implementatie van de fabrikant of deze al dan niet veilig zijn.

We onderscheiden twee manieren:

- Hardcoded sleutels
- Side-Channel Attack

4.4.1 Hardcoded sleutels

Bij de LoRaMAC libraries bijvoorbeeld wordt de AppKey rechtstreeks in de code ingegeven. Door toegang tot de hardware van een end device kan de AppKey dus teruggevonden worden aan de hand van firmware dump of een microcontroller debug interface.

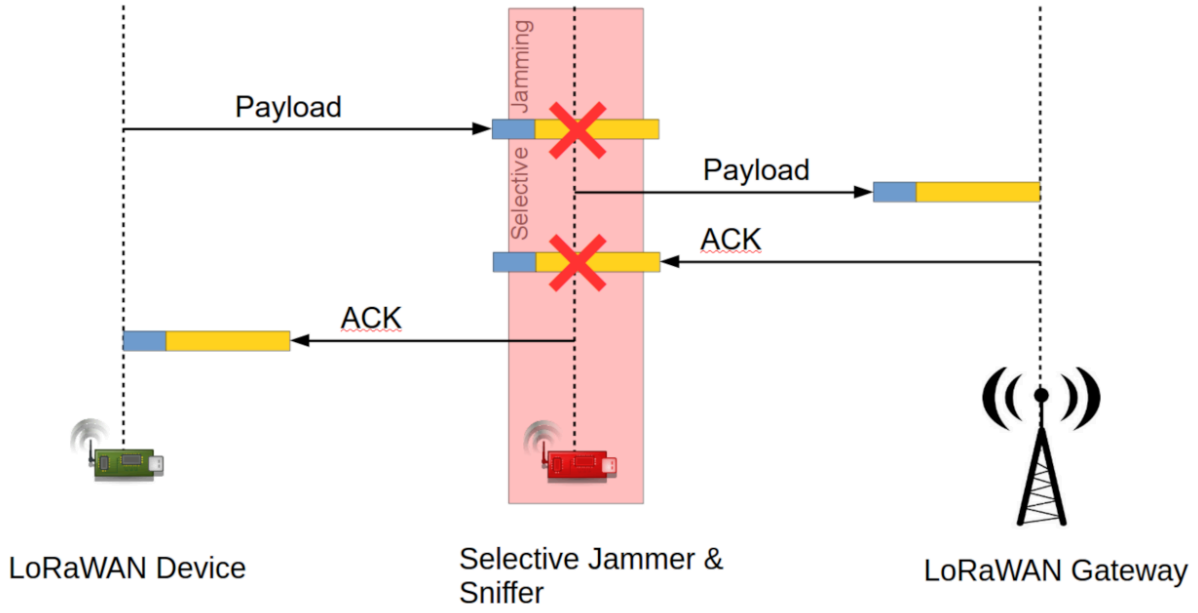
4.4.2 Side-Channel Attack

In Side-Channel Attacks word gevoelige data indirect verkregen door het meten van een fysisch element van het doelwit toestel. Bij microcontrollers met een lage kloksnelheid (in de MHz) is het mogelijk informatie af te leiden uit metingen van stroomverbruik. LoRaWAN end devices gebruiken meestal zo'n microcontrollers. Aanvallers kunnen door het AES-CTR algoritme als doelwit te nemen zo de AppSKey en NwkSKey te pakken krijgen doordat de plaintext payload door dit algoritme gaat.

4.5 Wormhole Attack

Een Wormhole Attack is het kwaadwillend rerouten van data pakketen. Dit beïnvloed de stabilitiet van het netwerk, maar ook de beschikbaarheid van data. Voor LoRaWAN kan dit door een Sniffer te combineren met Selective Jammer en een Replay Attack. Een Replay Attack op zich is zeer moeilijk. Zeker vanaf LoRaWAN v1.1 en 1.0.4 waarbij de DevNonce naast de Frame Counters ook een teller is geworden. Door dit te combineren met Jamming is dit echter wel mogelijk.

Onderstaand diagram toont de werking aan van een Wormhole Attack in twee richtingen.



Figuur 16 Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). Bidirectional wormhole attack in LoRaWAN [Diagram] LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. Sensors, 22(9), 3127. https://doi.org/10.3390/s22093127

Verder laten LoRaWAN Wormhole Attacks ook toe de metadata te manipuleren. Dit aspect kan verder gebruikt worden om DoS en battery-draining attacks uit te voeren. Zo kan bijvoorbeeld het Adaptive Data Rate (ADR) mechanisme gemanipuleerd worden door metadata spoofing waardoor een end device kan geforceerd worden om een bepaalde Spreading Factor en Transmission Power te gebruiken die niet detecteerbaar zijn door legitieme packet forwarders.

4.6 Energy Attack

Een Energy Attack is een DoS aanval gericht op batterij gevoede toestellen waarbij het stroomverbruik van het toestel zo hoog mogelijk wordt gemaakt.

Bij LoRaWAN kan dit op twee manieren:

- Direct Jamming
- Downlink Package Reception Mode uitbuiting

4.6.1 Direct Jamming

De eenvoudigste manier is door het end device zelf te jammen. Een end device wacht na versturen steeds op een ACK downlink message als bevestiging dat het uplink message is ontvangen. Krijgt het geen ACK dan zal het uplink message heruitgezonden worden.

4.6.2 Downlink Package Reception Mode uitbuiting

In Klasse A end devices, waarbij het stroomverbruik het laagst is van alle klassen, is het hoogste stroomverbruik tijdens transmissie waarbij beide de RF verzender en ontvanger actief zijn. Na verzenden van een uplink message zijn er twee momenten voor het ontvange van downlink messages waarna de ontvanger weer in slaap modus gaat. Deze zijn beperkt in tijd en zeer kort mits er niets ontvangen wordt. Als een aanvaller nu kan synchroniseren met de transmissie en een downlink message stuurt die maximaal duurt wordt de ontvanger in Downlink Package Reception Mode geforceerd voor een veel langere tijd dan normaal. Hiermee kan het stroomverbruik aanzienlijk verhoogd worden en de batterij levensduur met jaren verkort worden.

5. Praktische Tests

5.1 Leren werken met RN2483

5.1.1 Wat is RN2483?

De RN2483 is een radio module gebaseerd op LoRa. Deze werkt op de 868MHz en 464MHz frequenties.

5.1.2 Hardware

De hardware schakeling voor de RN2483 is redelijk simpel, maar je moet de datasheet goed lezen!

RN2483	Arduino Nano
TX	RX
RX	TX
RST	12
3V3	3V3
GND	GND

De RN2483 werkt op 3.3V. Verbind geen 5V aan de 3V3 pin! Dit kan de RN2483 kapot maken.

TX en RX zijn de communicatie pinnen van de RN2483. De communicatie gebeurt volgens het UART protocol. De default baudrate van de RN2483 is 57600.

Je moet altijd een newline en carriage return achter het commando zetten dat je verstuurt.

5.1.3 Software

Ook de software om met de RN2483 te communiceren hebben we simpel gehouden. Dit betekent dat je veel handmatig moet instellen, maar je hebt wel meer controle over de module dan je zou hebben met een library. Hoe je de RN2483 moet instellen vind je in de datasheet.

Voor je kan verbinden met TTN moet je wat instelling in stellen. Dit is het moeilijkste en belangrijkste. Het uitzoeken van welke instelling op welke manier ingesteld moeten zijn was niet heel simpel. Uiteindelijk met veel experimenteren en leren over LoRaWAN is het ons gelukt om deze juist in te stellen. Om deze instellingen in te stellen heb je een soort van interface nodig om te communiceren met de RN2483. Deze kan eender welke interface zijn die over UART ondersteunt.

Wij hebben gekozen voor een Arduino Nano en hebben dan ook een klein scriptje geschreven dat het commando leest vanuit de seriele monitor op baudrate 9600 en dan dit commando exact kopieert naar de softwareserial poorten op pin 4 en 5 met baudrate 57600.

In principe is dit alles wat je nodig hebt. Nu kan je in de seriele monitor al je commando's schrijven en deze worden dan verstuurd naar de RN2483.

```
#include <SoftwareSerial.h>
SoftwareSerial mySerial(4, 5); // RX, TX
void setup() {
        Serial.begin(9600);
        mySerial.begin(57600);
        Serial.println("test");
}

void loop() {
        if (mySerial.available()) {
                Serial.write(mySerial.read());
         }
        if (Serial.available()) {
                mySerial.write(Serial.read());
        }
}
```

Nu dat je een interface hebt kan je beginnen met de nodige instellingen van RN2483 in te stellen

Instelling	Commando	Beschrijving
Reset Frequentie	mac reset 868/r/n	
Set DevEUI	mac set deveui <deveui>	<deveui> moet je vervangen door de deveui van de module. Deze kan je achterhalen door middel van hetvolgende commando: mac get deveui/r/n Als er nog geen deveui is ingesteld dan moet je kan je de hweui gebruiken. Deze kan je achterhalen door middel van hetvolgende commando: sys get hweui/r/n
Set AppEUI	mac set appeui <appeui>	<appeui> moet je vervangen door de appEUI dat je hebt ingesteld in TTN.
Set appKey	mac set appkey <appkey>	<appkey> moet je vervangen door de appKey die je hebt ingesteld in TTN
Set Output Power	mac set pwridx 5	Deze zet je best zo hoog mogelijk om zo veel mogelijk stroom te besparen. (5 is max, 1 is min)
Set Data Rate	mac set dr 5	
Set adaptive data rate	mac set adr on	Deze zet je best aan als je graag een groot mogelijk bereik wilt hebben.
Set automatic replies	mac set ar off	In onze opstelling gebruiken we enkel klasse A LoRaWAN devices. Er zijn geen replies nodig.
Save	mac save	Bewaar de instellingen zodat je deze niet opnieuw moet instellen als de stroomtoegang verloren geraakt

Nu dat de RN2483 helemaal juist is ingesteld kan je verbinden met TTN.

5.2 Testing

5.2.1 Verbinden met TheThingsNetwork

Om te verbinden met TTN moet je eerst je device registreren met de TTN. Dit lijkt in het begin heel moeilijk, maar samen met de datasheet lukt dit heel vlotjes. Eens je module geregistreerd is, juist ingesteld met de commando's van de het vorige deel en je hebt bereik met een gateway van TTN, dan kan je gewoon verbinden met 1 simpel commando:

mac join otaa/r/n

5.2.2 Data sturen naar TheThingsNetwork

Om data te sturen naar TTN is het ook gewoon een heel simpel commando:

mac tx uncfn 1 <data>

je moet <data> vervangen door de data die je wilt doorsturen in HEX geëncodeerd.

5.2.3 Proberen Jammen

Om te jammen is het in principe niet meer als gewoon luider dan de rest, ruis te versturen op dezelfde frequentie. Dit hebben we geprobeerd door de volgende instellingen aan te passen en dan de volgende commando's uit te voeren:

Commando	Beschrijving
mac set pwridx 1	Dit zet de power index op het maximum
mac set adr off	Dit zet adaptive data rate af, om te jammen moet je zeker op dezelfde frequentie en data rate zitten. Adaptive data rate kan de frequentie en data rate aanpassen afhankelijk van signaal sterkte naar de gateway.
mac tx uncfn 1 <data>	Dit continue uitvoeren. Zo hoopte we om te jammen terwijl dat de jammer naast de module zit die je wilt jammen.

Dit zorgde voor geen signaal verlies. Onze theorie is dat de output power nog niet hoog genoeg is om voldoende te jammen. We hebben daarna het volgende geprobeerd:

Commando	Beschrijving
radio set pwr 14	Dit zet de output power op het maximum dat de module aankan, dit is net buiten de LoRaWAN specificatie. We hoopte dat dit een groter effect zou hebben.
mac set adr off	Ook hier weer moet adaptive data rate afgezet worden
mac tx uncfn 1 <data>	Deze keer was er af en toe een beetje signaalverlies te merken op de module die gejammed wordt, maar dit was niet groot genoeg om met zekerheid te zeggen dat het komt door de jammer.

Het jammen blijkt een stuk moeilijker met de RN2483 dan verwacht. We zijn er zeker van dat dit een stuk simpeler zou zijn met een SDR. Een andere mogelijkheid dat we niet voluit getest hebben is om meer spanning en stroom te geven aan de chip dan wat die verwacht. Zo zou de power output hoger kunnen zijn, maar dan riskeer je de integriteit van de RN2483.

6. Conclusie

Alhoewel we er niet in geslaagd zijn een succesvolle aanval uit te voeren, hebben we heel veel bijgeleerd. Zowel over de security werking van LoRaWAN als ook de werking van de RN2483. We hebben heel veel ervaring opgedaan over werken met LoRaWAN en LoRa modules.

We zijn wel positief dat met wat meer tijd een jammer bouwen en daarmee een wormhole attack uitvoeren haalbaar is.

7. Referenties

1. Perković, T., Rudeš, H., Damjanović, S., & Nakić, A. (2021). Low-Cost Implementation of Reactive Jammer on LoRaWAN Network. *Electronics*, *10*(7), 864.

   https://doi.org/10.3390/electronics10070864

2. Dams, T. (2022). *Cyberboswachters* (0.4.2.2 ed.). AP Hogeschool.

   https://learning.ap.be/pluginfile.php/1785831/mod_resource/content/7/book.pdf

3. Wikipedia contributors. (2022, May 24). *LoRa*. Wikipedia.

   https://en.wikipedia.org/wiki/LoRa

4. *What are LoRa and LoRaWAN?* (2021, December 12). The Things Network.

   https://www.thethingsnetwork.org/docs/LoRaWAN/what-is-LoRaWAN/

5. LoRa Alliance. (2021, May). LoRaWAN® Regional Parameters (No. RP002-1.0.3).

   https://LoRa-alliance.org/wp-content/uploads/2021/05/RP-2-1.0.3.pdf

6. *LoRaWAN®*. (n.d.). The Things Network.

   https://www.thethingsnetwork.org/docs/LoRaWAN/

7. *LoRa/LoRaWAN tutorial 21: OTAA, ABP and LoRaWAN Security*. (2018, October 20). YouTube.

   https://www.youtube.com/watch?v=KrNDOBzhxeM

8. *The missing puzzle pieces of LoRaWAN Security - by Johan Stokking*. (2018, September 19). YouTube.

   https://www.youtube.com/watch?v=6IDaUxhEgaI

9. *What is new in LoRaWAN 1.1?* (2017, November 2). YouTube.

   https://www.youtube.com/watch?v=ewsXKc3bk1U

10. *LoRaWAN Security in 5 Minutes*. (2022, February 22). YouTube.

    https://www.youtube.com/watch?v=UIu-2zTs8dM

11. *Everything you need to know about LoRaWAN in 60 minutes - Johan Stokking (The Things Industries)*. (2021, February 1). YouTube.

    https://www.youtube.com/watch?v=ZsVhYiX4_6o

12. LoRa Alliance. (2020, October 7). *Resource Hub*.

    https://LoRa-alliance.org/resource-hub/

13. Gemalto, Actility and Semtech. (2017, February). *LoRaWAN Security Whitepaper*. LoRa Alliance.

    https://LoRa-alliance.org/wp-content/uploads/2020/11/LoRaWAN_security_whitepaper.pdf

14. LoRa Alliance. (2020a, February). *LoRaWAN Security FAQ* (No. v2).

    https://LoRa-alliance.org/wp-content/uploads/2020/11/la_faq_security_0220_v1.2_0.pdf

15. *LoRaWAN security webinar*. (2019, January 16). Actility. YouTube.

https://www.youtube.com/watch?v=S6nJzSc4iy4

16. *LoRaWAN 1.0.4 - Alper Yegin (LoRa Alliance Technical Committee)*. (2021, February 5). YouTube. https://www.youtube.com/watch?v=20pyKQV0BKw
17. *From LoRaWAN 1.0 to 1.1: Security Enhancements - Renaud Lifchitz - The Things Conference 2019*. (2019, February 11). YouTube. https://www.youtube.com/watch?v=FsO5zxYHfKw
18. *End Device Activation*. (2021, November 26). The Things Network. https://www.thethingsnetwork.org/docs/LoRaWAN/end-device-activation/
19. Ruotsalainen, H., Shen, G., Zhang, J., & Fujdiak, R. (2022). LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors*, *22*(9), 3127. https://doi.org/10.3390/s22093127