

ISM Wireless

Bluetooth Low Energy
LoRa (WAN)

Ward De Ridder
on8wr



AP HOGESCHOOL
ANTWERPEN

AP.BE

About me

- Training Coordinator + lecturer associate degree IoT @ AP University of Applied Science Antwerp
- Previously: Radio engineer @ (AEG) TranzCom
- Member of OT5A contest team
- Fri3d camp orga
- President & Trainer Badminton Klub Berlaar VZW
- Technical consultant (freelance)

ISM Banden

ISM Banden

- *industrial, scientific, and medical*
- Bij BIPT: Niet-specifieke korteafstandsapparatuur
- “Vrij te gebruiken”
 - Met een heel aantal voorwaarden:
 - Maximale vermogen
 - Maximale duty cycle
 - Maximale bandbreedte
 - Beperkte modulatietypes / ...
 - CE

ISM Frequencies

- 26.957-27.283 MHz
- 433.05-434.79 MHz
- 863-870 MHz
- 2400-2483.5 MHz
- 5725-5875 MHz
- 24-24.25 GHz
- 61-61.5 GHz
- ...

België	Radio-interface Specificatie	SRD/Niet-specifieke toepassingen	B01-21 - V4.1 - 18-02-20
--------	------------------------------	----------------------------------	--------------------------

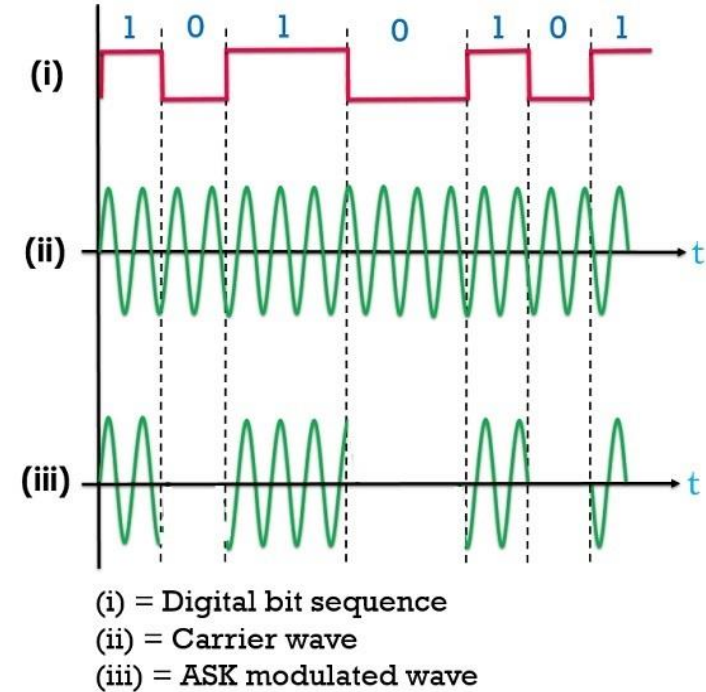
	Nr	Parameter	Beschrijving	Opmerkingen
Normatief gedeelte	1	Radiocommunicatiedienst	Mobiel	
	2	Toepassing	Niet-specifieke kortereafstandsapparatuur	
	3	Frequentieband	868-868.6 MHz	
	4	Channelling		
	5	Modulatie/Bezette bandbreedte		
	6	Richting / Scheiding		
	7	Zendvermogen/Vermogensdichtheid	25 mW e.u.v.	
	8	Regels inzake kanaaltoegang en -bezetting	Vereisten betreffende technieken om toegang te krijgen tot spectrum en om interferentie te onderdrukken zijn van toepassing. Als alternatief is een maximale duty cycle van 1 % toegestaan.	
	9	Vergunningsstelsel	Algemene machtiging	Op basis van NIB/NPB (Non interference basis/ non protection basis)
	10	Extra essentiële eisen		
	11	Veronderstellingen inzake frequentieplanning		
Informatief gedeelte	12	Geplande wijzigingen		
	13	Referentie	Meest recent versie van Beschikking 2006/771/EG EN 300 220 ERC/REC 70-03	Uitsluitend de versie(s) vermeld in de meest recente lijst geharmoniseerde normen onder de richtlijn 2014/53/EU (RED) zoals gepubliceerd door de Europese Commissie in het PB van de EU kan (kunnen) worden gebruikt om vermoeden van overeenstemming te genieten.
	14	Notificatienummer		
	15	Opmerkingen	Klasse 1 volgens de Beschikking 2000/299/EG	

Digitale modulatie

Korte introductie

Amplitude Shift Keying

- Gelijkaardig aan CW
- Bij 1 is er signaal, bij 0 is er geen signaal



Multi-ASK (4-ASK or Quad ASK)

ASK with more than two input levels

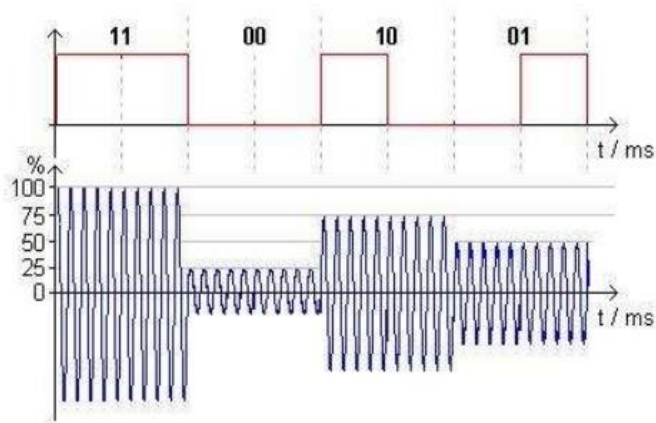
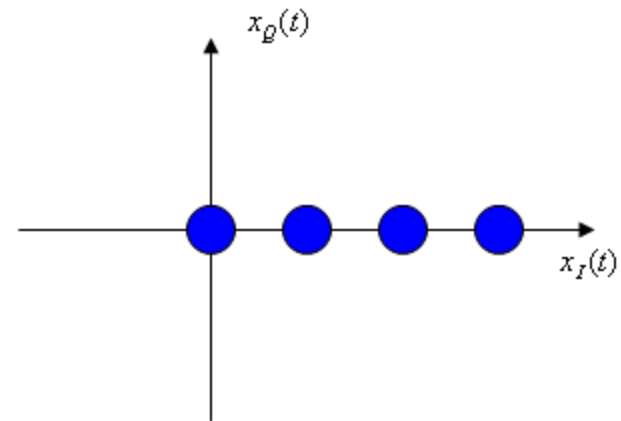


Image source: <https://www.slideshare.net/Tehnanali/digital-modulation-61719297>



Frequency Shift Keying

- 1 frequentie voor 0
- een andere frequentie voor 1

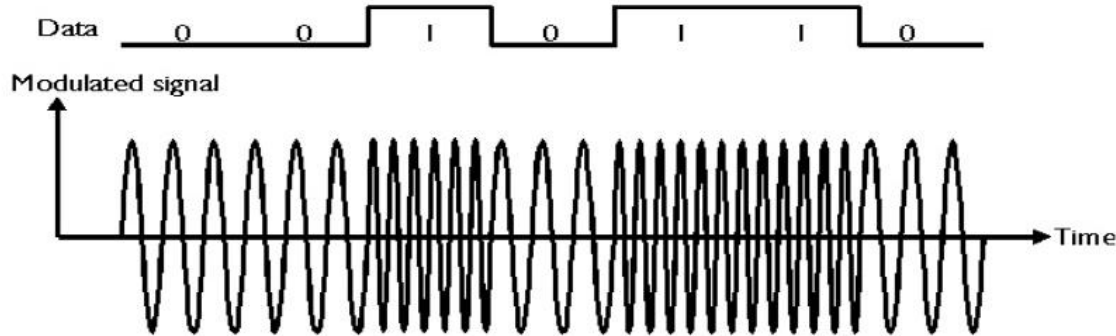
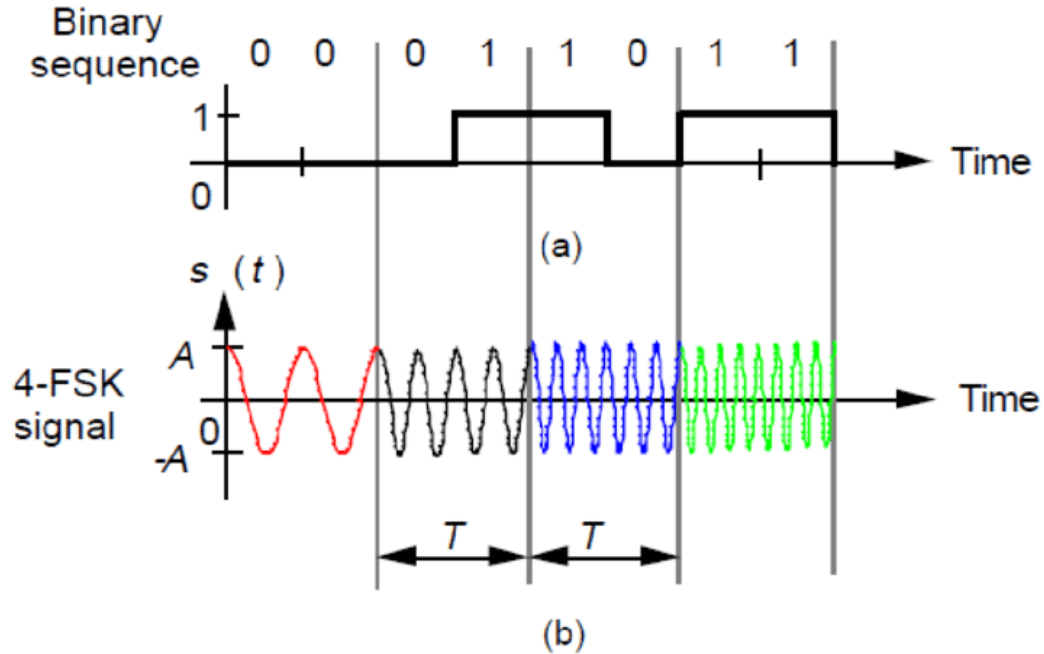


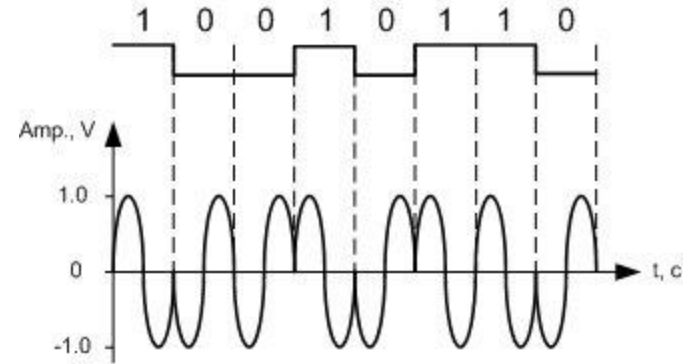
Image source: <https://www.slideshare.net/Tehnanali/digital-modulation-61719297>

Multi-FSK



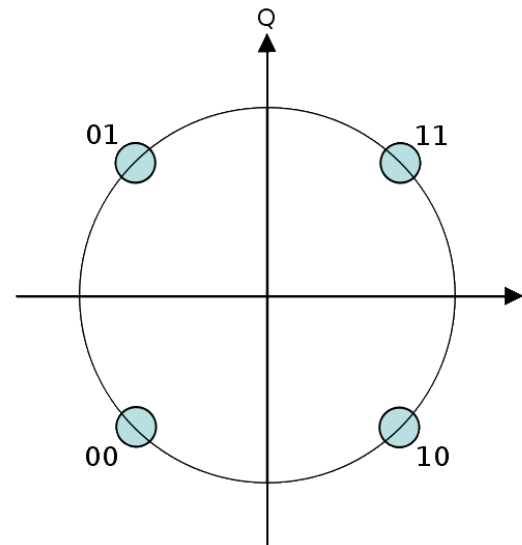
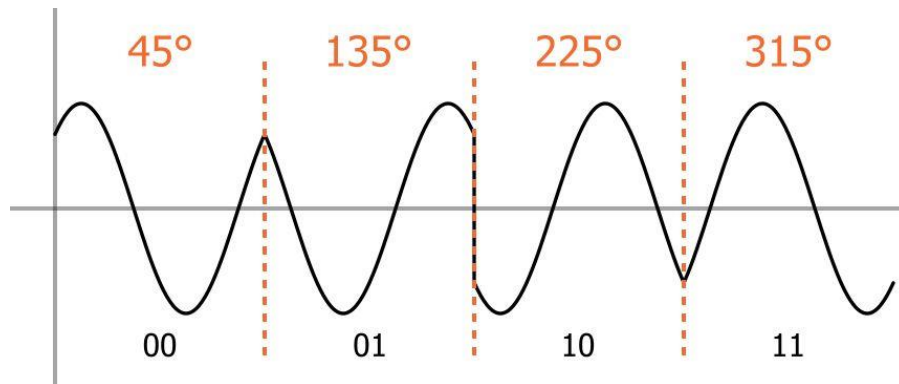
Phase Shift Keying

- Zo lang de info hetzelfde blijft blijft het signaal gelijk
- Als we tussen 1 en 0 switchen krijgen we een fasedraaiing.



Phase shift keying (PSK)

Multi-PSK



Kwadratuur (Quadrature) amplitudemodulatie

- Meer info als enkel ASK of enkel PSK

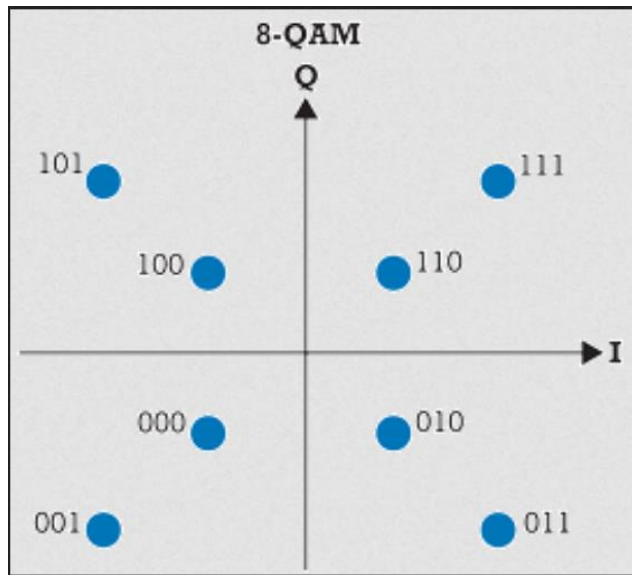


Image source: <https://dsp.stackexchange.com/questions/40991/how-to-draw-the-function-wave-to-send-symbols-using-qam>

QAM-256

•140	•132	•164	•32	•160	•147	•146	•108	•110	•106	•234	•250	•251	•235	•133	•141
•12	•4	•36	•0	•128	•151	•150	•109	•238	•42	•170	•186	•187	•171	•163	•143
•76	•20	•16	•179	•136	•135	•134	•142	•174	•43	•217	•1	•3	•139	•131	•195
•92	•28	•24	•88	•89	•113	•115	•99	•46	•47	•15	•9	•11	•138	•130	•175
•126	•60	•124	•120	•121	•241	•243	•227	•14	•30	•31	•8	•10	•152	•208	•144
•62	•61	•239	•122	•123	•55	•183	•247	•215	•26	•27	•72	•74	•184	•216	•220
•63	•199	•231	•167	•127	•119	•181	•245	•213	•68	•64	•65	•78	•223	•248	•252
•59	•51	•35	•166	•125	•117	•53	•244	•212	•84	•80	•81	•94	•95	•232	•236
•58	•50	•34	•162	•85	•21	•149	•148	•249	•116	•112	•19	•83	•87	•168	•172
•56	•54	•38	•221	•93	•5	•69	•71	•2	•6	•22	•18	•82	•210	•218	•90
•57	•185	•189	•253	•29	•13	•77	•67	•66	•70	•86	•118	•114	•211	•219	•91
•156	•157	•191	•255	•25	•153	•178	•176	•177	•49	•33	•214	•246	•155	•192	•196
•158	•159	•200	•97	•104	•190	•182	•48	•145	•17	•204	•222	•254	•240	•224	•228
•154	•233	•201	•73	•105	•188	•180	•52	•209	•197	•205	•237	•173	•242	•226	•230
•194	•202	•203	•75	•107	•40	•41	•169	•193	•225	•229	•7	•39	•103	•102	•98
•198	•206	•207	•79	•111	•44	•45	•137	•129	•161	•165	•23	•37	•101	•100	•96

Afwegingen digitale modulatie

Afstand – vermogen – bitrate – (latency)

- Bepalende factoren
- Keuzes maken
- Afstand
 - Personal area
 - Local Area
 - Wide Area

Afstand – vermogen – bitrate – (latency)

- Vermogen
 - Energiebron
 - Levensduur per lading
 - ...
- Bitrate
 - Bps
 - Kbps
 - Mbps
 - Gbps

Afstand – vermogen – bitrate – (latency)

- Latency
 - Hoe lang duurt het voor uw pakketje aankomt

Wi-Fi

- Afstand
 - +- 50m binnen
 - Afhankelijk van heel veel parameters
 - Afstanden tot ...km mogelijk met straalverbindingen
- Vermogen
 - 1W – 30dBm EIRP
- Bitrate
 - <2Gbps

LoRa(WAN)

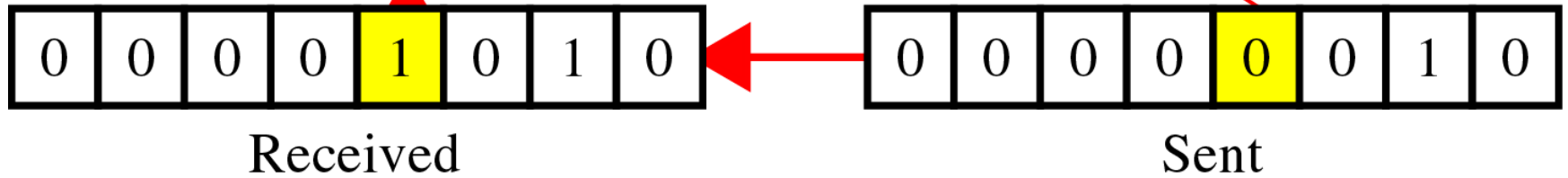
- Afstand
 - 5km
 - Record 1336km
- Vermogen
 - 25mW – 14dBm ERP
- Bitrate
 - 25 bytes duurt 2 seconden
 - Duty cycle 1%
 - 1 bericht per 3 minuten

Error detectie / correctie

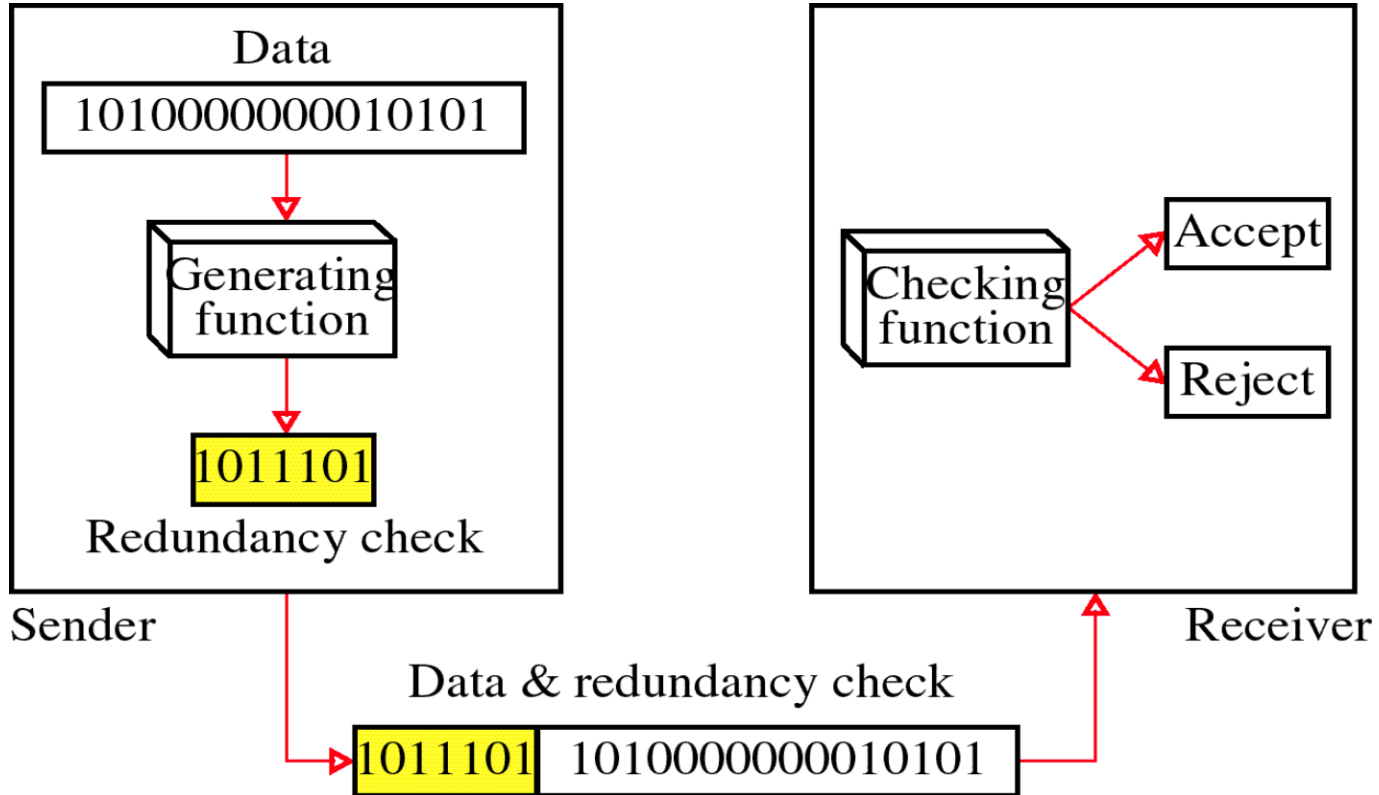
Korte introductie

Error

0 changed to 1



Redundancy Check



Error detectie en correctie

- Bij sommige methodes van error detectie kunnen we in zekere mate de gemaakte error verbeteren
- Dit is heel belangrijk bij bijvoorbeeld LoRa waar we niet om een heruitzending kunnen vragen
- Hoe meer errors we willen kunnen corrigeren hoe meer overhead

Voorbeeld van error correctie (2d pariteit)

1	0	1	0	1		1
1	1	1	1	0		0
0	1	1	1	0		1
1	0	1	0	1		0

no errors

1	0	1	0	1		1
1	0	1	1	0		0
0	1	1	1	0		1
1	0	1	0	1		0

parity
error

parity
error

LoRa

Wat is LoRa

- PHY radio protocol voor IoT
- Gebruikt Chirp Spread Spectrum
- Proprietair van Semtech
- Long Range, Low Power, Low Datarate
- Bits of kilobits per seconde
 - Hangt af van het kanaal en de modulatie



Wat is LoRaWAN

- Draadloos IoT network
 - Open Standaard
- Voegt adressering toe
- Meerdere basisstations
- Kan de datarate aanpassen
- Meerdere niveaus van encryptie
- RFC8376 - LPWAN

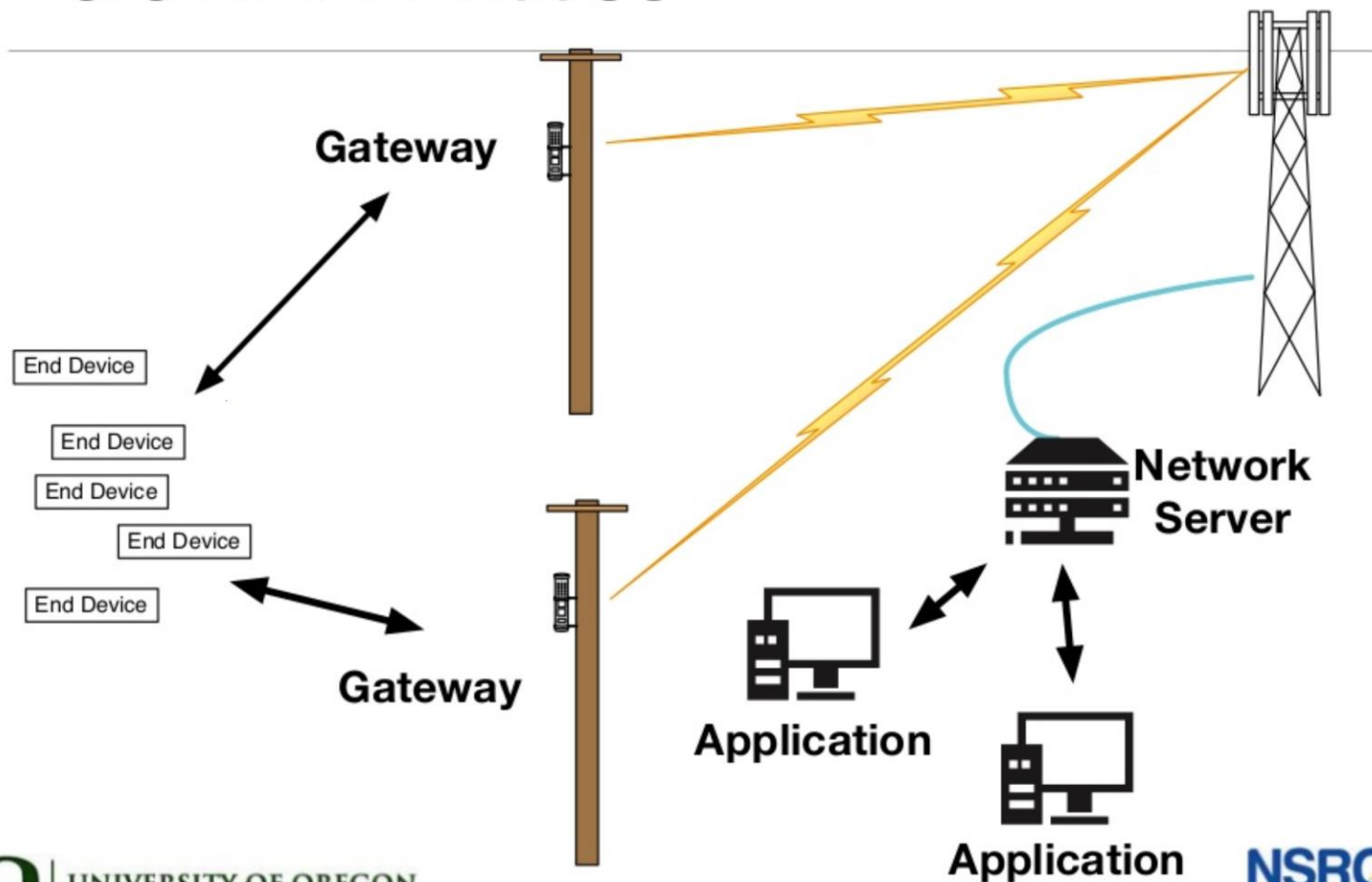


LoRaWAN België

- Belgische netwerken
 - The Things Network
 - Community driven
 - Open network
 - Commerciele netwerken
 - Proximus
 - Wireless Things
 - Helium



LoraWAN Entities



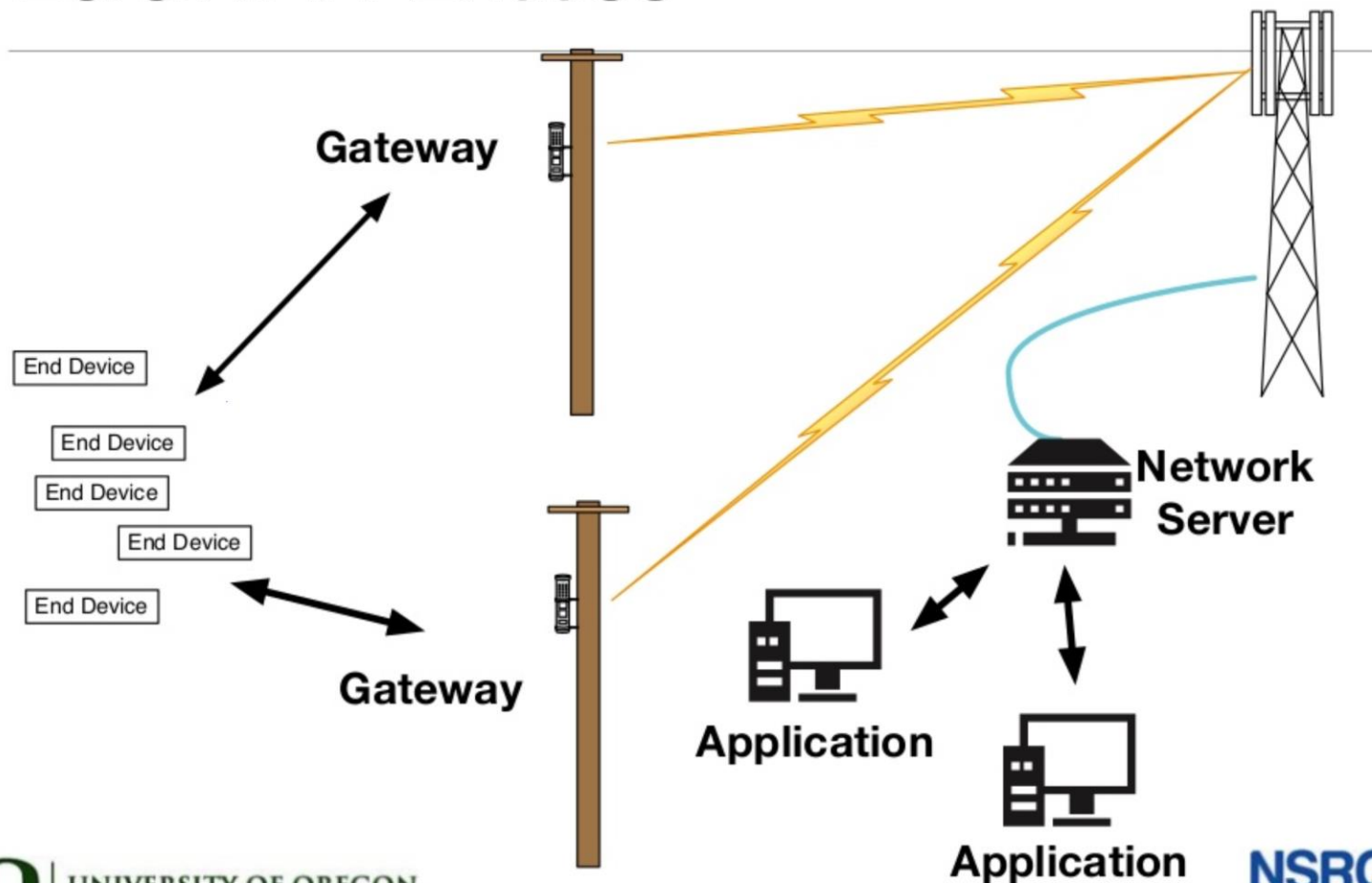
End Device

- LoRa client device, wordt soms NODE of MOTE genoemd
- (in LoRaWAN) praat met de gateways
 - Nooit met andere devices onderling
- Heeft een (globaal) uniek 64 bit EUI
 - Extended Unique Identifier (hardware adres)
- Heeft een (network) uniek 32bit deviceadres
 - Deze wordt op het netwerk gebruikt.

Device Classes

- Klasse A (laagste verbruik)
 - Communicatie wordt altijd door het eind device geïnitieerd.
 - Na zending luistert het even of de gateway berichten heeft.
- Klasse B (gemiddeld verbruik)
 - Kan zenden zoals een Klasse A device
 - Luistert op vaste tijdstippen ook voor berichten
- Klasse C (minder geschikt voor batterij)
 - Kan zenden zoals een Klasse A device
 - Luistert permanent → laagste latency, hoogste verbruik

LoraWAN Entities



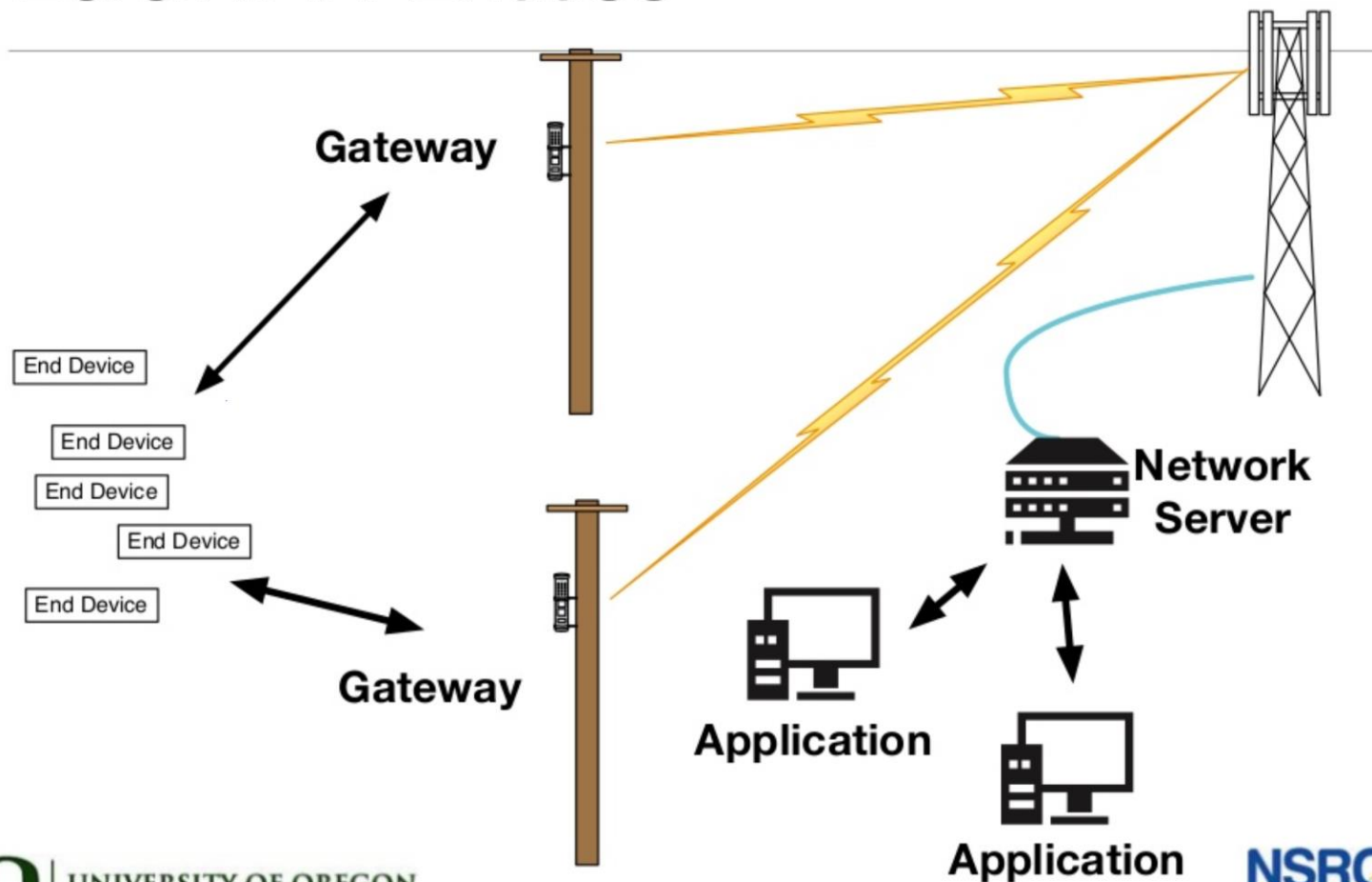
LoRaWAN gateway

- Wordt soms concentrator of base-station genoemd
- Communiceert met end-devices via LoRaWAN
- Communiceert met het netwerk via TCP/IP
- Luistert (meestal) op meerdere kanalen tegelijkertijd
- Kan ook (beperkt) zenden

LoRaWAN gateway



LoraWAN Entities



Netwerk Server

- Beheert alle communicatie van en naar de gateway
- Is het centrum van de ster topologie
- Stelt de informatie ter beschikking van de end-gebruiker door middel van een API

Uplink Berichten

- Berichten van het end-device naar het netwerk
- Kan door een of meerdere gateways worden ontvangen
- Als dit bericht door meerdere gateways wordt ontvangen is het aan de netwerkserver om de data te de-dupliceren

Downlink Berichten

- Communicatie van de netwerk server of applicatie naar de eind-devices
- Kan gericht zijn aan 1 device of aan een groep devices
- De Netwerk Server beslist welke gateway het bericht moet versturen

LoRaWAN Encryptie

- Alle berichten zijn geëncrypteerd
 - Met een Netwerk Key
 - deze is gekend door het netwerk, daarmee kan het netwerk het adres lezen
 - Deze key wordt tegenwoordig meer voor integriteit gebruikt, om te controleren of het bericht klopt, dan voor security.
 - Met een Application Key
 - Gekend door de maker van de applicatie, niet gekend door het network
 - Onze network provider weet niet wat we versturen

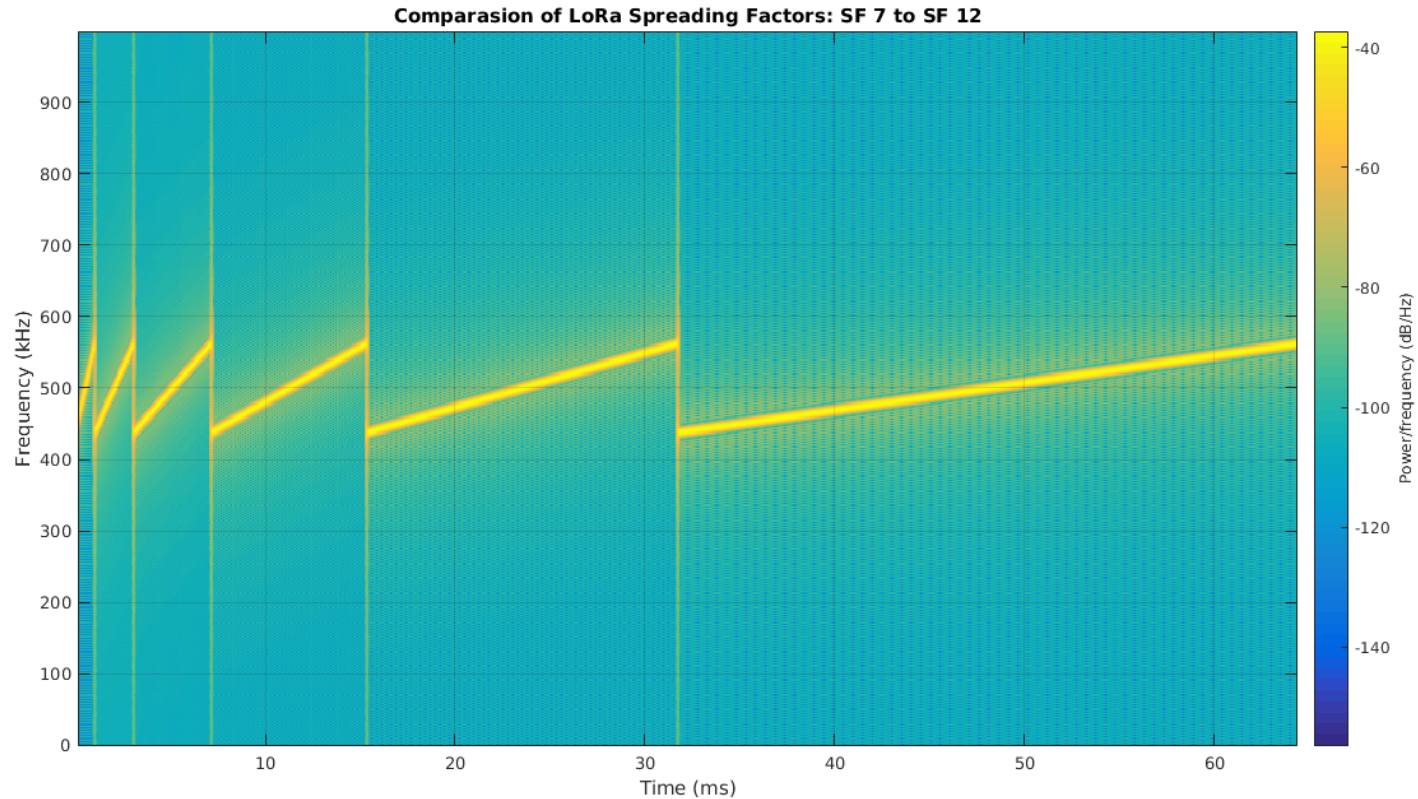
Authenticatie

- ABP - Authentication By Personalisation
 - Eind-device heeft een vaste Netwerk en Applicatie key
 - Gaat zich op basis daarvan authenticeren
- OTAA – Over The Air Authentication
 - Eind-device meldt zich aan met zijn EUI (uniek hardware adres)
 - Krijgt van de server (via de gateway) een Application en Netwerk key terug
 - Na eenmalige authenticatie werkt dit verder zoals ABP

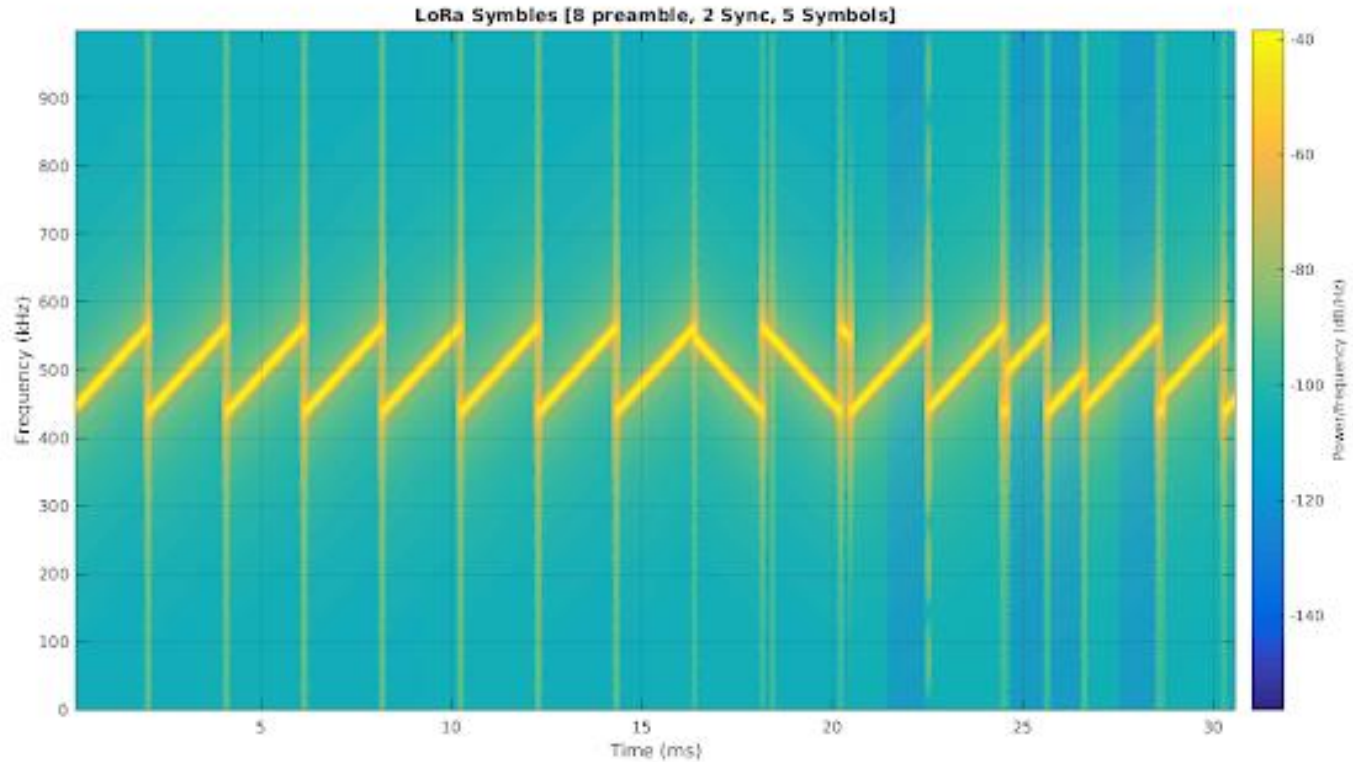
Chirp Spread Spectrum

- Modulatie die gebruikt wordt door LoRa
- 3 mogelijke bandbreedtes
 - 125KHz
 - 250KHz
 - 500KHz
- 6 verschillende Spreading Factors, die stapsgewijs de air-time vergroten
 - SF7 – SF12

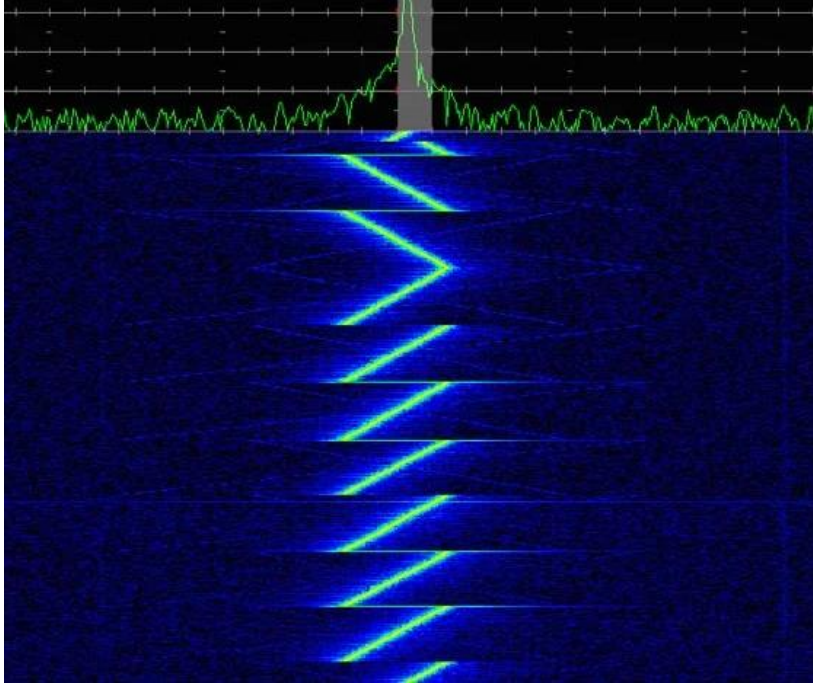
Spreading factors



LoRa bericht

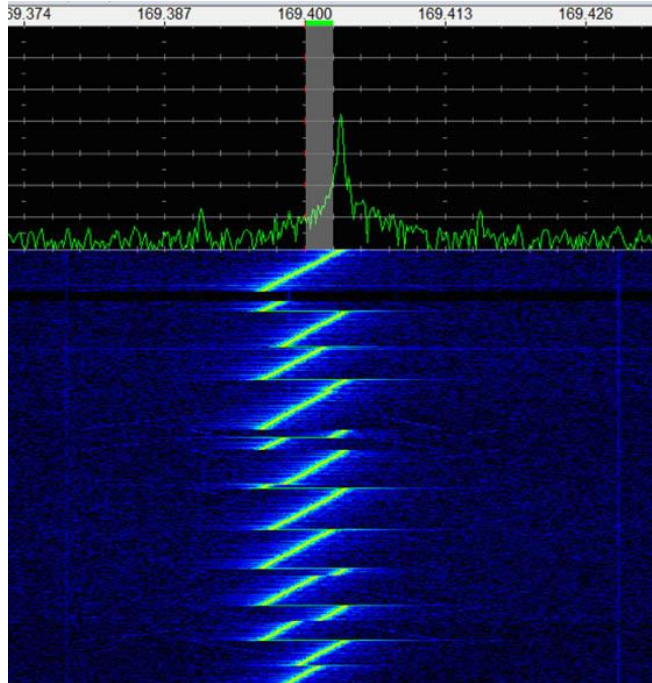


Preamble



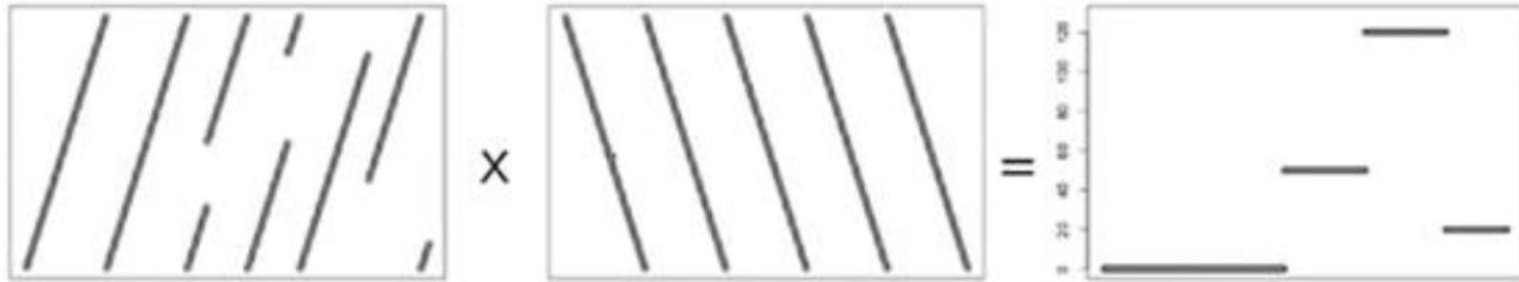
- Synchronisatie tussen zender en ontvanger
- Gaat voor aan ieder bericht

Lora bericht

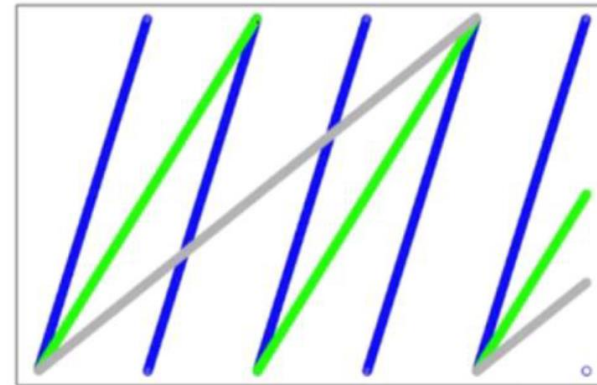


- Bericht zelf, gebruikt ook chirps

Chirp demodulation



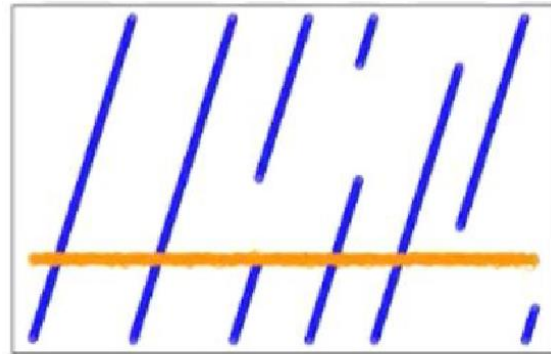
Frequency



Time

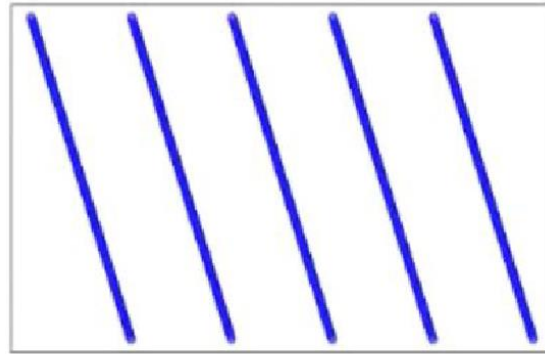
- SF7
- SF8
- SF9.

Smalbandige interferentie



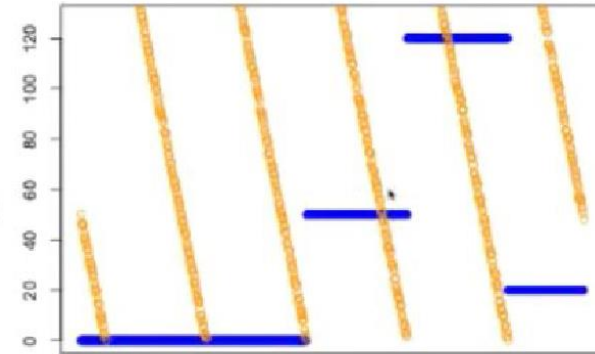
Received Lora signal
Narrowband interferer

$\times$



Inverse chirp

$=$

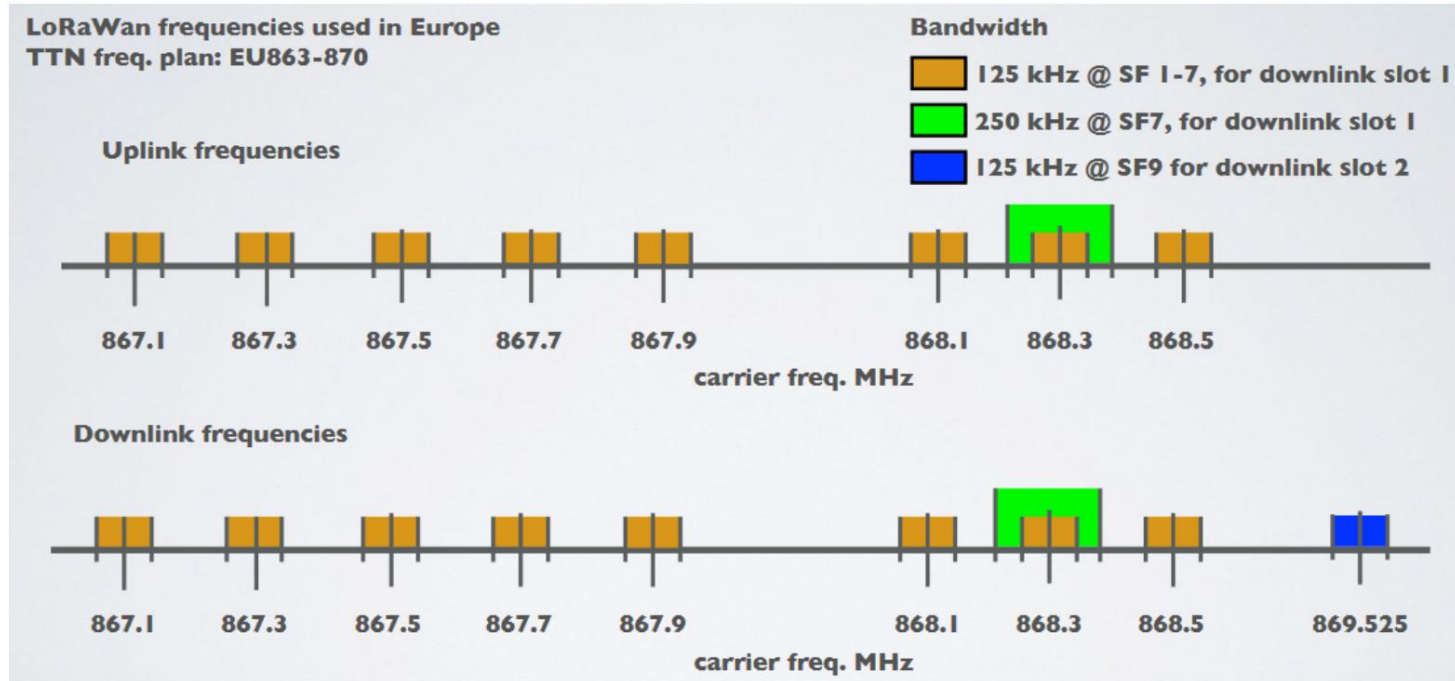


Decoded symbols

Voordelen chrip

- Zeer breedbandig, niet gevoelig voor smalbandige storing
- Berichten met verschillende SF kunnen op dezelfde frequentie gelijktijdig worden ontvangen
- Chrip is minder gevoelig voor multi-path propagatie

Frequenties The Things Network



Frequenties

- 868.1, 868.3 en 868.5 moeten volgens de standard door ieder netwerk worden ondersteund
- De andere frequenties zijn vrij te kiezen door het network
- Iedere keer we een pakket verzenden gebruiken we een andere frequentie

Wetgeving

Name	Band (MHz)	Limitations
G	863.0 – 868.0	EIRP<25 mW – duty cycle < 1%
G1	868.0 – 868.6	EIRP<25 mW – duty cycle < 1%
G2	868.7 – 869.2	EIRP<25 mW – duty cycle < 0.1%
G3	869.4 – 869.65	EIRP<500 mW – duty cycle < 10%
G4	869.7 – 870.0	EIRP<25 mW – duty cycle < 1%

Bluetooth

Bluetooth classic



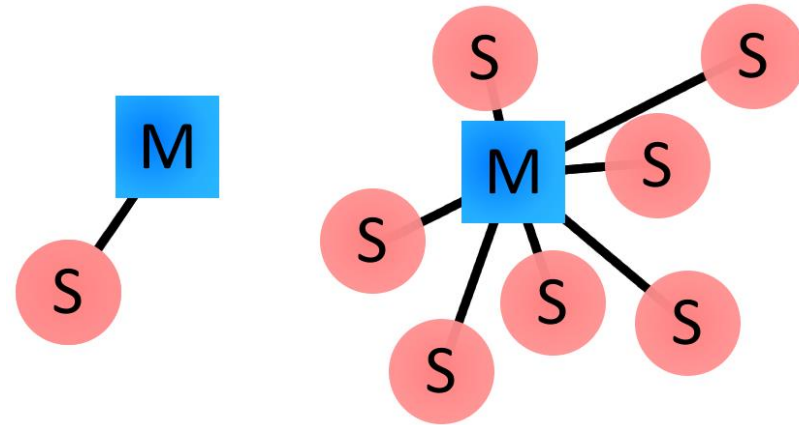
- Ontwikkeld in 1989 door Ericsson
- 2,4GHz
- Afstand 1-100m
- Connection-oriented: audio, netwerk, bestandsoverdracht
- Datarate 2.1Mbps
- Gemaakt om kabels te vervangen (netwerk kabel, usb kabel, ...)

Van waar komt de naam?

- Van de Deense koning “**Harald Bluetooth**” die in de 10e eeuw vele verschillende Deense stammen in een enkel koninkrijk heeft verenigd.
- Bluetooth kreeg deze naam omdat
 - Ontwikkeld in scandinavië (Ericsson, Sweden)
 - Het was een tijdelijke werknaam
 - Bluetooth bedoeld is om verschillende industrieën te verenigen, zoals gsm, computer, automotive, ...

Bluetooth classic

- Bluetooth classic werkt voornamelijk master-slave
- Master = bijvoorbeeld laptop, smartphone
- Deze kan meerdere slaves hebben
 - Muis
 - Headphone
 - Keyboard
 - ...
- Permanente verbinding
- Slave praat enkel en alleen met 1 master, niet onderling
- Iedere master kan 7 actieve slaves hebben



Bluetooth classic Pairing

- Je scant met je device voor zichtbare Bluetooth devices
 - Het kan zijn dat je zichtbaarheid moet aanzetten
 - Of het device in pairing-mode moet zetten
- Je device stuurt zijn MAC adres door naar het device waar je mee wil verbinden
- Er wordt (eventueel) een authenticatie gedaan, doormiddel van pin code
- Vanaf dat de devices elkaars MAC-address kennen kunnen ze verbinding maken.

Bluetooth classic power classes

Class Number	Max Output Power (dBm)	Max Output Power (mW)	Max Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	10 cm

Bluetooth (classic) profielen

- Profielen zijn voorafgesproken protocollen voor bepaalde doeleinden.
- Ze spreken af hoe bepaalde communicatie moet verlopen voor verschillende communicatietypes
- Om devices met elkaar te kunnen laten spreken moeten ze dezelfde profielen ondersteunen.
- Dit is ook hoe een smartphone weet welke diensten een apparaat ondersteund, en daarvoor het juiste icoontje kan weergeven.

Een device kan meerdere profielen ondersteunen.

Bluetooth (classic) profielen voorbeelden

- Serial Port Profile (SPP):
 - Hiermee kunnen we Bluetooth gebruiken voor Seriële dataoverdracht, alsof we een RS232 verbinding hebben.
 - Dit is een van de eerste toepassingen van Bluetooth ooit geweest.
- Human interface device (HID)
 - Toetsenbord, muis, joystick, ...

Bluetooth (classic) profielen voorbeelden

- Headset Profile (HSP)
 - Bluetooth oortje om mee te telefoneren
- Hands-Free Profile (HFP)
 - Zelfde functionaliteit als HSP
 - Extra functionaliteit zoals een call opzetten, contactenlijst bekijken, ...
 - Gebruikt bij hands-free sets in auto's.

- Advanced Audio Distribution Profile (A2DP)
 - Gebruikt om muziek door te sturen
 - 1 richting per verbinding
 - Maar kan wel luidspreker of micro zijn
 - Betere kwaliteit dan Headset Profile
- A/V Remote Control Profile (AVRCP)
 - Gebruikt om muziek te sturen, play, pauze, next, ...
 - Gebruikt icm met A2DP

Bluetooth low energy

- Geïntroduceerd in Bluetooth 4.0 (2010)
- Applicaties
 - Sensors op batterijen zoals hartslag, fitness, ...
 - Locatie tracking, iBeacon
- Doel
 - Low power
 - Low cost
 - Low bandwidth (100kbps)
- Hoe
 - Radio meestal uitgeschakeld
 - Kleine pakketjes
- Hoeft geen verbinding te hebben, kan ook broadcasts sturen

Bluetooth classic vs BLE voorbeeld

Protag G1

- Bluetooth 2.0
- 270mAh 3,7V
- Battery life: 7-14 dagen

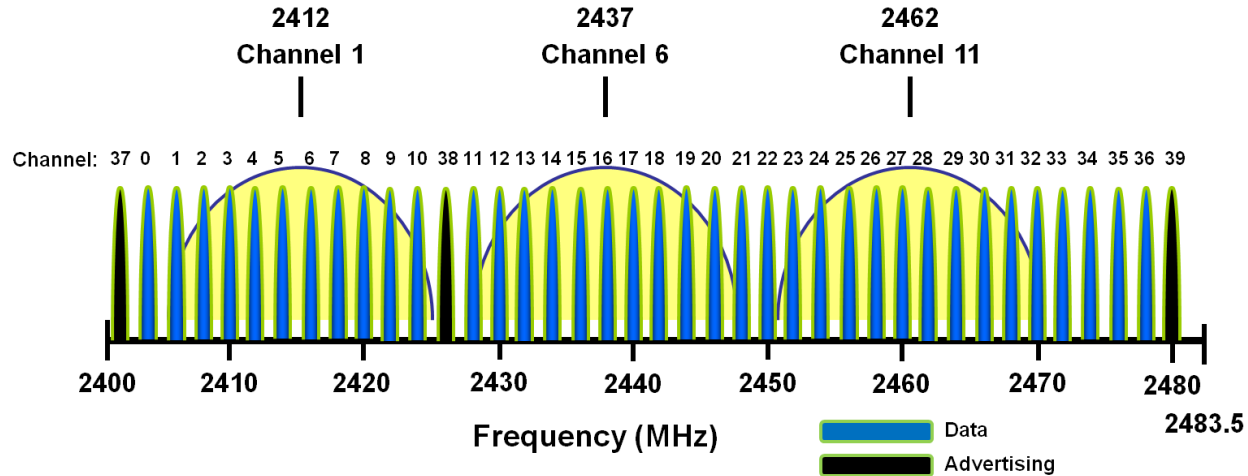
Protag Elite

- Bluetooth Low Energy
- 150mAh 3,7V
- Battery life: 6-12 maanden



BLE Frequency Usage

2.4 GHz PHY Channel Assignment Bluetooth® Low Energy vs. IEEE 802.11 (United States)

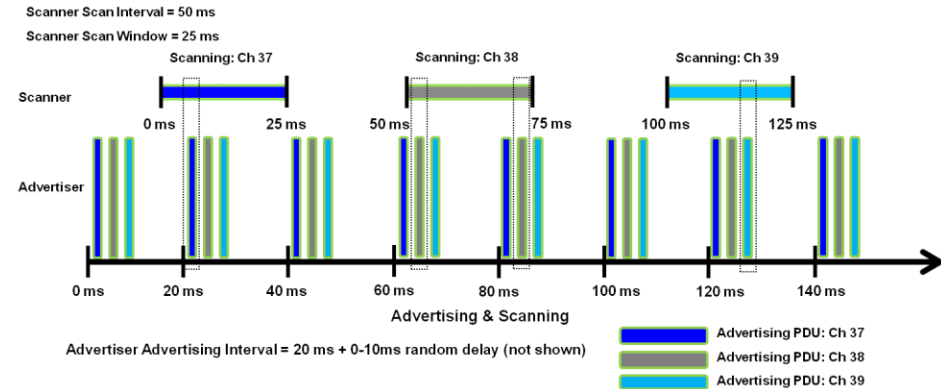


kanalen

- Advertising kanalen
 - Gebruikt om devices te vinden
 - Gebruikt voor broadcasts
 - Gebruikt om verbindingen op te zetten
 - Deze kanalen gebruiken frequenties die buiten de klassieke 2.4GHz wifi-frequenties vallen.
- Data kanalen
 - 2-richtingscommunicatie tussen verbonden devices

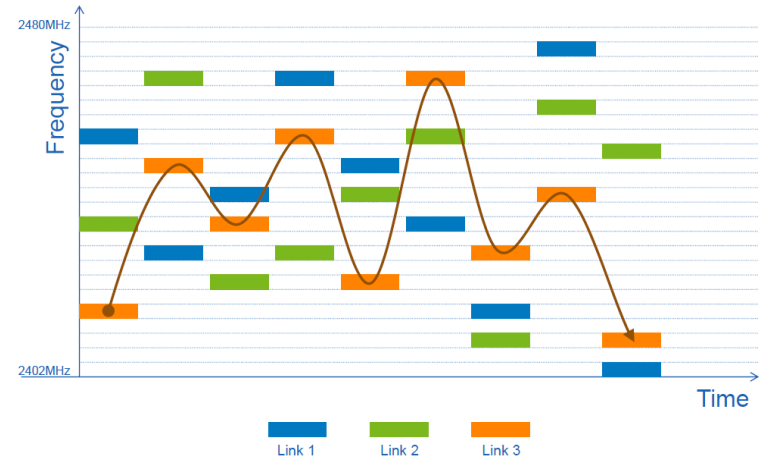
Scanner / Advertiser

- Scanner devices luisteren op gedefinieerde scanner intervals een voor een op de verschillende kanalen
- Advertiser devices zenden op de 3 kanalen met een gedefinieerde interval time, met een random tijd offset.
- Communicatie is succesvol als de scanner op het juiste kanaal luistert wanneer de advertiser zendt.
- Deze intervals kunnen door de applicatie gekozen worden.



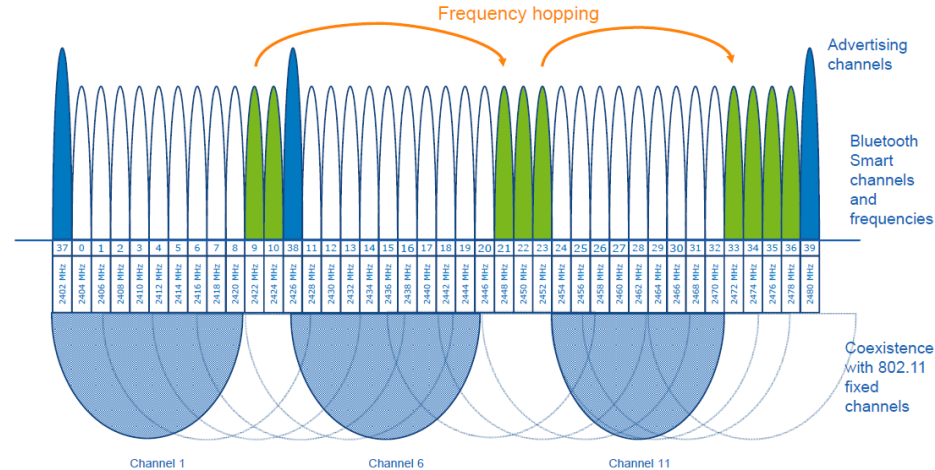
Frequency Hopping (bij data kanalen)

- Ieder pakketje wordt op een ander kanaal gestuurd, om storingen te beperken
- Het gebruikte hopping patroon wordt vooraf afgesproken via een advertising kanaal.



Adaptive Frequency Hopping

- We sluiten kanalen met veel storingen uit van ons hopping patroon
- Deze storende kanalen stellen we dynamisch vast
- We gebruiken alleen de goede kanalen om tussen te hoppen.

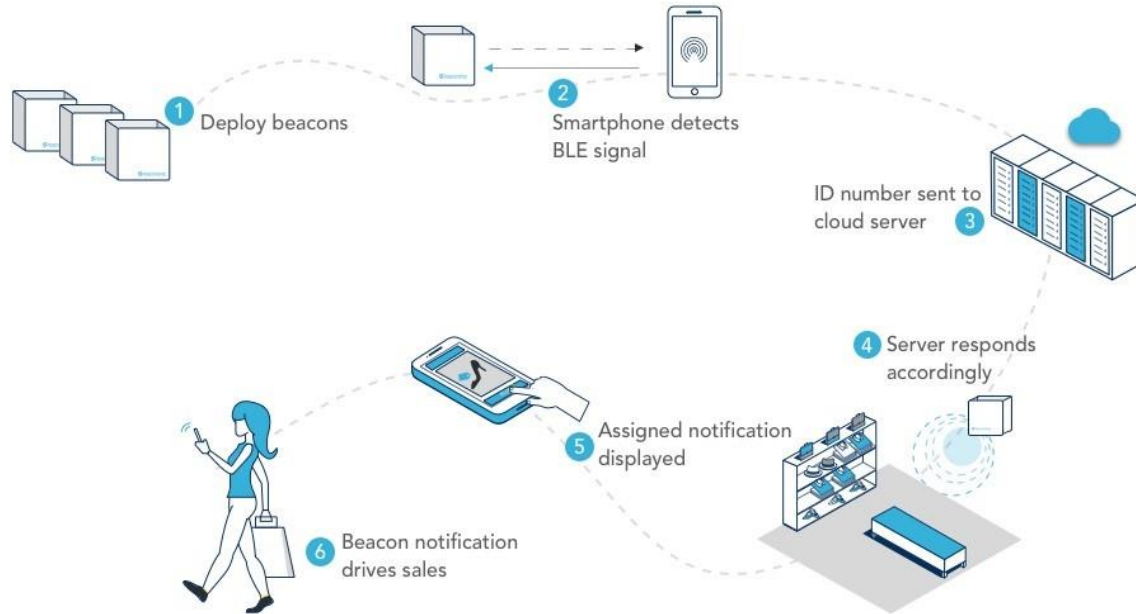




iBeacon

- Ontwikkeld door Apple in 2013
- Ook door andere leveranciers onder de naam BLE beacon
- Stuurt een identifier uit naar apparaten in de omgeving
- Hierdoor kunnen we bijvoorbeeld indoor plaatsbepaling doen.
- iBeacon met 100ms interval 1-3 maanden op knoopcel
- 2-3 jaar bij een beacon interval van 900ms.

iBeacon



BLE Beacon use cases

- WAZE GPS in tunnels
 - <https://www.youtube.com/watch?v=Hr90jJ-0WbU>
 - Beacons kosten €25 / stuk
 - Om de 40m een baken
- Carrefour doet een test in Roemenië waar ze met hun app push-notificaties sturen naar klanten afhankelijk van waar ze zich in de winkel bevinden.



BLE USECASE Coronalert

- Gebruikt om contacten te traceren om bij risicocontact in quarantaine te kunnen gaan
- Gebruikt een Europese open standard Decentralized Privacy-Preserving Proximity Tracing, afgekort DP-3T of dp³t.
- Standaard gebruikt BLE om interacties tussen gebruikers te kunnen loggen.

Dp^{3t}

- Ephemeral ID (vertaald: vluchtige / kortstondige ID)
 - ID die wordt uitgewisseld om contacten te traceren
 - Bestaat uit een hash van een (random) Secret Key (SK) die dagelijks wordt vernieuwd, gecombineerd met een tijdsindicatie, die om de paar minuten verandert waardoor we maar een beperkte tijd dezelfde key uitzenden.
 - Omdat we SK niet kennen van andere devices, lijkt deze data random, en kunnen we de key van enkele minuten geleden niet koppelen aan de nieuwe key.

Dp³t: handshake

- Smartphones wisselen regelmatig (met random intervals) af tussen de scanner en de advertiser rol.
- De advertiser stuurt zijn (Ephemeral) ID heel de tijd door
- Als de scanner een nieuwe ID opvangt, stuurt deze een antwoord naar de Advertiser met zijn ID.
- Client en server loggen dan de ID, samen met een (ruwe) timestamp en signaalsterkte.
 - Die worden gebruikt om afstand en tijd te bepalen.

Dp³t: besmetting rapporteren

- Als we positief getest zijn krijgen we een code die we moeten ingeven in onze Coronalert app.
- Die code geeft ook aan vanaf hoeveel dagen geleden contacten moeten worden verwittigd.
- De gebruiker stuurt zijn Secret Keys door van de dagen die moeten worden gerapporteerd.
- Gebruikers krijgen op geregelde tijdstippen een lijst door van besmette SK's, en kunnen op basis daarvan alle verstuurde ID's gaan berekenen, en vergelijken met hun lokale database.

Dp³t: conclusies

- De app van de eindgebruiker download zelf de lijst met Secret Keys van een centrale server.
- De app gaat dan lokaal de mogelijke ID's genereren op basis van de SK, en deze vergelijken met alle ID's in de database.
- Op basis van het aantal ID's dat overeenkomt en de signaalsterkte kan gekeken worden of het om een hoog of om een laag risico contact gaat.
- Alles gebeurt client-side, de overheid weet niet waar je geweest bent / weet zelfs niet dat je een risicocontact had.
- Bekijk / analyseer zelf je data: <https://covid.aaltra.eu/nl/>