IEEE 802.15.4 ZigBee

H4 – MOBILE OG TRÅDLØSE SYSTEMER

Michael Nyman Schmidt, Thomas Fisker Andersen, Jimmi Hansen og Thomas Agerbo Kaanbjerg

AUGUST 2017

Indhold

Hvad er ZigBee

ZigBee er en trådløs teknologi protokol, som kan benyttes I mange forskellige produkter og enheder. Det kan for eksempel findes i røgalarmer, stikkontakter, belysning eller sensorer hjemmet/virksomheden. Disse produkter vil tilsammen udgøre et lokalt personligt netværk også kaldet PAN (Personal Area Network), hvor alle enheder vil være i stand til kommunikere med hinanden. Det gør at man er i stand til at kontrollere og overvåge alle enhederne fra et og samme sted. ZigBee har mange forskellige applikations profiler, som kan benyttes I forskellige situationer, vi har dog valgt af fokusere på "Smart Home", som kræver en Coordinator enhed som hjernen af netværket.

Ved hjælp af en gateway, som for eksempel "SmartThings" fra Samsung, kan du få dine enheder på internettet og tilgå remote.

Muligheder

Der er to indgangsvinkler til IOT.

1. Enheder vi kender i dag, såsom trådløs overvågningskamera, printer og TV, der er koblet direkte op på en router enten over Wi-Fi eller kobber kabel.

2. En type smartenhed der kan snakke eks. ZigBee og kommer ud på LAN via en hub.

Mulighed 2 dækker over en lang række protokoller hvoraf ZigBee er en af de største, tæt efterfulgt af Z-wave. Ofte kan dette godt sammensættes og styres af en hub, hvis den understøtter protokollen, de forskellige protokoller kan dog ikke snakke sammen.

Kompatibilitet

ZigBee er som en åben protokol blevet valgt af flere udviklere og markeder.

Her en liste over hvad ZigBee for eksempel kan sættes op med:

- Phillips Hue
- Samsung Smart Things
- Google Home
- Amazone/ Alexa
- Microsoft /cortana
- M,M.

Et udvalg af firmaer der laver Zigbee kompatible produkter er:

Huawei, Philips, Schneider, SmartThings, ARM, Belkin, Danfoss, Ikea, Intel, Samsung, Simens Velux, D-link og mange andre.

Link til fuld liste - http://www.zigbee.org/zigbeealliance/our-members/

Foruden kompatibilitet med ZigBee, kommer man ikke uden om alternativet Z-wave, som minder meget om ZigBee. Nogen af de væsentlige forskelle er overførselshastigheden som på Z-wave er meget lavere, men til gængæld har den en højere rækkevidde.

Hvis man stod i en situation, hvor man ville i gang med selv at sammensætte sig et smarthome, kan man godt blande de to protokoller med en hub, som for eksempel "SmartThings" fra Samsung, der understøtter begge platforme.

Netværks standard

ZigBee benytter standarden IEEE 802.15.4, som er en af-art af IEEE 802.15 Trådløs PAN (Personal Area Network). Første udgave af 802.15.4, blev frigjort tilbage i 2003, efterfølgende er der løbende blevet frigivet opdaterede versioner af 802.15.4.

Frequency	Europe 868 MHz, 1 channel	Americas 915 MHz, 10 channels	Worldwide 2.4 GHz, 16 channels
Data Rate	20kbps ... 100kbps	40kbps ... 250kbps	250kbps

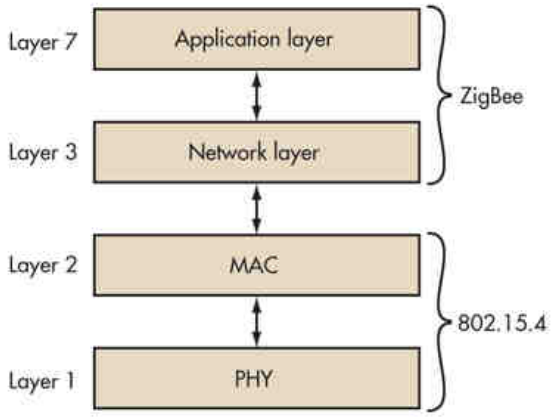
802.15.4 er designet til lavhastighedskommunikation, maksimum data rate er 250 kbps.

Tabellen herunder viser hvilke ISM (Industrial, Scientific, and Medical Band) frekvensbånd 802.15.4 kan arbejde i.

Derudover er protokollen designet til at bruge så lidt strøm så muligt og har en meget lang batterilevetid, op til 5-7 år oplyses flere steder.

802.15.4 arbejder på de to første lag i OSI modellen, dvs. det Fysiske og Data Link laget.

ZigBee arbejder på Netværkslaget og Applikationslaget.



802.15.4 bruger 4 typer af frame pakker Data, ACK, MAC command og beacon.

802.15.4 har en trådløs rækkevidde på 10 - 30 meter indendørs og 100 - 150 meter udendørs. Hvis du forstærker signalet, kan du opnå en udendørs rækkevidde på 540 meter.

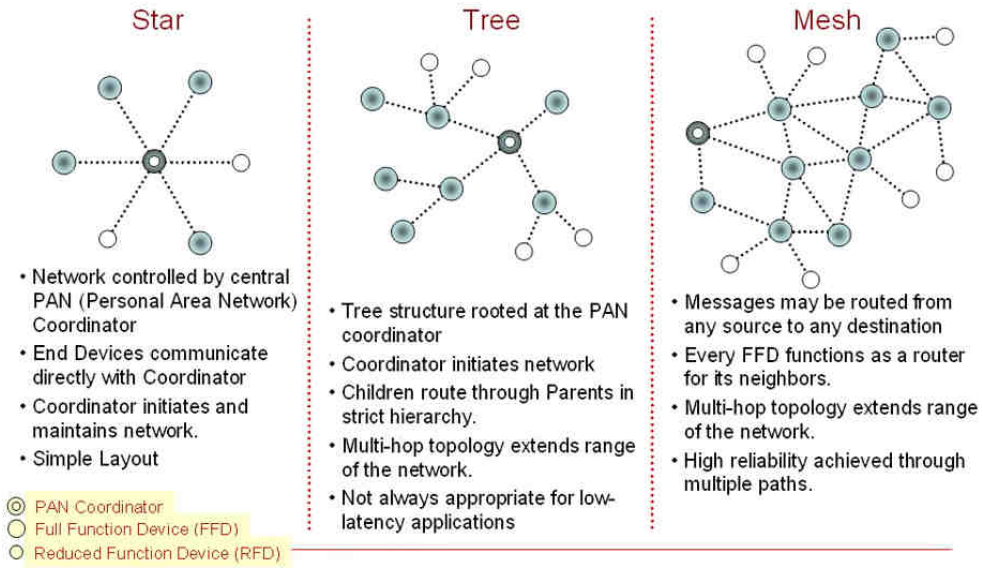
802.15.4 benytter sig af CSMA-CA (Carrier-sense multiple access with collision avoidance), da der kan være mange PAN netværk I området. Så hver gang ZigBee produkter har noget at sende, mærker de efter om der er ledigt I luften. Hvis ikke, venter de et tilfældigt antal millisekunder og forsøger igen, på den måde undgår de at de alle forsøger at sende samtidig.

ZigBee Architecture

ZigBee protokollen i større omfang fungerer som et Mesh netværk og hvert produkt har forbindelse til hinanden.

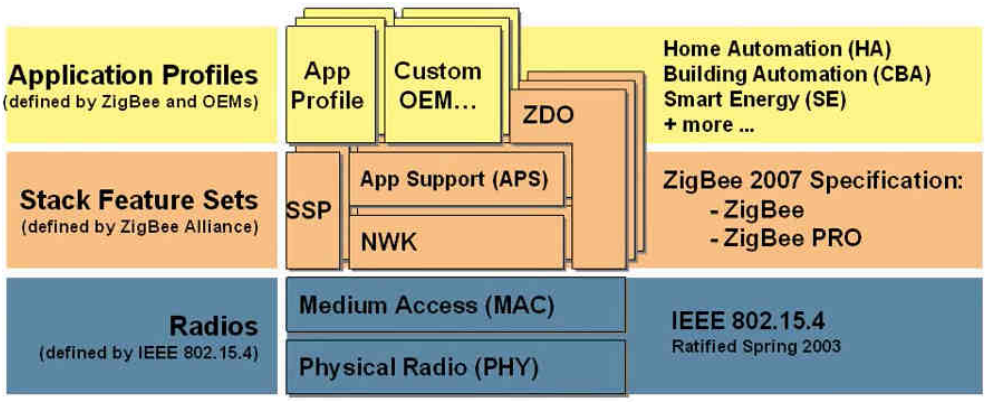
I et ZigBee Mesh netværk er det ikke alle produkter der kan route trafikken videre, dette er forbeholdt produkter med en pålidelig strømkilde så som pære, strømudtag, el-persienner osv. også kaldet ZigBee Router enheder (ZR). Dette gør at jo flere enheder du har I dit Mesh netværk, jo mere stabilt bliver det ved at eliminere single point of failure.

Network Topologies



I ZigBee systemarkitekturen starter vi ud med de nederste lag, Pyhsical Radio (PHY) relaterer sig til radiosignalerne og hvordan de agerer i luften og Medium Access Control (MAC) som hvert eneste netværkskort bruger til at identificere sig med. Disse er styret af IEEE 802.15.4 standarden og er med til at sørge for, at ZigBee kan eksistere sammen med de andre IEEE 802 protokoller.

ZigBee System Architecture



Det næste lag er kaldet Stack Feature Sets, det er hovedsageligt netværkslaget agering, som er defineret af ZigBee Alliance, beskrevet I ZigBee 2007 Specification: ZigBee eller ZigBee PRO.

Det sidste lag omhandler Applikations Profiler, disse er defineret af forskellige arbejdsgrupper indenfor ZigBee Alliance, som kan bestå af OEM og leverandører, som har ekspertise inden for området. Hovedsageligt hvordan applikationerne skal skrues sammen, som for eksempel benytter IKEA med deres nye trådløs produkt serie sig af Light link, som helt eliminerer behovet for en Coordinator enhed, dog er muligheden der stadig.

Node typer, PAN IDs, og adresser

Der findes tre forskellige nodes I et ZigBee netværk som kan se på billedet nedenunder.

ZigBee Concepts: Node Types

ZigBee Type	Notes
ZigBee Coordinator (ZC)	Special router that forms the network; only 1 per PAN
ZigBee Router (ZR)	No duty cycling available
ZigBee End Device (ZED)	Does not participate in routing; may be sleepy; requires ZC/ZR "parent" for network participation

Et hvert ZigBee "Smart Home" netværk starter ud med en Coordinator enhed (ZC), det er denne enhed, den første router enhed (ZR) skal tage kontakt til, for at forbinde til netværket. Efterfølgende kan andre enheder forbinde via Coordinatoren eller en anden router enhed (ZR), ikke et End Device, da de ikke router trafik. Coordinatoren kan sammenlignes med en router på et LAN netværk. Den sørger for at route trafik mellem alle enhederne på PAN netværket, i samarbejde med de andre enheder, som også er I stand til at route. Det er også dens opgave at uddele adresser til de enheder på netværket, at bestemme hvilket PAN ID netværket skal have samt at vælge hvilken kanal netværket skal køre på, fra 11-26.

PAN ID er en 16 bit adresse og bliver tilfældigt genereret. Denne adresse bliver delt mellem alle nodes på netværket, på denne måde er de i stand til at sortere pakker fra, som kommer fra et andet netværk og derved ikke bruge kræfter på dem.

I tilfælde af at der kommer en anden Coordinator enhed indenfor rækkevidde med samme 16 bit adresse, vil Coordinatoren benytte sig af extended PAN ID på 64 bit. Denne adresse er også kendt af alle enhederne på netværket, dog bliver den ikke brugt og kun oplyst under tilslutning. Coordinatoren tildeler så en ny 16 bit adresse til netværket. Extended PAN ID bliver også brugt under en Active Scan, hvor enheder uden for netværket undersøger hvilke netværk der er tilgængelige.

Router enheder (ZR) i et ZigBee netværk, er enheder der som regel har en altid tilgængelig forsyning af strøm, så som en LED. Da det at route trafik forud sager højere strømforbrug. Det er også enheder som altid er aktive, uanset deres funktion, for eksempel kan en LED både være tændt og slukket samtidig med at den er aktiv på netværket.

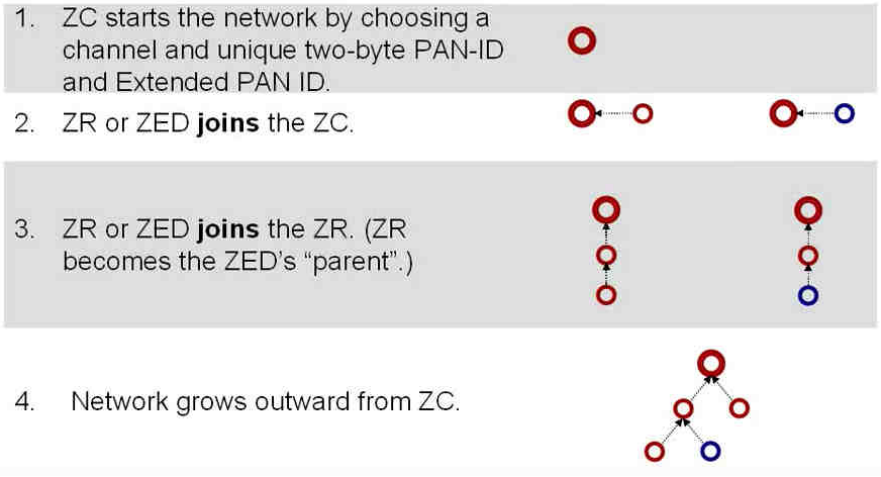
Et End Device (ZED) er den sidste form for enhed på et ZigBee netværk, den kan bruge batteri og er beregnet til at bruge så lidt strøm så muligt, den router derfor ikke trafik og har ofte en sleep funktion, det kan for eksempel bare være en stikkontakt som ved aktivering sender et signal ud til den enhed den skal tænde, samtidig spørger den på netværket efter ændringer, derefter går den tilbage I sleep tilstand. End Devices kan sågar også køre helt uden batteri og kun bruge kinetisk energi, som beskrevet i strømforbrug sektionen.

Der findes flere enheder af End Device typen, for eksempel Mobil End Device, denne holder ikke forbindelse til det øvrige netværk særlig lang tid, det såkaldte parent forholdt et End Device typisk vil oprette med en Router enhed.

Netværks aktivitet

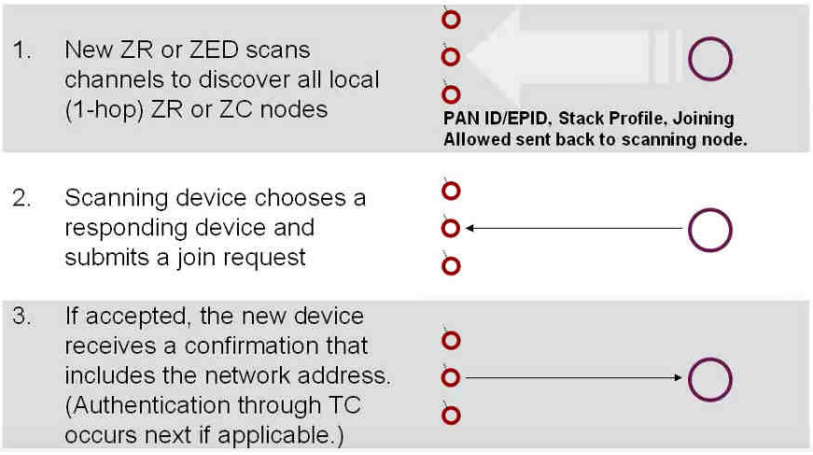
Når et ZigBee Home Automation netværk skal oprettes for første gang, starter man ud med en Coordinator enhed. Den vælger hvilken kanal, PAN ID (16-bit) og EPAN ID (64-bit) netværket skal bruge. Når den næste enhed skal tilsluttes netværket skal enheder igangsætte en Active Scan for at finde de tilgængelige netværk. Denne beacon forespørgsel lytter ZigBee Coordinatoren (ZC) efter og sender svar tilbage med PAN ID og EPAN ID, er den nylig tilsluttede enhed en Router, begynder denne nu også at lytte efter beacons fra nye enheder, som endnu ikke er på netværket. Det er kun End Devices som ikke kan tilføje nye enheder til netværket, da disse ikke router trafik.

Creating Network



Som nævnt, når en ny enhed skal tilsluttes et netværk igangsætter den en Active Scan Beacon Request. Denne request lytter alle ZigBee Coordinatorer (ZC) og ZigBee Routers (ZR) inden for rækkevidde til og svarer på med PAN ID og EPAN ID og deres Stack Profile, altså om det er ZigBee eller ZigBee PRO. De sender også tilbage om de har tilladelse til at tilføje flere enheder til netværket. Enheder der gerne vil tilsluttes vælger derefter den (ZC) eller (ZR) med bedst forbindelse og sender en Join Request. Hvis den bliver accepteret, får den en bekræftelse tilbage med netværks informationer og en tilfældig adresse.

Joining a Network



Enheder har ofte NON VOLITARY RAM, hvilket betyder at de husker deres netværk og adresser. Det vil sige at opstår der strøm afbrydelser, vil dit ZigBee netværk hurtigt være oppe igen.

Sikkerhed

ZigBee security er baseret på symmetriske nøgler, der benytter en AES 128 bit kryptering. ZigBee kan både kryptere og godkende data pakker på MAC, NWK og Applikations niveau.

ZigBee bruger udtrykket "Trust Center" om en enhed der:

- Opbevarer nøgler til netværket
- Uddeler nøgler til nye enheder
- Godkender nye enheder til netværket

Er der en ZigBee Coordinator (ZC) på netværket fungerer denne som "Trust Center".

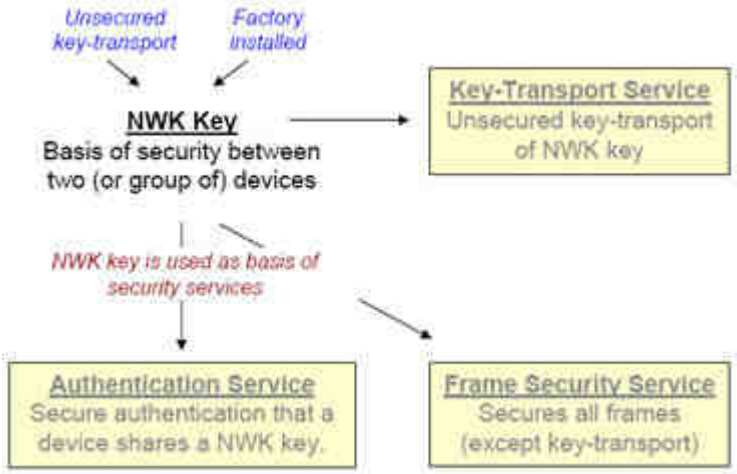
Der er 3 typer nøgler:

- Master Key
  - Bruges ikke til at kryptere frames, men bruges som de første "shared secret" imellem enheder, når de skal blive enige om Link Keys - også kaldet "Key Establishement Procedure (SKKE)"
    Nøgler, der kommer fra Trust centeret (Coordinator) bliver kaldt Trust Center Master Keys - alle andre kaldes Application Layer Master Keys.
- Link Key
  - En unik nøgle, som deles mellem 2 enheder for at beskytte frames på APS laget. Én af disse enheder er normalt "The Trust Center".
- Network Key
  - En global nøgle, som bruges på alle enheder i netværket.

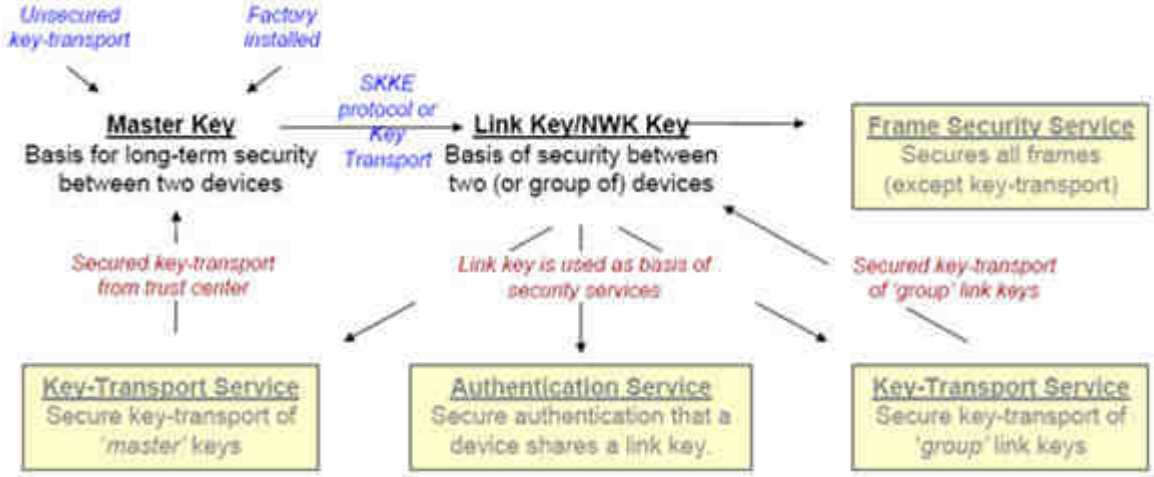
Der er ydermere indbygget anti-replay authentication, i form af en frame-counter, der i teorien gør gentagelse af f.eks. funktionen, der bliver kaldt, når en dør skal åbnes eller lignende.

Nedstående illustrationer viser hvordan udveksling af nøgler foregår, ved både standard security og i high security (ZigBee Pro).

Standard Security



High Security – (ZigBee Pro)



Fælles Sprog

DotDot

Et fælles sprog som er designet til at blive brugt i IOT enheder. Dette er som sådan ikke et programmeringssprog, men et kommando sprog.

Det er blevet designet på baggrund af den fart ZigBee har haft på markedet og er derfor baseret derpå. Den er blevet lavet i samarbejde med ZigBee Alliancen og er en open source standard.

Green Power

Strøm forbrug

De fleste produkter som benytter ZigBee teknologien kan holde strøm I op til 5-7 år. Det lave strømforbrug begrænser derfor også afstanden hvert produkt kan sende til omkring 10 meter. Men tager man MESH netværkstopologien i betragtning, kan det samlede netværk strække sig til maximalt 65536 (2^16bit) enheder indenfor et enkelt PAN. Det er dog ikke alle produkter som anvender ZigBee protokollen der er i stand til at route, da dette kræver ekstra strømforbrug.

ZigBee Green Power

ZigBee Green Power er en måde hvorpå man helt kan slippe for brugen af batterier i mange produkter, så som stikkontakter mm. Dette sker ved at opfanger den kinetiske energi som bliver skabt ved at man trykker på kontakten. Den opsamlede energi bliver opbevaret i en silikone form som er designet til at køre på meget små mængder af energi eller en lille solcelle som blot bruge lyset eller varmen i rummet, den energi er nok til at sende flere signaler ud af enheden og så bliver routet videre I Mesh strukturen I hjemmet.

Green Power produkterne benytter sig af denne Ultra-low RF silicon, som bruger betydelig mindre strøm, der ud over benyttes der også en åben global standard IEEE 802.15.4 som sparer energi ved at reducere pakke længden, round-trip, Rediscovery og svartiden på udstyr der har været offline i længere perioder, typisk fordi disse ikke har været I brug.

Kilde henvisning

Hvad er ZigBee

http://www.zigbee.org/

Kompatabilitet

http://www.zigbee.org/zigbeealliance/our-members/

ZigBee Architecture

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

https://www.youtube.com/watch?v=noaspZ53swg&list=PL24BC4F9A51A9B5B5&index=1

Netværks aktivitet

https://www.youtube.com/watch?v=noaspZ53swg&list=PL24BC4F9A51A9B5B5&index=1

Sikkerhed

http://www.daintree.net/resources/zigbee-security/

http://modsec.zimmerle.org/wireless-sec-papers/zigbee%20-%20sec.pdf

https://www.ecnmag.com/blog/2013/09/zigbee-and-smart-home-security-issue

http://processors.wiki.ti.com/images/7/7b/10_-_ZigBee_Security.pdf

http://www.libelium.com/security-802-15-4-zigbee/#!prettyPhoto

Netværks standard

Texas Instrument slap 129.pdf

http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless

https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance

Node typer, PAN IDs, og adresser

https://www.youtube.com/watch?v=noaspZ53swg&list=PL24BC4F9A51A9B5B5&index=1

Fælles sprog

http://www.embedded.com/electronics-blogs/say-what-/4458281/Delving-deeper-into-dotdot---ZigBee-s-new--Universal-Language-for-the-IoT-

https://www.speakdotdot.com/dotdot/

Strømforbrug

http://www.zigbee.org/zigbeealliance/white-papers/