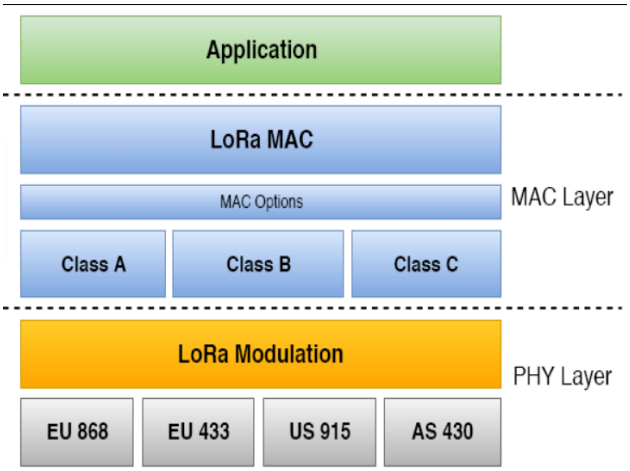
Giriş

Son yıllarda Nesnelerin İnterneti(Internet of Things - IoT) cihazlarının sayısı ve kullanımı arttıkça, kablosuz olarak uzak mesafelere ulaşma ihtiyacı artmaktadır. IoT uygulamalarının uzun menzilli, düşük veri oranı, düşük enerji tüketimi ve maliyet etkinliği gibi özel gereksinimleri vardır. Bu IoT uygulamalarının gereksinimleri yeni bir kablosuz iletişim teknolojisi olan **LPWAN'ın** ortaya çıkmasına sebep oldu. Bu yaptığım makale çalışmasında sizlere **LoRa Modülasyonu** ve ardından **LPWAN Teknolojisi** ve **LoRaWAN Uçtan Uca Mimarisi** hakkında bilgiler vermeye çalışacağım.

Bu makale çalışmamda LoRaWAN uçtan uca mimarisi anlatırken **toplamda üç ana başlık** kullanacağım.



Şekil 1: LoRaWAN Uçtan Uca Mimarisi Katmanları

Şekilde de görüldüğü üzere bu ana başlıkları **ilk** olarak LoRa modülasyonunun incelendiği **fiziksel katman(physical layer)**, **ikinci** olarak LoRaWAN uçtan uca mimarisinin anlatıldığı **MAC Layer** kısmı, **üçüncü** olarak ise **Uygulama(App) Katmanı(layer)** tarafı olacaktır. Bundan sonra ise makale çalışmasına sizlerin de hakim olması için bazı temel kavramları evvelden anlatmamız gerekecektir.

Kablosuz İletişim Nedir?

Verilerin **radyo frekansı(RF)** kullanılarak elektromanyetik dalgalar üzerinden havadan gönderilmesine denir. Elektromanyetik dalgalar, antenler üzerinden oldukça uzak mesafelere yayılabilirler. Bu özellik, elektromanyetik dalgaların hava üzerinden veri iletiminde taşıyıcı olarak kullanılmasına olanak sağlar. Mesajlar **modülasyon** denilen tekniklerle elektromanyetik dalganın üzerine bindirilerek antenler üzerinden uzak mesafelere gönderilir. Buna kısacası kablosuz iletişim diyoruz.

Modülasyon Nedir?

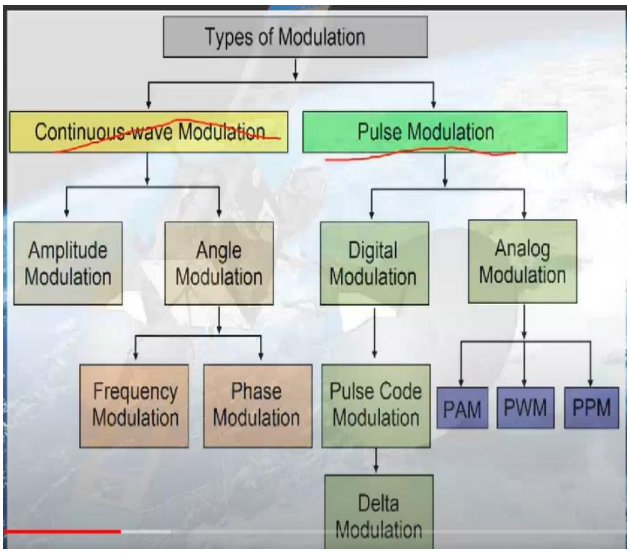
Modülasyon yapılmasının temal amacı; temel banttaki mesaj işaretini istediğimiz frekansta taşımaktır. Ayrıca anten boyunun formülünü düşünürsek;

$$\lambda = \frac{c}{f}$$

Şekil 2: Anten Boyu = Işık Hızı / Frekans

Buradaki anten boyunu küçültmek için frekansı artırmak gerektiğini görürürüz(ışık hızı zaten sabit). Frekansı artırmak için taşıyıcı başka bir sinyal ile frekansı yükseltmek gerekir(yani modülasyon).

Birçok modülasyon tekniği kullanılmaktadır. Eğer gönderilecek mesaj analog ise **analog modülasyon**(FM: Frequency Modulation, AM: Amplitude Modulation), dijital ise **dijital modülasyon** teknikleri kullanılarak mesajlar gönderilmektedir.



Şekil : Modülasyon Çeşitleri

1) **Fiziksel Katman(Physical Layer) Katmanı**

LoRa Tarihçesi ve Modülasyonu:

LoRa teknolojisi 2009 yılında Cyclo adlı bir Fransız firmasında ilan edilmiş ve 2012 yılında **Semtech** tarafından satın alınarak patentlenmiştir. Buna ilaveten 2015 yılında **LoRa-Alliance** tarafından standartlaştırılması tamamlanmıştır. Bu tarihten itibaren birçok ülkede kullanılmaya başlanan LoRa şu anda 162 ülkede aktif olarak kullanılmaktadır. LoRa **lisanssız ISM(Industrial Scientific Medical)** frekans bandında yayın yapmaktadır ve bu da farklı frekans değerlerini işaret etmektedir. Bu değerler Avrupa'da 868 MHz, Kuzey Amerika'da 915 MHz ve Asya'da 433 MHz.

LoRa uzun mesafe iletimi sağlayabilmek adına kullanılan kablosuz modülasyon yöntemi veya bir diğer ifadeyle **fiziksel katmandır(physical layer)**. Geleneksel kablosuz haberleşme teknolojilerinin fiziksel katmanda kullandıkları modülasyon olan FSK(Frequency-Shift Keying, Frekans Kaydırmalı Anahtarlama) modülasyonunun aksine LoRa, **CSS(Chirp Spectrum Spectrum) modülasyonu** kullanmaktadır. Bu sayede güç tüketimi yeteneğine ilaveten uzun iletim mesafesi olanağına da sahip olmaktadır.

Chirp Spread Spectrum Modülasyonunu kısaca anlatabilmek için bazı ilgili anahtar kelimeleri bilmemiz gerekecek.

Desibel(dB) Kavramı:

Çıkış gücünün giriş gücüne logaritmik oranıdır. dB = 10log10(P2/P1)

dBm Kavramı:

Kablosuz sistemlerin gücünü belirtmek için kullanılır. 1mW = 0 dBm.

BandWidth(Band Genişliği):

Temel band(spektrumu 0 Hz civarında) işaretlerinin genlik spektrumu 0'dan farklı olduğu en yüksek pozitif frekansına band genişliği denir. Diğer bir ifadeyle sinyalin yayıldığı frekans(Hertz) aralığıdır diyebiliriz.

LoRa Chip Rate(chips/s (Rc)):

Bu oran band genişliğine eşittir.

LoRa Bit Rate(Bit Hızı):

Her sembol SF bitlerinden oluştuğu için bit hızı:

$$Bit\ Rate = SF.\frac{Bandwidth}{2^{SF}}$$

Coding Rate(Kodlama Hızı):

Kodlama hızı, hata algılama(error detection) ve düzeltmeyi(correction) gerçekleştirmek için iletilen bit sayısını artıran bir orandır. CR = 4/8 oranında, her seferinde 8 bit iletilir, oysa gerçekte 4 bit iletmek istemekteyiz. Bu iletilen bit sayısının 2 katı olduğu anlamına gelir.

Adaptive Data Rate(ADR):

ADR'nin temel amacı LoRaWAN uç düğümlerinin(end-device) pil gücünden tasarruf etmektir. ADR bir end-device ve gateway arasındaki kablosuz bağlantı tüm kazanç ve kayıpların toplamını tahmin ederek bir link budget ayarlar. Örnek olarak, küçük bir paket iletilmesi gerekiyorsa düşük bir bant genişliği ayarlanır veya iletilecek düğüm yakında ise yayılım faktörü düşürülerek daha hızlı bir iletim sağlanır. ADR, Lora düğümleri ve ağ arasında asenkron olarak çalışır. ADR ayarlanması genel olarak ağ tarafından yapılır ve algoritması LoRa Alliance tarafından belirlenmiştir.

SNR(Signal-Noise Ratio):

Alınan sinyal gücünün(Pr), gürültü tabanı sinyali gücüne(Pn) oranıdır(Pr/Pn (dB)). Gürültü tabanı, iletilen sinyali bozabilen ve bu nedenle yeniden iletimlerlere sebep olabilecek istenmeyen girişime neden olan istenmeyen bir alandır. SNR 0'dan büyükse, alınan sinyal gürültü tabanının üstünde gerçekleşiyor demektir. 0'dan küçük ise, alınan sinyal, gürültü tabanının altında gerçekleşiyor demektir. Normalde gürültü tabanı iletişim yapabilmek için sınırdır fakat LoRa haberleşmesi gürültü tabanının altında gerçekleşir. Genel olarak, LoRa için SNR değerleri -20dB ile +10dB arasında değişir. +10dB'ye yaklaştıkça gelen sinyal daha az bozulmuştur. LoRa, gürültü tabanının -7.5 dB ila -20 dB altındaki sinyalleri demodüle edebilir.

Link Budget:

İletilen(Pt) güç ile alıcının hassasiyeti arasındaki farka link budget denir(dBm). Örneğin; iletici hassasiyetine 13 dBm dersek, alıcı hassasiyetine -80 dBm dersek link budget 93 dBm olur.

RSSI(Received Signal Strength Indication):

Alınan sinyalin gücü demektir(Pr(dBm)). Her haberleşme çeşidi ve donanım üreticisi için RSSI aralığı farklıdır. RSSI hassasiyeti, alıcının alınan sinyali doğru şekilde dekod edebilmesi için kabul edilebilir bir bit hata oranı cinsinden minimum sinyal gücü seviyesini gösterir. RSSI negatif olarak temsil edilir ve 0'a yaklaştıkça sinyalin gücü artmaktadır.

Sensitivity(Duyarlılık/Hassasiyet):

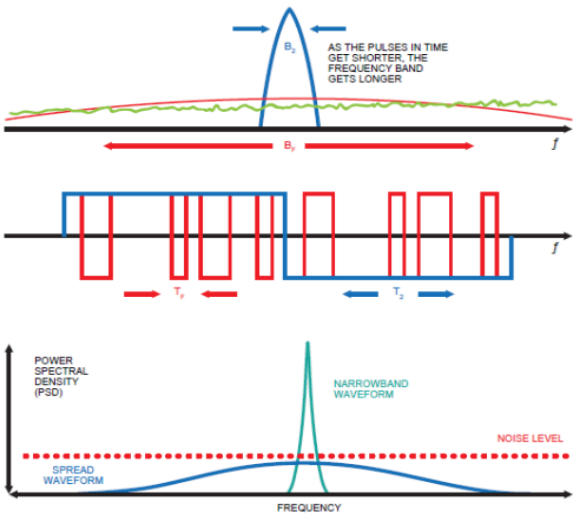
Sinyali almak için alıcıda bulunması gereken minimum Pr gücüdür(yani minimum RSSI). Alınan sinyal RSSI hassasiyet seviyesinin altındaysa sinyal algılanamaz.

Şu durumlar sağlanırsa sinyal düzgün iletilir:

İlk şartımız, RSSI değeri alıcının sensitivity seviyesinden büyük olmalı. İkinci şartımız SNR değeri sinyalin alıcı tarafında algılanmasını imkansız kılacak belli bir eşik(threshold) değerinin altına düşmemeli.

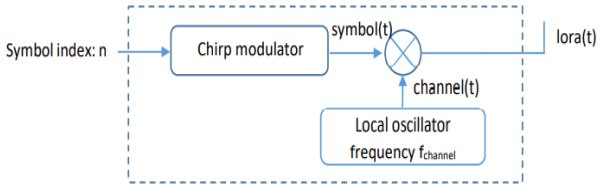
CSS Modülasyonuna Giriş

LoRa modülasyonu var olan Chirp Spread Spectrum(CSS) teknolojisinden türetilen tescilli spread-spectrum modülasyon tekniğidir. CSS, **Doğrudan Sıralı Yayılı Spektrum'un(Direct Sequence Spread Spectrum = DSSS)** bir alt kategorisi olarak kabul edilir. DSSS'e biraz değinecek olursak, bu sistemde verici sinyalinin taşıyıcı fazı şekilde gösterildiği gibi bir **kod dizisine(chip sequence-code sequence**) göre değişir.



DSSS system carrier phase transmitter signal changes

Veri sinyali önceden tanımlanmış **bit dizisiyle(kod dizisi (chip sequence-code sequence))** yüksek oranda bir yayılma faktörüyle çarpılırken, orjinal veri sinyalinden daha yüksek frekans komponentlerine sahip bir sinyal oluşturulur. Bu da sinyal band genişliğinin orjinal sinyal band genişliğinin ötesine yayıldığı anlamına gelir.



LoRa modulation block diagram

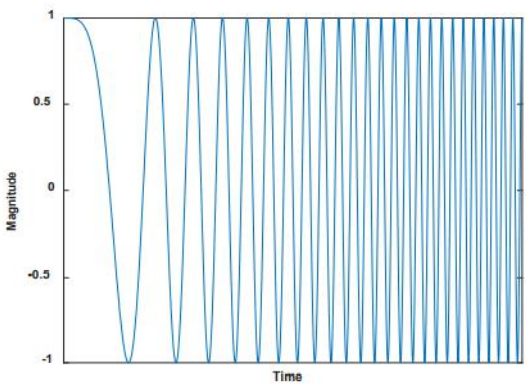
RF terminolojisinde kod dizisinin bitlerine **chip** denir(yukarıdaki resim). Ayrıca her sembolü kodlamak için kullanılan bit sayısına **yayılım faktörü(Spreading Factor(SF))** denir**.** İletilen sinyal RF alıcısına ulaştığında, RF vericisinde kullanılan SF'nin aynı bir kopyası ile çarpılır ve orjinal sinyalin kopyasıyla sonuca erişiriz(**demodülasyon**).

Bunu yapıyoruz ki elimizdeki kod dizisi(chip sequence) bize daha yüksek bir **link budget** elde etmemize olanak tanısın. İşlem kazancı(Gp), kanalımız negatif SNR'ye sahip olsa bile alıcının orjinal veri sinyallerini kurtarmasına izin verir(**işlem kazancı** (veya "işleme kazancı"), yayılmış (veya RF) bant genişliğinin yayılmamış (veya temel bant) bant genişliğine oranıdır. Genellikle desibel (dB) cinsinden ifade edilir. Örneğin, 1 kHz'lik bir sinyal 100 kHz'e yayılırsa, sayısal oran olarak ifade edilen işlem kazancı şöyle olur: 100 000 /1000 = 100. Veya desibel olarak, 10 log $_{10}$ (100) = 20 dB). LoRa modülasyonu FSK modülasyonuna kıyasla üstün bir Gp'ye sahiptir.

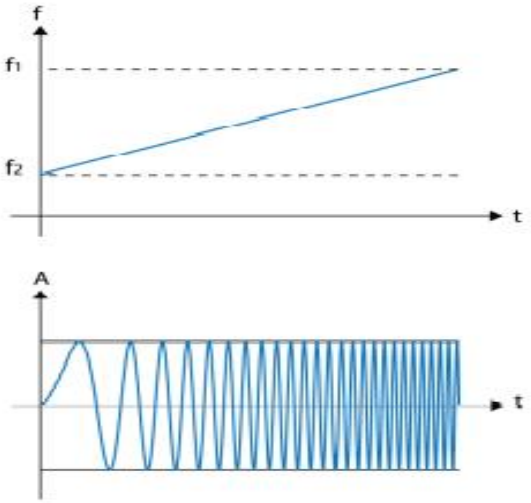
LoRa işlem kazancı(process gain Gp) bir **yayılma kodu(spreading factor) veya bir chip dizisi(chip sequence**) ile çarpılmasıyla RF kanalına dahil edilir. Chip hızını artırarak toplam sinyalin spektrumunun frekans bileşenlerini artırıyoruz. **Yani sinyalin total enerjisini artık daha geniş bir frekans aralığına yayarak alıcının daha düşük bir SNR ile sinyali ayırt etmesine izin veririz.**

Semtech'in LoRa Chirp Spread Spectrum teknolojisi düşük maliyetli ve düşük güçlü DSSS alternatifi sunar. Dataların iletilmesi için Spread Spectrum kullanılması gerektiğini belirtmiştim. Yani yine az evvel belirttiğim **kod dizisi bitleri(chip) yerine** Chirp Spread Spectrum Modülasyonunda adlandırılan **"Chirp"** kullanır(Chirp: **C**ompressed **H**igh **I**ntensity **R**adar **P**ulse). LoRa modülasyonunda sinyal spektrumunun yayılması şekilde gösterildiği gibi, bilgileri kodlamak için belirli bir süre boyunca **frekansı sürekli artan veya azalan geniş bantlı doğrusal frekans modülasyonlu darbeleri kullanan** bir **chirp** sinyali üretilerek elde edilir. Chirp sinyali zamanla

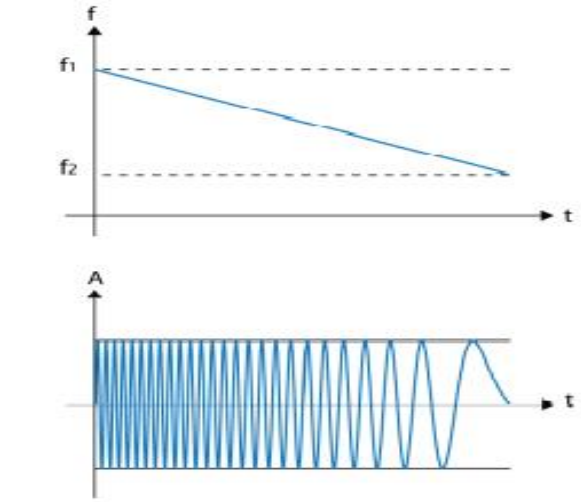
düzenli olarak artan veya azalan sinus dalgasıdır.



Şekil: Zaman ekseninde Chirp sinyali



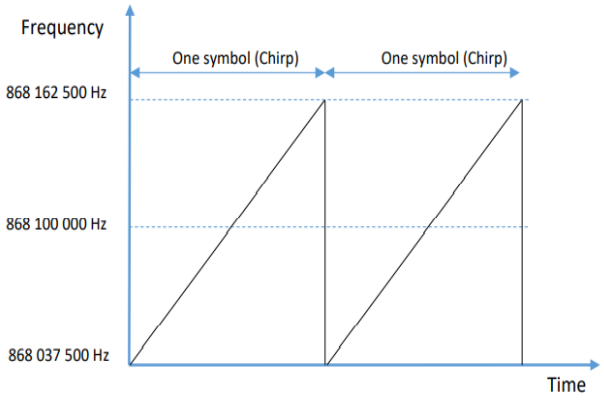
Şekil: Zaman içinde doğrusal olarak artan sinozoidal chirp dalga(Up-Chirp)



Şekil: Zaman içinde doğrusal olarak azalan sinozoidal chirp dalga(Down-Chirp)

Bu metodun avantajı verici ve alıcı arasındaki zamanlama ve frekans sapmalarının eşit olması, alıcı tasarımındaki karmaşıklığın büyük oranda düşmesidir.

LoRa, CSS modülasyonunu geliştirerek gürültüye ve girişime(cızırtı-bozulma) karşı daha da güçlü olmak için çeşitli yöntemler kullanır. Bunlardan birisi LoRa modülasyonu sırasında gönderilen bitleri kodlamaktır.

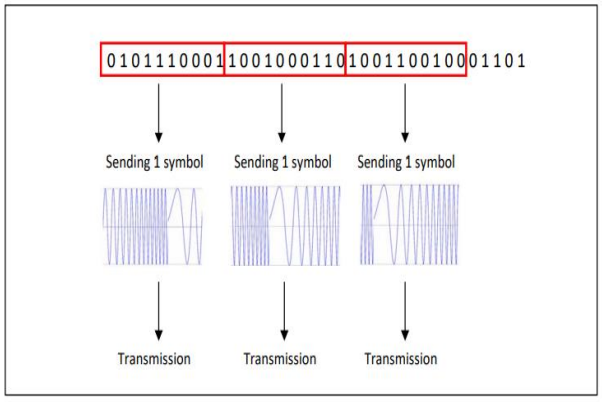


Şekil : 868 MHz'de Örnek Sembol(Chirp)

Her **sembolü** kodlamak için kullanılan bit sayısına **yayılma faktörü(Spreading**

Factor) denir(bahsetmiştik). LoRa'da her sembol, iletilen bir dizi biti temsil eder(**Bir sembolde iletilen bit sayısı = Yayılma Faktörü(Spreading Factor)**).

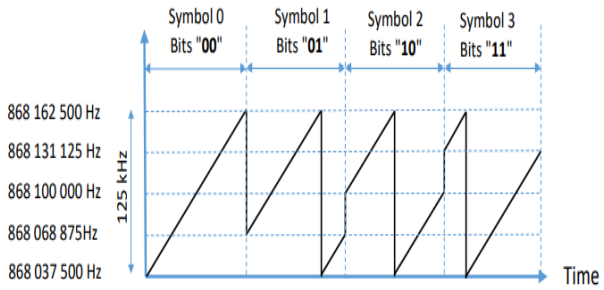
Örneğin, iletim yapmak için SF10 kullanıyorsak, bir **sembol(chirp)** 10 biti temsil eder. İletim sırasında bitler SF bit paketlerinde birlikte gruplanır. Aşağıdaki resimde bitleri 10'luk paketler halinde gruplandırıyoruz. 10 bitlik her paket belirli bir sembolle temsil ediliyor. 1024 olası binary kombinasyonu (2^10) kodlamak için 1024 farklı sembol vardır(1024 tane chip tutar). Bir LoRa sembolü(chirp), tüm frekans bandını kapsayan 2^SF chip'lerden oluşur.



LoRa Chirp transmission

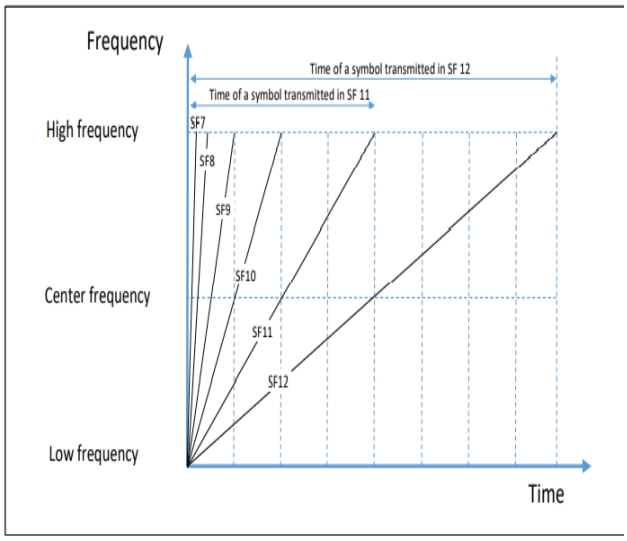
Şekil : LoRa Chirp iletiminin bit karşılığı

Her paket, olası **2^SF** formları arasında belirli bir sembolle temsil edilir. Semboller arasındaki tek fark, hepsinin bit paketlerini temsil eden belirli bir frekanstan başlamasıdır. İlgili şekilde 125 kHz band genişliği ile 868,1 MHz'de SF2 modülasyonunun teorik örneğini göstermektedir(Aslında SF2 diye bir şey yok, sembolleri 2 bitle temsil etmek için SF2 diyoruz.)



Şekil : Belli bitlerle sembol edilen chirp'ler

Yayılma faktörü bir cihaz için **7'den 12'ye** kadar çalışabilir. Daha yüksek yayılım faktörü sinyali gürültüye karşı dayanıklı hale getirir ve daha uzak mesafeli alıcıya ulaşmasını sağlar. Yayılım faktörünün artması sinyalin gürültülü bir ortamda daha uzak bir mesafeye iletilmesini sağlarken, karşıya iletilebilecek paket büyüklüğü gittikçe azalır. Bunun anlamı, düşük yayılım faktörüne sahip bir iletimle gönderilen paketi yüksek yayılım faktörü ile iletmek istersek daha uzun süre iletişimde kalmamız gerekir. Bir dezavantaj olarak da aynı frekansı kullanan diğer cihazlara girişim(bozulma) oluşturma ve LoRa ağları için gereksiz trafik oluşturmaktadır. Bu sebeple ağı yapılandırırken önerilen, **adaptif** şekilde data hızını ayarlamak olmalıdır. Bu şekilde bant genişliğini daha verimli kullanabilir ve güçten tasarruf edebiliriz. LoRa **adaptif data oranı(Adaptif Data Rate)** özelliğine sahiptir. **ADR** etkinleştirildiğinde cihaz efektif bir bağlantı için en düşük yayılım faktörünü seçecektir. Düşük yayılım faktörü ile kısa mesafeli iletişim sağlanırken daha yüksek büyüklüğe sahip paketler yollanabilir.



$$T_{symbol} = \frac{2^{SF}}{Bandwidth}$$

Spreading Factor	Symbol transmission time
SF7	1.024 ms
SF8	2.048 ms
SF9	4.096 ms
SF10	8.192 ms
SF11	16.384 ms
SF12	32.768 ms

Şekil : SF Faktörüne göre iletim zamanı

Şekilde de görüyoruz ki her sembolün iletim(transmission) zamanı yayılma faktörüne(SF) bağlıdır. Zaman 2 katı kadar artmaktadır. En yüksek SF en uzun iletim zamanıdır.

Ortogonallik:

LoRa modülasyonunun farklı Spreading Factor'lerini kullanan paketler birbirine **ortogonaldir.** Yani birbirine **görünmez** diyoruz. Bu yüzden farklı SF kullanan sinyaller birbirine gürültü olarak görünecektir. Bu sebeple aynı alıcı kanalına farklı yayılma faktörlerinde aynı anda ulaşan iki paket çarpışmayacak ve her ikisi de ileri de değineceğim **gateway** tarafından demodule edilecektir. Ancak aynı kanalda aynı anda gelen aynı yayılma faktörüne sahip iki paket bir çarpışmaya(collision) neden olabilir. İki paketten biri 6 dB daha güçlüyse o hayatta kalır.

Son olarak LoRa modülasyonu **karakteristiği** ile bu konuyu özetleyelim.

LoRa fiziksel katmanı **düşük verim**, **yüksek veri hızı** ve **yüksek link budget** için tasarlanmıştır. Sabit bir band genişliği yayılma faktörü ne kadar yüksek olursa chip hızının ve veri sinyalinin işlem kazancı(Gp) o kadar yüksek olur, bu da sensitivity'de ve link budget'da bir artışa neden olur . Ancak havada geçirilen süre(Time on Air) de artacak. Yayılma faktörlerindeki **ortogonallik**, hem aynı kanal frekansında hem de aynı zaman diliminde birden fazla LoRa sinyalinin iletilmesine izin verir.

2) MAC Katmanı(Layer):

Buraya kadar LoRa modulasyonunu -yani 3 ana başlıkta incelediğimiz makalemizde- physical layer kısmını tamamlıyoruz ve artık LoRaWAN konusuna değinmeye başlıyoruz. Burası makalemizin ikinci ana başlığı olan **"MAC Layer"** kısmıdır. Artık LoRaWAN kısmına başladığımıza göre ilk olarak LoRa ile LoRaWAN arasındaki farkı açıklamak gerekmektedir.

Buraya kadar anlattığım şey LoRa modülasyonunu kapsamaktadır. Bu modülasyonda CSS denilen özel bir tekniği kullanmaktadır. LoRaWAN ise bu modülasyon sayesinde end-device'den gelen bilgilerin internet ortamına çıkıp daha uzağa gitmesini sağlar. Bunu da bir **gateway(ağ geçidi)** ve **Network Server(Ağ Sunucusu)** gibi ileride açıklayacağım ekipmanlar ile yapmaktadır. LoRaWAN, LoRa physical layer(fiziksel katman) kısmının pek çok özellik eklenmiş halidir. Kriptografik güvenlik, mesajların farklı veri hızlarında

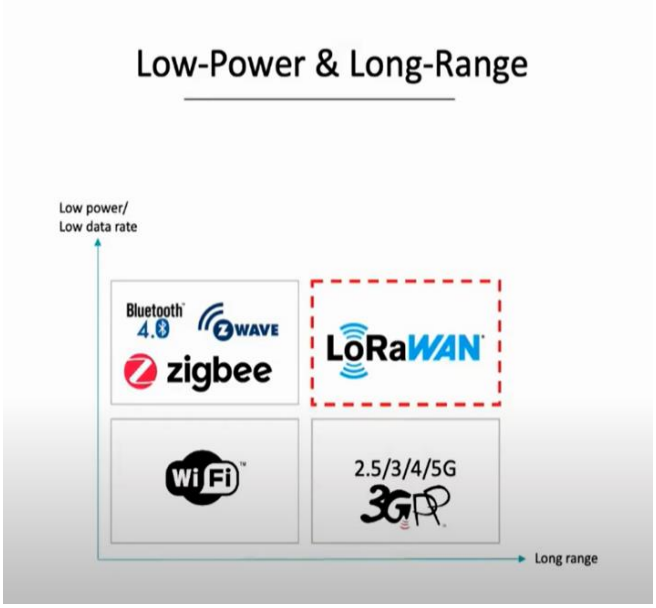
ayarlanıp iletilmesi ya da cihazların **roam** yapması LoRaWAN MAC layer tarafında gerçekleşir.

Şöyle daha anlaşılır olsun: İki gateway arası antenden antene giden sinyal veya uç cihazdan antene giden sinyal LoRa üzerine yerleşik LoRaWAN'dır. Göndermek istediğimiz mesajın 1 ve 0'lı versiyonunu radyomanyetik sinyallere çeviren veya bu radyomanyetik sinyalleri 1 ve 0'lara dönüştüren katman LoRa iken, bu mesajı şifreleyen kısım LoRaWAN'ın içinde olduğu MAC Layer tarafıdır.

MAC denme sebebine değinirsem uygulama katmanından(app. layer) gelen veriler, son cihaz(end-device) ile ağ geçidi(network server) arasında bağlantı kurmak için gerekli olan MAC komutları MAC yükü(payload) olarak taşınır ve ardından MAC katmanı MAC yükünü kullanarak MAC çerçevesini(katman – layer) oluşturur.

LPWAN Protokolü - LoRaWAN Uçtan Uca Mimarisi

IoT uygulamalarında farklı amaçlar için kullanılabilecek birçok kablosuz iletişim protokolü mevcuttur. Yakın mesafe düşük güç tüketiminde en yaygın kullanılan iletişim protokolü RFID ve NFC(Near Field Comm.)'dir. Bunlar 10 metreye kadardır. Kısa mesafede Bluetooth, Zigbee gibi protokoller üzerinden küçük veya orta boyutlu veri paketleri 50-100 metre arasında iletilmektedir(WPAN: Wireless Personel Area Network). Orta mesafede ve güç tüketiminin önemli olmadığı uygulamalarda(yaklaşık 1000 metre) Wi-Fi iletişim protokolleri kullanılır(WLAN:Wireless Local Area Network). Uzun mesafede büyük veri letimi için 4G/5G gibi hücresel(GSM) iletişim protokollerinden faydalanılmaktadır(WWAN: Wireless Wide Area Network).



Şekil : Diğer teknolojiler ile LoRaWAN

LPWAN protokolünü öne çıkarmak için şöyle düşünelim. Şimdi bizim elimizde 100 adet birbirinden uzak noktadan veri alacağımız sensor olduğunu düşünelim. Mesafelerden ötürü Bluetooth ve Wi-Fi'yi tercih edemiyoruz. Wi-Fi çok fazla güç harcayacaktır. GSM kullanılması düşünülebilir. 100 adet noktaya SIM kartlı modüller takılıp, veriler GSM şebekesi üzerinden alınabilir. İşin maliyeti ve sensörlerin hangi güç ile çalışacağı sorundur. **GSM standart olarak büyük veri paketlerini sürekli göndermek üzere tasarlanan bir teknolojidir.** Bant genişliği çok yüksektir. Sensör tarafında SIM kart gerektirdiği için operasyonel olarak pahalı bir çözümdür. LPWAN'ın avantajı sürekli bilgi göndermediğinden güç tüketimi azdır. Bu yüzden dar bir band genişliği yeterli olacaktır. LPWAN'ın içerisindeki **LoRaWAN, SigFox, NBIoT** gibi

teknolojiler bu alanı destekleyen teknolojilerdir.

LPWAN(düşük güç geniş haberleşme ağı) düşük güçlü WAN içindir. LPWAN denen şeyde 4 ana protokol vardır. Bunlardan ikisi NBIoT ve LTE-M olarak adlandırılır. Diğer ikisi de SigFox ve LoRaWAN olarak adlandırılan **freeband** alanında çalışır**. Kendi özel network ağımızı kurma şansımız olduğundan** LoRaWAN SigFox'a göre öne geçmiştir. Ayrıca verileri bir tabloda veya grafikte istediğimiz şekilde görüntüleyebilmek için dashboard özelliği sunmaktadır.

LoRaWAN, LoRa'nın tepesinde yer alır ve LPWAN'ın iletişim protokolünü ve ağ mimarisini tanımlar. Bir LoRaWAN ağı, sahaya dağıtılmış düğüm cihazları(end-devices), bu cihazla konuşan gateway'ler(ağ geçitleri), bu gateway'lerden veri alan ağ sunucusu(network server) ve uygulama sunucusundan(application server) meydana gelir.

LoRa tabanlı cihazlar üretilirken kendilerine benzersiz olacak şekilde tanımlamalar yapılır. Bu tanımlayıcılar sayesinde, paketlerin özel veya yerel ağlar yanı sıra bulut sistemlerine güvenli şekilde aktarılması sağlanır.

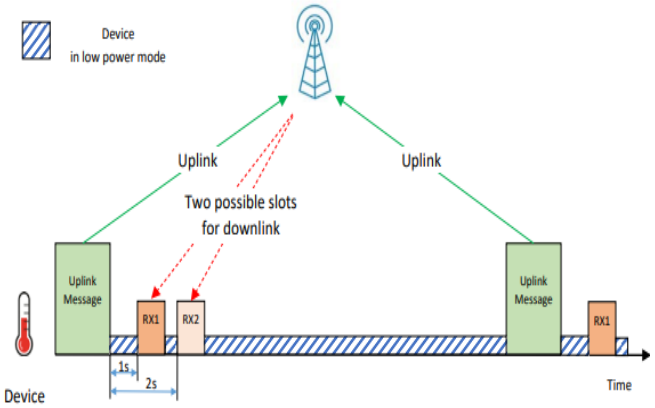
Ayrıca her LoRa gateway'i kendine has bir ID'ye sahiptir(64 bits EUI). Bu ID Network Server ile etkileşimde olan gateway'e kayıt olmaya ve aktif etmeye yarar.

LoRaWAN Sınıfları:

LoRaWAN end-devices'leri güç tüketimlerine ve downlink(aşağı-bağlantı) kapasitelerine göre **A(All)**, **B(Beacon)** ve **C(Continuous)** olarak sınıflandırılır. Cihaz sınıflarının kullanımı, batarya kullanım ömrüne karşı elimizdeki ağın(network'un) downlink iletişim gecikmesini gerçekleştirmesini sağlamaktadır.

A sınıfı cihazlar şu şekilde çift yönlü iletişimi desteklemektedir: uç cihazımız her bir uplink(yukarı iletim) sonrası **iki kısa gönderi penceresi(2 slot)** açar. Gönderi pencereleri uç cihaz tarafından kendi iletişim ihtiyaçları doğrultusunda rastgele bir şekilde takvimlenir.

Sadece cihaz mesaj gönderdikten kısa süre sonra aşağı mesaj gönderimi imkanı sağlamaktadır. Serverden başka herhangi bir zamanda gönderilen mesajlar bir sonraki takvimlenen mesajı beklemek zorundadırlar.

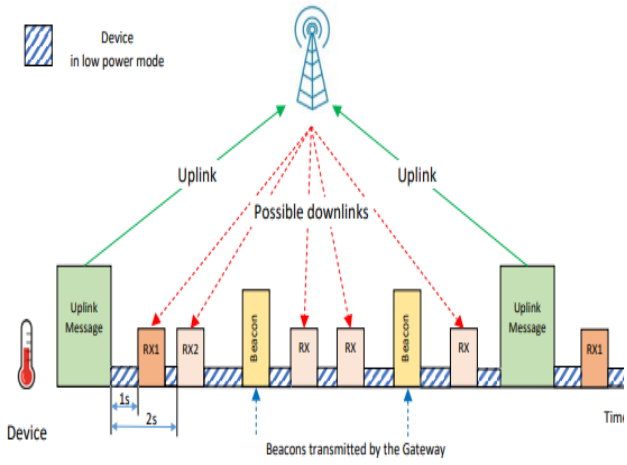


Şekil : A Sınıfı Cihaz Davranışı

Şekildeki gibi RX1, uplink iletiminin 1 sn sonra default olarak ayarlanır. Bu değer Network Server konfigürasyonuna göre değiştirilebilir. A sınıfı bir end-device yukarı bağlantı verilerini iletmediyse bir şey alamaz. Bu nedenle kolayca da ulaşım yapamayız. Tüm uç cihazlar ağa ClassA olarak başlar ve katılır.

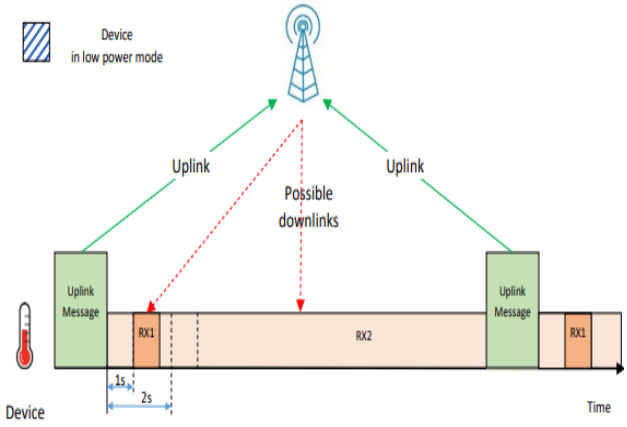
B Sınıfı cihazlara gelince, bunlar daha fazla dinleme periyodu bulundurmaktadırlar. A sınıfı dinleme periyoduna ek olarak B sınıfı

takvimlenen zamanlarda yeni dinleme periyodları açar. Bu dinleme periyodlarını senkronize etmek için uç cihaz gateway'den senkronize edilmiş şekilde **Beacon** alır. Bu sayede uç cihazın ne zaman dinleme yaptığını bilebilir.



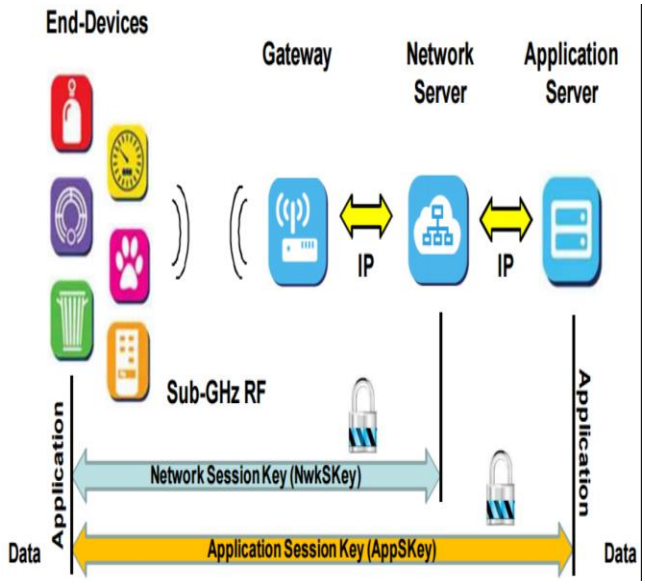
Şekil : B Sınıfı Cihaz Davranışı

C sınıfı cihazlar ise her zaman dinleme yapmaktadır. Sadece veri aktarımı yaparken dinlemeyi durdururlar. A ve B sınıfına göre daha fazla enerji tüketir.



Şekil : C Sınıfı Cihaz Davranışı

LoRaWAN Ağ Mimarisi



Şekil : LoRaWAN ağ mimarisi

Birden fazla ağ geçidi(gateway) merkezi bir ağ sunucusuna(network server) bağlıdır. LoRaWAN ağındaki son cihazlar belirli bir ağ geçidi ile ilişkili değildir. Dolayısıyla bir son cihaz tarafından iletilen paketler, birden fazla ağ geçidi tarafından –eğer kapsama alnında ise- alınabilir. Her ağ geçidi, alınan bu paketi son cihazdan bulut tabanlı merkezi ağ sunucusuna bazı ana taşıyıcılar(örn: hücresel, ethernet, uydu veya Wi-Fi) vasıtasıyla iletir. Bir başka deyişle LoRaWAN **gateway** sadece uç cihazlardan gelen ham veri veya komut paketlerini UDP/IP paketleriyle kapsülleyerek merkezi network server'a iletilmesinden sorumludur(resimdeki gateway – network server arası). **Network Server,** ağı yönetmekten, gereksiz gelen paketleri filtrelemekten (duplication), güvenlik kontrolleri yapmaktan, en uygun ağ geçidi üzerinden onayları (ACK) planlamaktan, geçerli olan paketleri uygulama sunucusuna(application server) iletmekten ve gerekirse son cihazlara(end device) aşağı

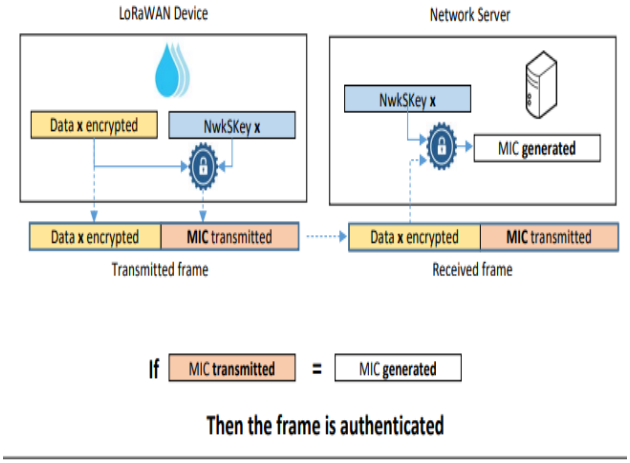
bağlantı(downlink) ve MAC komutları göndermekten sorumludur.

Uygulama katmanı, güvenliği, ağ operatörünün son kullanıcıların uygulama verilerine erişmemesini sağlar. Veriler ilk önce bir **Ağ Oturum Anahtarı(NwkSKey)** ile ardından bir **Uygulama Oturum Anahtarı(AppSKey)** ile AES şifreleme algoritmasını kullanarak şifrelenmektedir. Bu sayede verilere sadece ilgili uygulama sunucusu(app. server) erişebilmektedir.

Network Server, **NwkSKey** diye adlandırılan **128 bit AES** anahtarı sayesinde mesajı **authenticate(kimlik uyuşması)** eder. Authenticate süreci başarılı olursa Network Server Application Server'a mesajları transfer edecektir.

Authenticate Nasıl Olur?

Kimlik uyuşması işleminin gerçekleşmesi için çerçeveye(frame) bir MIC(Message Integrity Control) alanı eklenir. MIC, şifrelenmiş iletilmiş veriye ve NwkSKey'e bağlıdır. Mesajların alımı sırasında da aynı hesaplama yapılacaktır. NwkSKey end-devices'de ve Network Server'da aynı ise, iletilen MIC Alım sırasında üretilen mesajla aynı olmalıdır.



device authentication by the Network Server

Hazır LoRaWAN Network Server'indeyken genel özelliklerini de şöyle sıralamak istiyorum:

Cihazın adres kontrolü, mesaj çerçevelerinin(frame) authenticate edilmesi, alınan mesajların onayları, ADR özelliği sayesinde veri hızlarını control etmek, cihazdan gelen tüm MAC layer katmanlarına izin verilmesi, uygun app. server'a uplink mesajları iletmek, cihazlar ve join-server arasında **join-accept** ve **join-request** mesajlarının iletilmesi gibi sıralayabiliriz.

Application Server, Network Server'den encryption(şifrelenmiş) olmuş mesajları alır(İlk başlarda LoRaWAN'da mesajlar şifreleniyor yazmıştık, ayrıca LoRaWAN uyumlu end-device ve Network Server arasındadır). Encryption ve Decryption(şifre çözülmesi) **AppSKey** diye adlandırılan128 bit AES anahtarı sayesinde yapılmış olur(LoRaWAN uyumlu end-device ve Application Server arasındadır).

Şimdi şu **Katılma Prosedürüne(Join Procedure)** biraz daha değinmek istiyorum. İlk olarak Join Server'i tanıtalım. Join Server **uplink join-request** çerçevelerini işlemek ve **downlink join-accept** çerçevelerini oluşturmak için gerekli bilgileri içerir. End-devices'e hangi uygulama sunucusunun(app. server) bağlanması gerektiğini bildirir ve NwkSKey ve AppSKey anahtar oluşmasına katkı sağlar. Cihazın NwkSKey'ini ve AppSKey'ini uygulama sunucusuna iletir. Bu amaç doğrultusunda Join Server kontrolü altındaki her cihaz için şu komponentlere sahip olmalıdır. DevEUI(end-device serial unique identifier), AppKey(Application Encryption Key), NwkKey(network

Encryption Key), Application Server İdentifier, End-Device Service Profile.

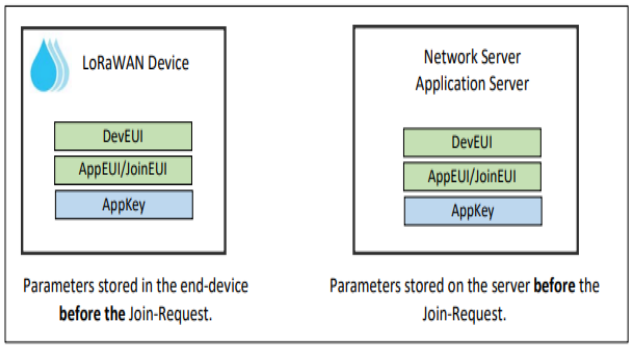
LoRaWAN Cihazları Aktivasyonu

Bir uç cihaz(end-device) ağ sunucusuyla iletişim kurmadan önce, uç cihaz etkinleştirilmeli ve **katılma prosedürünü(join procedure)** tamamlamalıdır. LoRaWAN spesifikasyonunda, bir uç düğüm(end-device), LoRaWAN ağına katılım için **Hava Yoluyla Aktivasyon (OTAA)** veya **Kişiselleştirme ile Aktivasyon (ABP)** yöntemlerinden herhangi birini kullanır. Bu metotlar arasındaki en önemli fark ABP'de uç cihaz herhangi bir katılım işlemine tabi tutulmadan, oturum anahtarlarını, haberleşmeye başlamadan önce kendi üzerinde bulundururken, OTAA metodunda bu anahtarlar ağa katılım yapılırken otomatik olarak türetilir.

OTAA Aktivasyon Metodu:

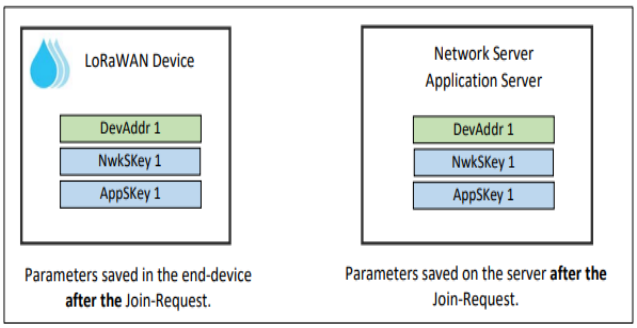
Önceki kısımda da Join Prosedürünü anlattığımıza göre ve burada da Join prosedürü ile karşılaşacağımız için hemen bunu okuyarak okumamıza devam edelim.

OTAA aktivasyon modu ile, LoRaWAN uç cihazı Network Server'a bağlanırken Join prosedürü boyunca(hatta sonrasında diyelim) DevAddr, AppSKey, NwkSKey oluşturulacaktır. Join prosedürünü gerçekleştirmek için LoRaWAN cihazı şunlarla yapılandırılmalıdır.



*Parameter stored **before** the Join-Request (OTAA)*

Şekil : Join-Request'den önce depolanan parametreler



*Configuration **after** the Join-Request (OTAA)*

Şekil : Join-Request'den sonra depolanan parametreler

Gösterdiğim gibi OTAA metodunda katılım prosedürü, uç cihazın katılım prosedürüne başlamadan önce DevEUI, JoinEUI ve AppKey gibi bilgilerle kişiselleştirilmesini gerektirir. Bu bilgiler sağlandıktan sonra uç cihaz artık hava yoluyla aktivasyona hazırdır. OTAA metoduna göre katılım prosedürü, bir uç cihaz ile sunucu arasında Join Request ve Join Accept gibi mesajlarla haberleşmesinden elde edilen uç cihaz adresi DevAddr, AppSKey ve NwkSKey anahtarlarıyla sonlanır. Bu anahtarlar elde edildikten sonra uç cihaz ile sunucular arasında veri ve komut aktarımı gerçekleştirilebilir.

DevEUI: LoRaWAN end-device için unique bir tanımlayıcıdır. Ethernet üzerindekşi bir

MAC adresine denktir denilebilir. Fabrikasyon çıkışlıdır ve değiştirmek mümkün değildir.

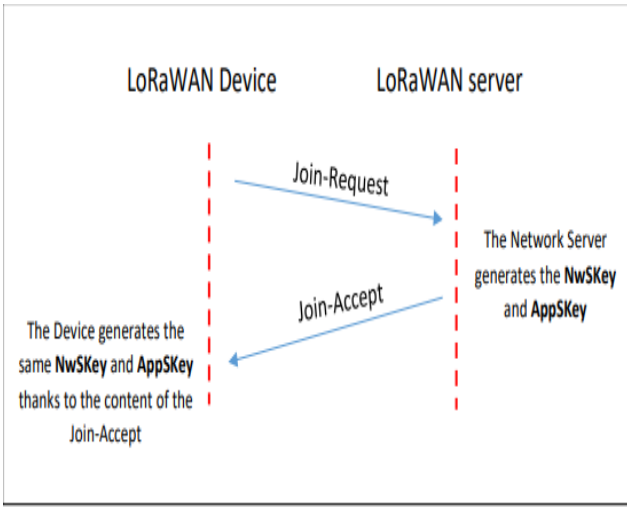
AppKey: Join-Request sürecine authenticate için kullanılır. 128 bit AES anahtarıdır. Join-Accept'i şifrelemek ve session key'ler oluşturmak için kullanılır. Gizli olup, paylaşılmamalıdır.

AppEUI: Eski LoRaWAN sürümlerinde uygulama tanımlayıcısı(application identifier) iken, güncel sürümlerde Join Server identifier olarak bize sunulur.

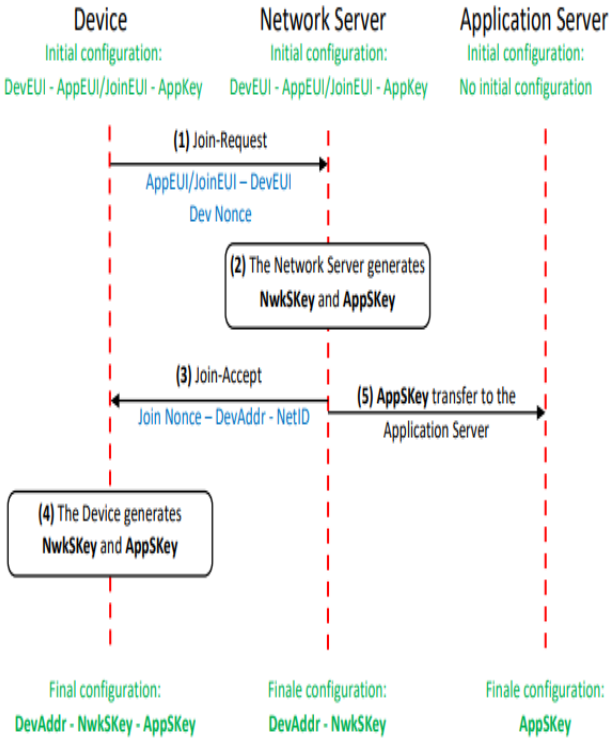
NwkSKey: Network Server ile authenticate içimn kullanılır.

AppSKey: Uygulama Sunucusu ile verilerin şifrelenmesi(encryption) için kullanılır.

DevAddr: Bir LoRaWAN Network içinde 32-birtlik tanımlayıcıdır.



Şekil : OTAA'da Join Prosedürü



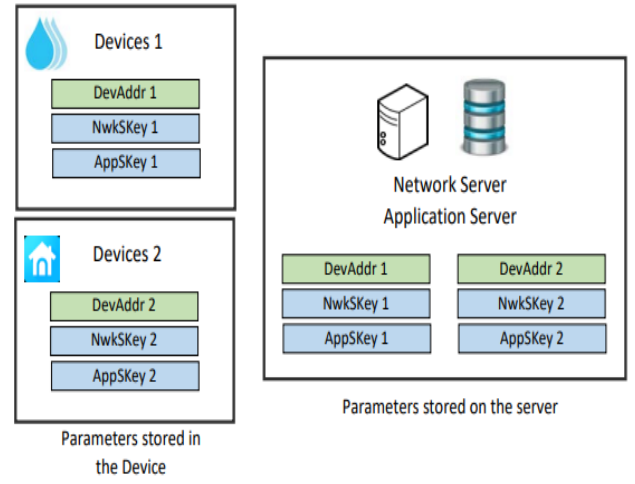
Şekil : Detaylı Join Procedure

Şekilde görüldüğü gibi (1) kısmındaki taraf henüz şifrelenmiş değildir. (2) ve (4) numaralı kısımlar karşılıklı üretilen anahtarlardır. (5) kısmındaki AppSKey'deki şifreli datalar sayesinde uygulama sunucusuna çıkılır.

ABP Aktivasyonu:

Bu metod bir protatipi test ederken ve bir LoRaWAN iletişimi kurarken kullanma eğilimindeyiz. Sabit bir DevAddr, NwkSKey, AppSKey end-devices'de depolanır. DevAddr, NwkSKey, AppSKey hem end-devices'de hem de LoRaWAN server'da depolanır. Yani DevAddr ve NwkSKey ve AppSKey gibi oturum anahtarlarının, katılım işlemi sırasında doğrudan DevEUI, JoinEUI, AppKey ve NwkKey'den türetilmesi yerine doğrudan cihaza depolanması anlamına gelir. Uç cihaz, başlatıldığı anda belirli bir LoRa

ağına katılmak için gerekli bilgilerle donatılmıştır. Mesajlar gönderilip alınabilir.



DevAddr, NwkSKey and AppSKey in ABP

AT Komutları: