Ermanno Goletto
Microsoft Most Valuable Professional
Microsoft Certified

LoRa Nozioni di base e approfondimenti

Introduzione

Negli ultimi anni l'Internet of Things (IoT) o "Internet delle cose" si sta diffondendo come insieme di tecnologie integrate, nuove soluzioni e servizi che hanno come obbiettivi l'aumento della qualità della vita delle persone, il miglioramento dei processi produttivi e dell'utilizzo di beni e servizi. In altre parole l'IoT è una possibile evoluzione dell'uso della Rete in cui gli oggetti (ovvero le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie alla possibilità di poter comunicare dati e accedere ad informazioni aggregate da parte di altri.

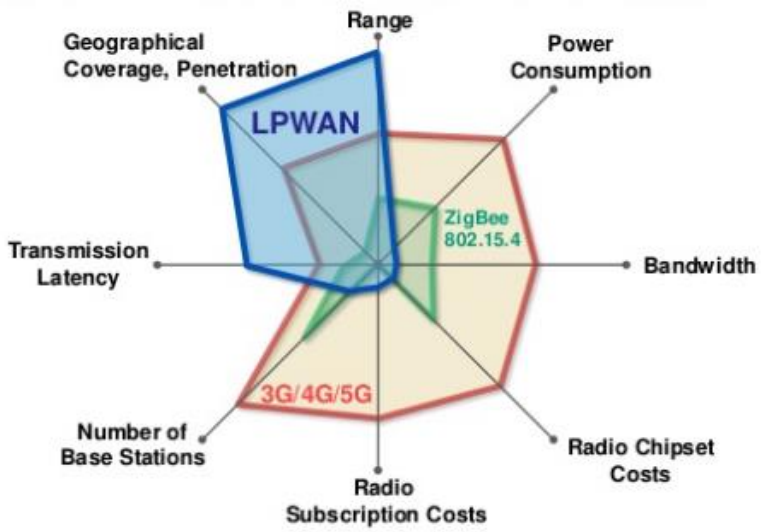
Stando all'ultimo Ericsson Mobility Report di Novembre 2018 si stima che nel 2024 i dispositivi IoT connessi in rete saranno 22.3 miliardi contro gli 8.6 miliardi del 2018 con tasso annuo di crescita o CAGAR (Compound Annual Growth Rate o) del 17%. Diversi sono i fattori chiave che determineranno la diffusione dell'IoT ovvero il costo dei dispositivi, il consumo energetico dei dispositivi e reti in grado di supportare un numero elevato di dispositivi con un'elevata copertura.

Argomenti

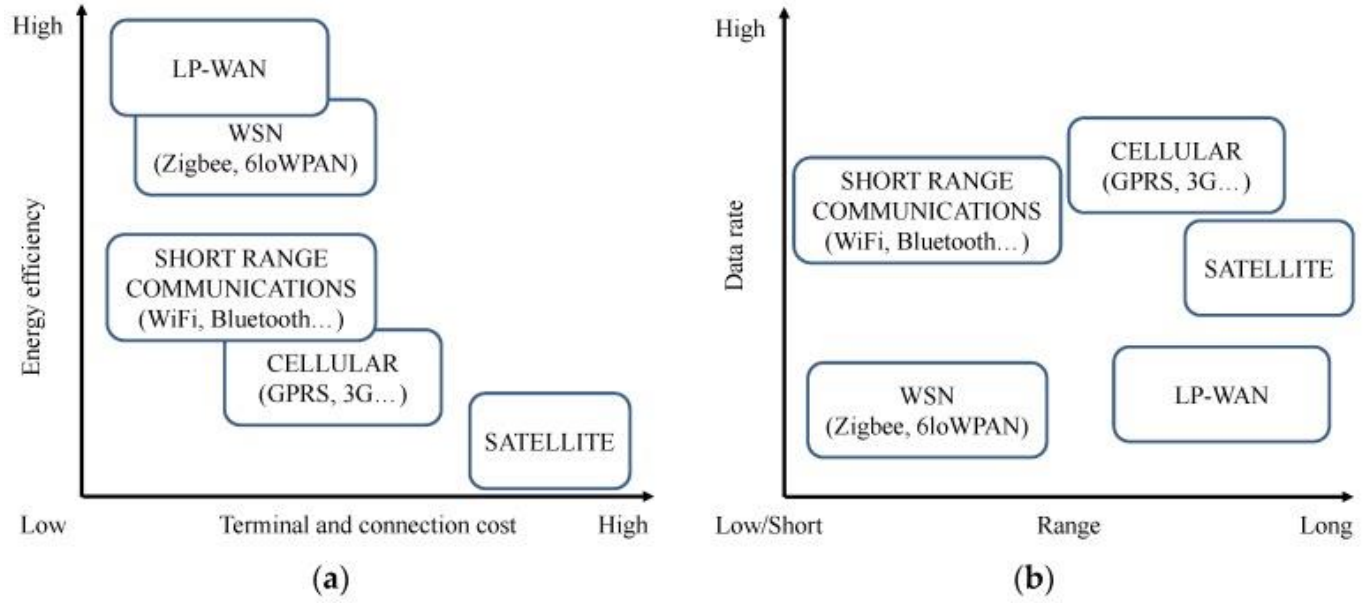
Applicazioni IoT e tecnologie LPWAN

In generale le tipiche applicazioni IoT non necessitano di trasmissioni dati continue, ma solo a fronte di variazioni delle grandezze misurate e non richiedono bitrate elevati. Tali caratteristiche vengono soddisfatte dalle tecnologie di rete **LPWAN (Low Power Wide Area Networks)** che richiedono una ridotta potenza di trasmissione e garantiscono una buona copertura e scalabilità

Al momento si stanno diffondendo due tecnologie LPWAN: **LoRa** basa su standard aperto aperto e **SIGFOX** basata su tecnologia proprietaria. Di seguito un confronto tra le tecnologie LPWAN e le altre tecnologie a radiofrequenza pubblicato sul sito Techplayon nell'articolo Low Power Wide Area Networks (LPWAN) del 12 giugno 2017 da cui emerge come le tecnologie LPWAN al momento offrano il miglior compromesso in termini di copertura, consumo energetico e costi dei dispositivi.



Di seguito una classificazione delle principali caratteristiche delle tecnologie abilitanti per l'IoT in base all'efficienza energetica rispetto al costo per terminale di trasmissione (a) e in base alla velocità di trasmissione rispetto alla distanza di trasmissione (b) (fonte State of the Art in LP-WAN Solutions for Industrial IoT Services):



Nella seguente tabella la previsione della diffusione delle tecnologie abilitanti per l'IoT pubblicata dal SNS Research nel report [The LPWA (Low Power Wide Area) Networks Ecosystem: 2017 – 2030] pubblicato a novembre 2016:

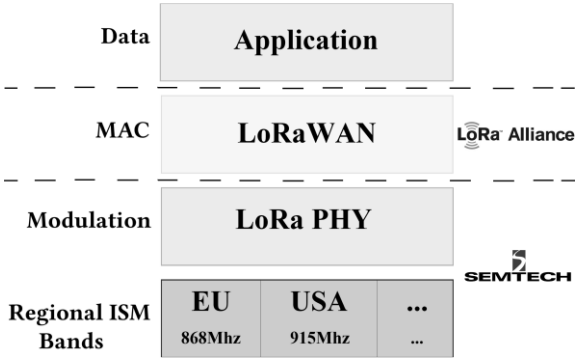
Global Wide Area M2M Connections by Technology: 2015 - 2030 (Millions)										
Technology	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2030**
2G & 3G Cellular	268	316	373	440	520	613	723	716	709	654
LTE & 5G Cellular	7	14	27	52	101	197	385	423	466	998
Satellite	4	5	6	7	9	10	11	13	14	33
LPWA	13	57	129	222	387	602	878	1'321	1'844	7'192
Wireline	122	131	141	151	163	175	186	193	199	263
Others	101	103	104	105	106	108	109	110	111	123
Total	**516**	**625**	**780**	**978**	**1'286**	**1'705**	**2'293**	**2'776**	**3'344**	**9'262**

Di seguito un sintetico confronto delle principali caratteristiche delle varie tecnologie LPWAN:

Caratteristica	Sigfox	LoRaWAN	NB-IoT
Modulazione	BPSK	CCS	QPSK
Frequenza	Banda libera 868 Mhz EU 915 Mhz USA 433 Mhz Asia	Banda libera 868 Mhz EU 915 Mhz USA 433 Mhz Asia	Banda licenziata LTE
Larghezza di Banda	100 Hz	250 kHz – 125 KHz	200 KHz
Data rate massimo	100 bps	50 kbps	200 kbps
Bidirezionale	Limitato /Half duplex	Si /HalfDuplex	Si /HalfDuplex
N° max di messaggi giornalieri	140	Illimitati	Illimitati
Range	10 km area urbana 40 km area rurale	5 km area urbana 20 km area rurale	1 km area urbana 10 km area urbana
Immunità a intereferenze	Molto alta	Molto alta	Bassa
Autenticazione e cifratura	No	Sì	No
Adaptive data rate	No	Sì	No
Localizzazione	Sì	Sì	No
Reti private	No	Sì	No
Standardizzazione	Sigfox company	LoRa-Alliance	3GPP

Panoramica sulla tecnologia LoRa

LoRa (Long Range) è una tecnologia che fa riferimento ad uno **stack composto da due livelli**. Il primo livello dello stack LoRa è il physical layer (PHY) ovvero lo **strato fisico** che utilizza una modulazione proprietaria derivata dal **Chirp Spread Spectrum (CSS)** mentre il secondo livello è il **protocollo per il livello MAC** (Media Access Control) chiamato **LoRaWAN**.



Physical Layer di LoRa

La tecnologia del physical layer è stata sviluppata e brevettata da Cycleo, una società francese, che nel 2012 è stata acquisita dalla californiana Semtech, per i dettagli sulla modulazione LoRa si veda il documento AN1200.22 - LoRa Modulation Basics.

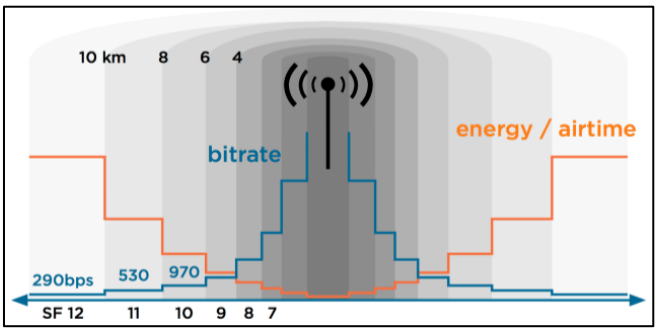
La modulazione CSS codifica i dati con un segnale sinusoidale con la frequenza variabile nel tempo, in questo modo si trasmette un segnale di base su una banda più ampia ottenendo un aumento della resistenza al rumore. Una caratteristica della modulazione CSS è l'utilizzo dello Spreading Factor (SF) che in base alla Bandwidth (BW), ovvero la larghezza di banda, permette di regolare il Bit Rate (Rb), ovvero la velocità in bit, e quindi la durata della trasmissione e di conseguenza anche i consumi di energia tramite la seguente formula:

$$R_b = SF * \frac{1}{\left[\frac{2^{SF}}{BW}\right]} \; bits/sec$$

Where:

SF = spreading factor (7..12)

BW = modulation bandwidth (Hz)



Durante la comunicazione le frequenze utilizzate ed il Data-Rate vengono modificate in base alle esigenze e alla distanza utilizzando il meccanismo dell'**Adaptive Data Rate (ADR)** che permette di aumentare l'efficienza energetica e di conseguenza la durata delle batterie. L'ADR può essere utilizzato solo da nodi statici in quanto in assenza di movimento è possibile determinare se la comunicazione a radiofrequenza è instabile.

Inoltre il canale selezionato viene cambiato in maniera casuale ad ogni nuova comunicazione, in modo da rendere la rete meno soggetta alle interferenze e se il nodo è servito da più gateway riduce la potenza di trasmissione in modo che il segnale sia ricevuto da meno gateway.

LoRa utilizza le bande di frequenza ISM (Industrial, Scientific and Medical) riservate alle applicazioni di radiocomunicazioni non commerciali, ma per uso industriale, scientifico e medico. In particolare, a seconda dell'area geografica e delle relative regolamentazioni, le due frequenze più diffuse sono **868 MHz in Europa** e 915 MHz in Nord America.

Di seguito le specifiche di LoRa per l'Italia e l'Europa (a riguardo si vedano le LoRaWAN™ Regional Parameters v1.1rB):

Country name	Band / channels	Channel Plan	Common Name	Regulatory document
Italy	433.05 - 434.79 MHz	EU433	EU433	CEPT Rec. 70-03
	863 - 870 MHz	EU863-870	EU868	Piano nazionale ripartizione frequenze

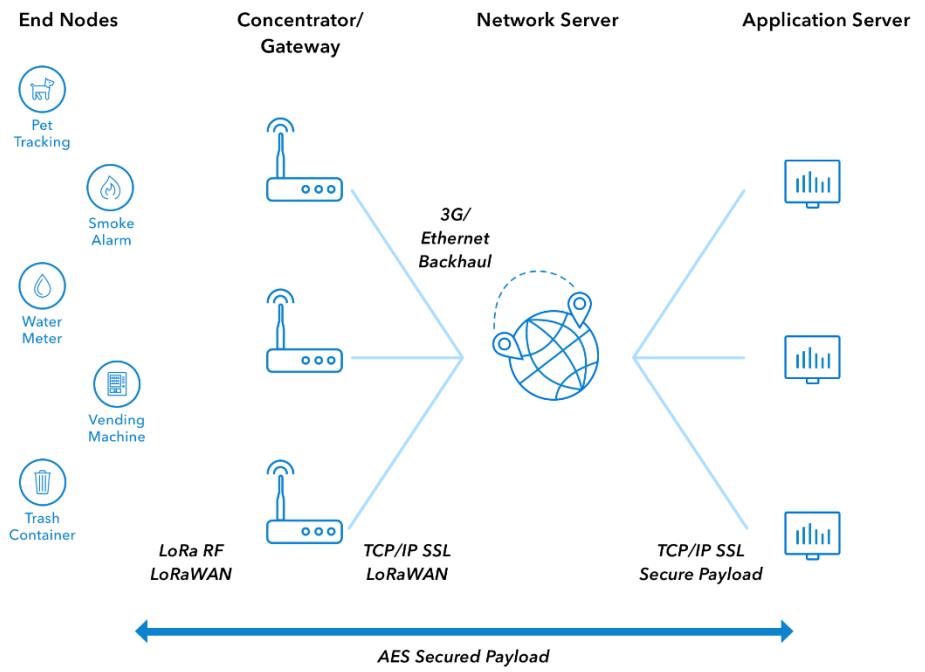
Specifiche	EU868
Banda di frequenza	867-869 MHz
Canali	10
BW canale uplink	125/250 kHz
BW canale downlink	125 kHz
Potenza TX uplink	+14 dBm
Potenza TX downlink	+14 dBm
SF uplink	7-12
Velocità di trasmissione	250 bps - 50 kbps

Protocollo LoRaWAN

Il protocollo per il livello MAC che usa LoRa come livello fisico e di tipo aperto ed è denominato LoRaWAN. Le specifiche di LoRaWAN sono redatte dalla LoRa Alliance, un'associazione no-profit fondata da varie aziende nata nel marzo 2015 che al momento conta circa 500 membri tra cui IBM, Cisco, HP, Foxconn, Semtech e Sagemcom con l'obbiettivo di standardizzare il protocollo e diffonderlo.

Al momento le specifiche LoRaWAN hanno raggiunto la versione 1.1, ma va precisato che una rete **LoRaWAN 1.1 è retro compatibile** ed in grado di interoperare anche con device legacy LoRaWAN 1.0.x. La LoRa Alliance prevede anche una certificazione LoRaWAN per i dispositivi che ne garantisce l'interoperabilità e la conformità su qualsiasi rete LoRaWAN confermando che il dispositivo soddisfa i requisiti funzionali delle specifiche del protocollo LoRaWAN.

L'architettura di rete LoRaWAN utilizza una **topologia a stella** in cui ciascun nodo finale comunica con più gateway che comunicano con il server di rete. Gli elementi principali della rete sono: i nodi, i gateway, il Network Server e l'Application Server. Di seguito uno schema dell'architettura di rete LoRaWAN:



La tecnologia LoRa prevede una **comunicazione di tipo bidirezionale**, ma la trasmissione da nodo a gateway o **messaggio di Uplink** è quella più frequente rispetto a quella da gateway a nodo o **messaggio di Downlink** dal momento che solitamente lo scopo dei nodi è quello di raccogliere dati per poi mandarli al Network Server e quindi all'Application Server.

I nodi inviano messaggi di Uplink ai gateway in radiofrequenza attraverso la modulazione LoRa. **I gateway inoltrano i messaggi al Network Server** aggiungendo informazioni riguardanti la qualità della comunicazione **attraverso una connessione IP** instradata su Ethernet, Wi-Fi o 3G.

I nodi inviano messaggi in Uplink a tutti i gateway nel loro raggio di trasmissione in modalità broadcast, il **Network Server** si occupa della **gestione dei messaggi di Uplink duplicati** e della **selezione del miglior gateway da utilizzare nel caso debba essere invito un messaggio di Downlink** al nodo.

Il Network Server si occupa anche di gestire la velocità di trasmissione dei nodi tramite il meccanismo dell'ADR (Adaptive Data Rate) per massimizzare la capacità della rete ed estendere la durata della batteria del nodo. Ad esempio il Network Server TTN utilizza i 20 messaggi di Uplink più recenti, a partire dal momento in cui viene impostato il bit ADR, per determinare il Data Rate ottimale, tali misurazioni contengono il frame counter, il rapporto segnale-rumore (SNR) e il numero di gateway che hanno ricevuto ciascun messaggio di Uplink.

L'Application Server si occupa invece di ricevere e analizzare i dati inviati dai nodi **e di determinare le azioni** che dovranno essere eseguite dai nodi.

Classi LoRaWAN

Il livello MAC implementato originariamente su ogni dispositivo LoRa si basa sul protocollo ALOHA puro, ovvero, come detto precedentemente, i nodi inviano messaggi in Uplink a tutti i gateway in ascolto instaurando una comunicazione di tipo broadcast.

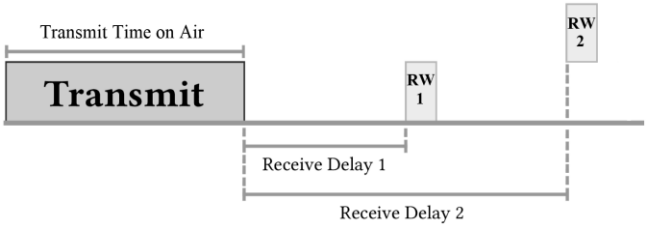
Quando un messaggio di Uplink viene ricevuto da un gateway questo invia un messaggio di acknowledgement che conferma la ricezione del messaggio. **Se due messaggi in Uplink vengono inviati nello stesso canale nello stesso istante si verifica una collisione e entrambi i messaggi di Uplink vengono persi**, anche se i frame non si sovrappongono completamente. Quando si verifica una collisione il gateway non invia alcun messaggio di acknowledgement e quindi i nodi attendono un tempo casuale prima di tentare di inviare nuovamente il messaggio in Uplink.

Partendo dalla comunicazione basata sul protocollo ALOHA puro il protocollo LoRaWAN è stato sviluppato in modo da garantire maggiore elasticità nella trasmissione. **Le specifiche di LoRaWAN definiscono tre tipologie di nodi**: nodi di **classe A**, di **classe B** e di **classe C**. **Tutti i dispositivi compatibili LoRaWAN devono implementare la classe A, mentre le classi B e C rappresentano delle estensioni**.

Nodi di classe A

Rappresenta la **modalità di default** dei nodi in cui **i nodi supportano la comunicazione bidirezionale con il gateway, ma questa viene sempre inizializzata dai nodi in maniera asincrona**.

I messaggi in Uplink, dal nodo al gateway, possono essere inviati in qualsiasi momento. **A seguito di un messaggio di Uplink il nodo apre due finestre di ricezione**. Il Network server può rispondere tramite un gateway con un messaggio in Downlink in una delle due finestre. Solitamente la prima finestra è aperta sullo stesso canale utilizzato nella trasmissione in Uplink, mentre la seconda finestra viene aperta su un canale differente, accordato in precedenza con il Network Server, per migliorare la resistenza alle interferenze.

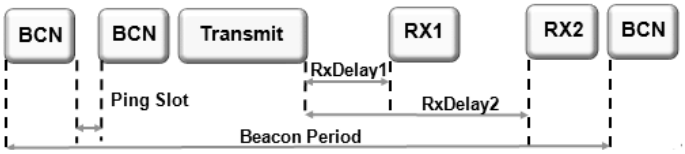


Questa classe è la più efficiente dal punto di vista energetico ed è utilizzata da quei nodi che cercano di rimanere inattivi per un tempo più lungo tempo possibile, ed in cui le comunicazioni in Uplink sono le più frequenti, come ad esempio nei sensori.

Nodi di classe B

I nodi in classe B estendono le funzionalità della classe A implementando delle finestre di ricezione programmate per i messaggi di Downlink inviati da Network Server tramite i gateway. Tramite l'utilizzo di segnali temporizzati trasmessi dal gateway, i nodi aprono periodicamente delle finestre di ricezione consentendo quindi l'invio di messaggi in Downlink ai nodi indipendentemente dal fatto che siano stati inviati messaggi in Uplink dai nodi.

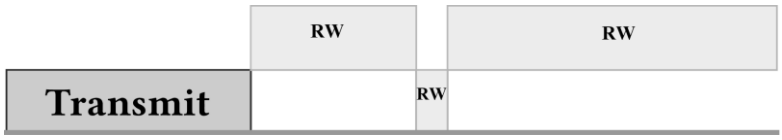
Scendendo nel dettaglio i nodi sono sincronizzati con il Network Server attraverso un meccanismo che sfrutta dei pacchetti beacon trasmessi dai gateway ogni 128 secondi. Un pacchetto beacon contiene uno specifico tempo di riferimento in cui far aprire ai nodi della rete una finestra di ricezione extra, chiamata ping slot.



Questa classe è utilizzata da quei nodi che hanno la necessità di ricevere dei comandi, come ad esempio gli attuatori.

Nodi in classe C

I nodi in classe C estendono le funzionalità della classe A implementando una finestra di ricezione sempre aperta, a meno che il nodo non stia trasmettendo. Questo permette una comunicazione con bassa latenza, ma va ad aumentare molto il consumo di energia rispetto ai nodi in classe A.



Questa classe è utilizzata da quei nodi che in cui la ricezione di comandi deve rispettare vincoli dal punto di vista temporale. Questa operatività si traduce in un **elevato consumo energetico** che rende solitamente necessario che questi nodi siano connessi alla rete elettrica.

Attivazione dei nodi in una rete LoRaWAN

Ogni nodo di una rete LoRaWAN dispone delle seguenti informazioni:

- l'**indirizzo identificativo del device** denominato **DevAddr** (Device Address) che identifica il nodo nella rete e si compone di **32 bit**, di cui i sette più significativi identificano la rete mentre i rimanenti sono assegnati in maniera arbitraria dal Network Server;
- un **identificativo di applicazione** denominato **AppEUI** (Application Identifier) composto da **64 bit**. Questo è l'identificativo esclusivo dedicato al proprietario dell'applicazione a cui è assegnato il dispositivo, l'AppEUI è conservato all'interno del dispositivo
- una **chiave di sessione di rete** denominata **NwkSKEY** (Network Session Key), questa chiave **AES-128 bit** è specifica per il nodo ed è utilizzata dal Network Server e dal device per generare il MIC (Message Integrity Code) per il controllare l'integrità del messaggio e per criptare e decriptare il FRMPayload (Frame Payload).
- una **chiave di sessione per l'applicazione** denominata **AppSKey** (Application Session Key), questa chiave **AES-128 bit** è specifica per il dispositivo ed è utilizzata dall'Application Server e dal nodo per criptare e decriptare il payload dei messaggi specifici di un'applicazione in modo da creare un canale di comunicazione sicuro end-to-end

LoRaWAN rende disponibili due modalità per associare un nodo alla rete: la modalità **Over-The-Air Activation (OTAA)** e la modalità **Activation By Personalization (ABP)**.

Modalità Over-The-Air Activation (OTAA)

Nella modalità Over-The-Air Activation (OTAA) **i nodi devono eseguire una procedura di join** prima di poter scambiare dati con il Network Server. La procedura di join deve essere eseguita nuovamente ogniqualvolta le informazioni riguardo la sessione vengano perse.

Per eseguire la procedura di join il nodo deve possedere:

- un **DevEUI** di **64 bit** che **identifica globalmente il nodo**;
- un **AppEUI** di **64 bit** che **identifica l'applicazione**;
- una **chiave AES-128** denominata **AppKey**;

La chiave AppKey sarà utilizzata per generare la chiave di sessione di rete NwkSKEY e la chiave di sessione per l'applicazione AppSKey.

La procedura di join consiste in un messaggio MAC di join request tramite cui un nodo invia anche il proprio DevEUI e l'AppEUI, di seguito la struttura del messaggio di join request:

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

Al messaggio MAC di join request **il Network Server risponde con un messaggio MAC di join accept** inviando al nodo il DevAddr e un valore casuale chiamato AppNonce utilizzato dal nodo per ricavare l'AppSKey e la NwkSKEY. Di seguito la struttura del messaggio di join accept:

Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

Modalità Activation By Personalization (ABP)

Nella modalità Activation By Personalization (ABP), **i nodi non devono eseguire una procedura di join** inviando messaggi MAC request-join accept, come descritto precedentemente, **perché l'indirizzo identificativo del device DevAddr, la chiave di sessione di rete NwkSKey e la chiave di sessione per l'applicazione AppSKey sono memorizzate direttamente nel nodo**. In altre parole in questa modalità il nodo possiede già le informazioni necessarie per associarsi ad una rete LoRaWAN.

Attivazione dei nodi e sicurezza

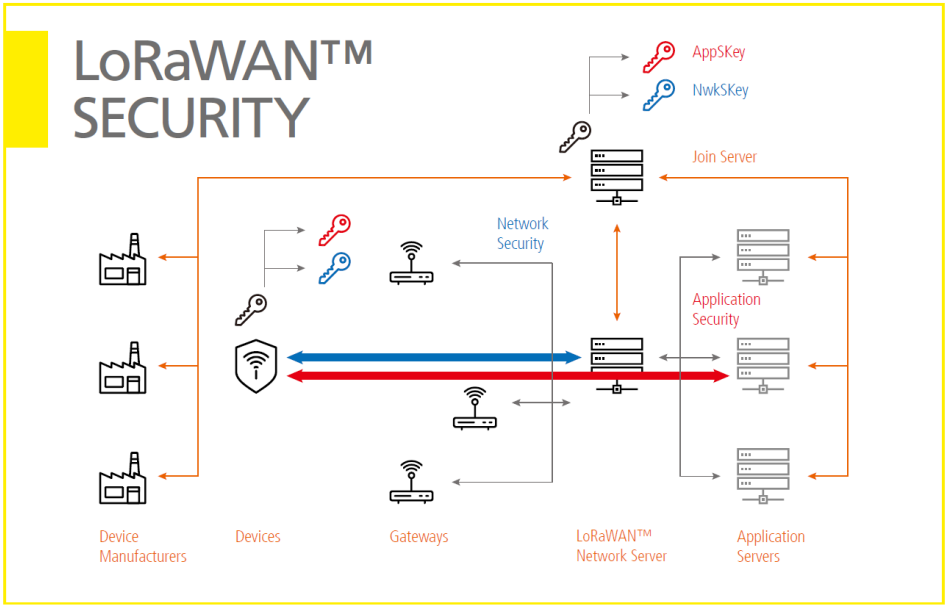
E' importante che ogni nodo abbia un set di chiavi NwkSKey e AppSKey uniche in modo che le chiavi di un nodo vengono compromesse non venga anche compromessa la sicurezza degli altri nodi della rete come riportato nelle LoRaWAN Specification v1.0:

> *"Each device should have a unique set of NwkSKey and AppSKey. Compromising the keys of one device shouldn't compromise the security of the communications of other devices.*
>
> *The process to build those keys should be such that the keys cannot be derived in any way from publicly available information (like the node address for example)."*

Inoltre occorre tenere presente **sebbene la modalità di attivazione Activation By Personalization (ABP) sia più semplice da implementare**, l'hardcode nel dispositivo del DevAddr e delle chiavi di sicurezza NwkSKey e AppSKey **implica una minor sicurezza**. I nodi infatti sono spesso posizionati in ambienti fisici non controllabili e quindi potrebbero essere oggetto di furto col conseguente rischio che le chiavi vengano estratte dal noto. Nel caso in cui le chiave siano derivate in base al nodo ad esempio basandosi sul suo indirizzo la compromissione di tali chiavi tramite reverse engineering implica anche la compromissione delle chiavi degli altri nodi. A riguardo si veda ad esempio la whitepaper LoRa Security Building a Secure LoRa Solution pubblicata da MWR Labs:

> *"Key extraction from Node devices is probable given that they will likely be physically outside of controlled environments. It is important therefore that the theft of keys from one Node does not compromise other Nodes in the system.*
> *One potential vulnerability is where Nodes use Activation-By-Personalisation (ABP) for joining, but use keys derived by the Node based on features such as the device address. If this could be worked out through reverse engineering of one Node, then all other communications to any Node would then be compromised."*

Di seguito l'architettura di sicurezza di LoRaWAN tratto dalla LoRa Alliance Security Whitepaper:



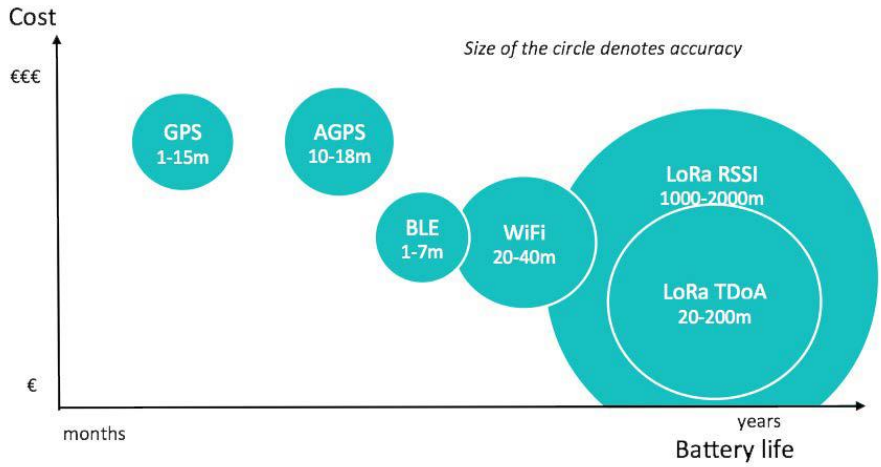
Geolocalizzazione

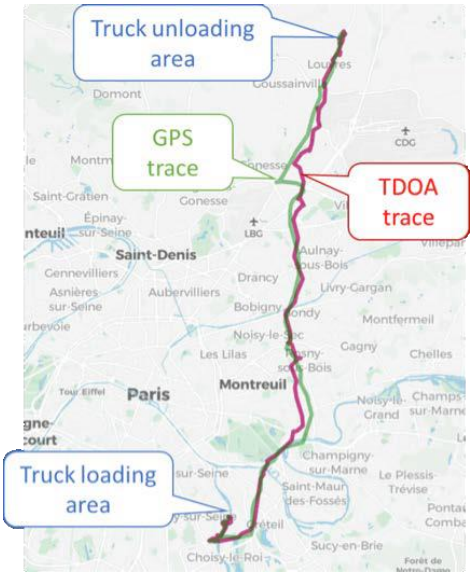
Come descritto nella [LoRa Alliance Geolocation Whitepaper] pubblicata dalla LoRa Alliance, LoRaWAN fornisce nativamente la funzionalità di geolocalizzazione che è supportata da ogni tipo di nodo senza richiedere ulteriore potenza di calcolo.

Sono disponibili due metodologie per la geolocalizzazione:

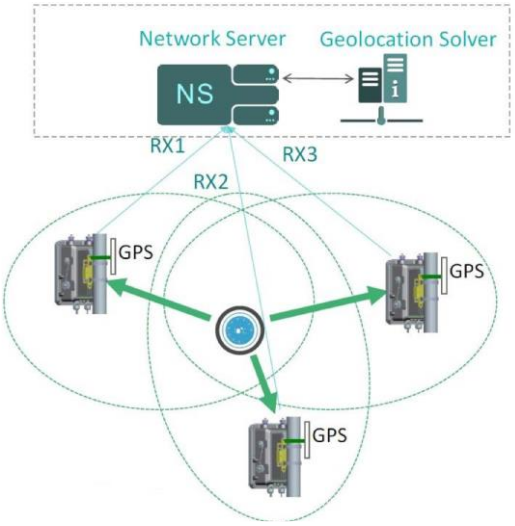
- un **primo metodo basato sul Received Signal Strength Indication (RSSI)**, ovvero sulla misurazione della potenza del segnale ricevuto, **che fornisce un rilevamento della posizione indicativa con un'accuratezza compresa tra 1000-2000m**;
- un **secondo metodo basato sul Time Difference Of Arrival (TDOA)**, ovvero sulla misurazione della differenza del tempo di arrivo del segnale, **che fornisce un rilevamento della posizione precisa con un'accuratezza 20-200m**.

Nel seguente grafico un confronto tra le vare tecnologie di localizzazione e un confronto tra localizzazione tramite GPS con LoRaWAN TDOA tratto da un caso reale:





Un nodo di una rete LoRaWAN può essere localizzato se le sue trasmissioni in Uplink sono ricevute da tre o più gateway, in generale la precisione della geolocalizzazione migliora al crescere del numero di gateway.

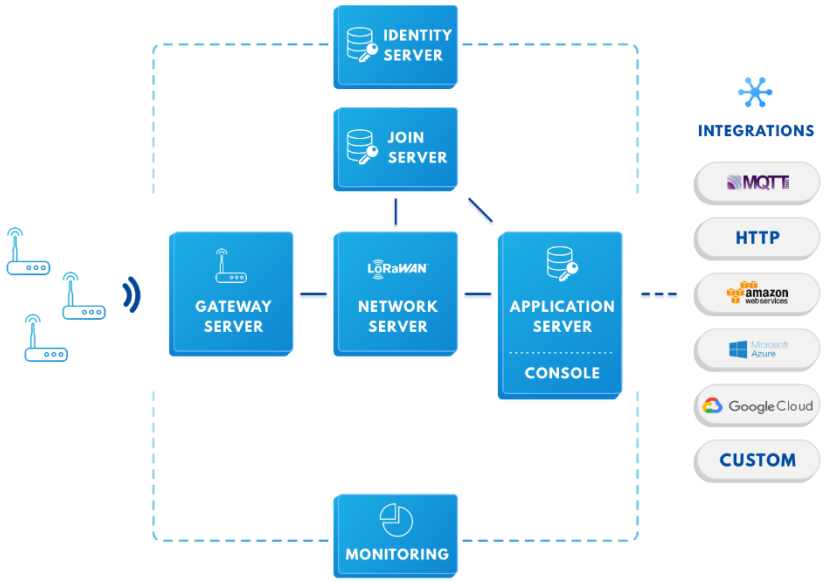


Quando diversi gateway ricevono contemporaneamente lo stesso messaggio di uplink possono rilevare la posizione del nodo tramite tecniche di multilaterazione.

Affinchè sia possibile geolocalizzare i nodi tramite TDOA è necessario che I gateway abbiano una sincronizzazione temporale accurata ottenuta tramite un GPS sui gateway o con un altro mezzo che consenta di sincronizzare il clock dei gateway con differenze di poche decine di nanosecondi.

Network Server e Application Server offerti da The Things Network (TTN)

Uno dei primi progetti che ha avuto come obbiettivo quello creare un LoRaWAN network server stack, ovvero un'infrastruttura di gestione per reti LoRa e un Frontend applicativo, è The Things Network (TTN). TTN è nato nell'agosto 2015 con una prima sperimentazione ad Amsterdam in un progetto per la cura e la gestione delle imbarcazioni nei canali, di seguito lo schema del Things Network LoRaWAN Stack:



Come enunciato nel Manifesto della comunità The Things Network si propone di costruire una rete per l'IoT completamente aperta, decentralizzata, posseduta e gestita dagli utenti. Per realizzare tale obbiettivo i codici, i firmware, i progetti e le conoscenze per la produzione dei dispositivi fisici necessari alla rete sono open source.

E' possibile eseguire il **deploy del Things Network LoRaWAN Stack in 4 modalità**:

- **Public Community Network**: in questa modalità è possibile utilizzare **una rete decentralizzata e collaborativa** a cui sono connessi migliaia di gateway in tutto il mondo, utilizzati da sviluppatori e aziende per creare use cases. E' possibile utilizzare i gateway già installati o aggiungere gateway aggiuntivi se è necessaria una copertura aggiuntiva. Al link The Things Network in Italy è possibile avere l'elenco delle community TTN italiane, al momento vi sono in Italia 28 community e 170 gateway.
- **Software as a Service**: in questa modalità è possibile creare una **rete LoRaWAN privata** con la possibilità interconnettersi con la rete pubblica, ovvero il peering con la Public Community Network. Questa modalità è fornita a pagamento da The Things Industries con un Service Level Agreement (SLA) e un uptime guarantito nei livelli di servizio Professional e Service Provider.
- **Private Cloud**: in questa modalità è **possibile mantenere il Network Server in un'infrastruttura privata on-premises** per poter mantenere il controllo sulla distribuzione, la qualità del servizio (SLA e uptime) e il livello di sicurezza e per evitare che i dati abbandonino il proprio dominio. Questa modalità è fornita a pagamento da The Things Industries nei livelli di servizio Enterprise e Service Provider.
- **On-Site**: in questa modalità è possibile creare **reti carrier-grade on-site** in cui i dati non abbandonano mai il sito fisico installando il Network server sul gateway stesso o realizzare reti offline. Questa modalità è fornita a pagamento da The Things Industries nei livelli di servizio Enterprise e Service Provider.

Al momento il Things Network LoRaWAN Stack è giunto alla terza versione (V3) in cui è stato reso disponibile il supporto nativo a LoRaWAN 1.1, la possibilità di utilizzare lo stack per l'implementazione di reti private sia in private cloud o on-premises, la possibilità di eseguire il peering tra reti pubbliche e private, servizi aggiuntivi come LoRaWAN FOTA (LoRa Firmware-over-the-Air), monitoring e alerting, multi-tenancy, multi-region private deployments.

Nel post The Things Network Stack V3 Update sono stati fornite maggiori informazioni sulle novità della V3 e la previsione di quando alcune di esse saranno disponibili:

	Private gateways	Multi-tenant	Multi-region	Auto-scaling	FOTA	SLA	Support	Availability
Hosted	Y	Y	Y	Y	Y	Y	Y	2019 Q1
Private Cloud	Y	N	Y	Y	Y	N	Y	2019 Q1
Images and Binaries	Y	N	Y	Y*	Y	N	Y	2018 Q4
Open Source	Y	N	Y	N	N	N	Y	2018 Q4
Community Network	N	N	Y	Y	N	N	N	2019 Q1

*** not yet in MVP (Minimum Viable Product)**

- ***Hosted*** *is our flagship V3 SaaS offering; fully featured, hosted and SLA backed*
- ***Private Cloud*** *is the V3 Stack in your own AWS, Azure or GCP account, with integrations with their IoT platforms*
- ***Images and Binaries*** *allow for deploying the V3 Stack on-premises, on various architectures, enabling single binary deployments on gateways to custom Kubernetes deployments in the cloud*
- ***Open Source*** *allows you to compile from source and run the Stack on your development machine*
- ***Community Network*** *is the free to use The Things Network public community network*

Per quanto riguarda la creazione di Applicazioni in TTN questo è possibile tramite vari approci:

- **Data API**: consentono di ricevere eventi e messaggi dai device e di inviare messaggi ai device. E' possibile utilizzare le Data API tramite:
  - SDKs & Libraries che mettono a disposizione TTN Client per Go, Java, Node-RED, Node.js e Python
  - MQTT (Message Queue Telemetry Transport) un protocollo per connettività machine-to-machine (M2M) / IoT che è stato progettato per il trasporto in modo leggero di messaggi publish/subscribe. TTN è in grado di utilizzare MQTT per la pubblicazione dell'attivazione dei device, dei messaggi dei device e dei messaggi di risposta a device tramite librerie MQTT Client disponibili per ogni linguaggio e piattaforma (a riguardo si veda MQTT.org Wiki e i progetti Eclipse Paho, Eclipse Mosquitto e MQTTBox)
- **Application Manager API**: che consentono la gestione di applicazioni, gateway e device tramite:
  - SDKs & Libraries che mettono a disposizione TTN Client per Go, Java, Node-RED, Node.js e Python
  - HTTP: ovvero tramite Community endpoints esposti con gRPC API o HTTP API

Firmware-over-the-Air (FOTA)

La LoRa Alliance nella pagina introduttiva About LoRaWAN prevede il **supporto alla funzionalità Firmware Over-The-Air (FOTA)** per l'aggiornamento dei firmware dei dispositivi **mediante il supporto a multicast disponibile per i nodi in classe B e C** (in cui è possibile avere un a finestra di ricezione indipendente da quella di trasmissione) descritto nelle specifiche LoRaWAN Specification v1.1 in cui viene evidenziato che le specifiche non descrivono un modo per configurare il multicast group e le chiavi di cifratura demandando questa configurazione al livello applicativo o ad una configurazione manuale sul nodo:

> ***11.2 Unicast & Multicast MAC messages***
>
> *Messages can be "unicast" or "multicast". Unicast messages are sent to a single end-device and multicast messages are sent to multiple end-devices. All devices of a multicast group must share the same multicast address and associated encryption keys. The LoRaWAN Class B specification does not specify means to remotely setup such a multicast group or securely distribute the required multicast key material. This must either be performed during the node personalization or through the application layer.*
>
> ***17.2 Class C Multicast downlinks***
>
> *Similarly to Class B, Class C devices may receive multicast downlink frames. The multicast address and associated network session key and application session key must come from the application layer.*

Nel documento tecnico LoRaWAN Remote Multicast Setup Specification v1.0.0, che definisce un application layer per lo scambio di messaggi su LoRaWAN per nodi in classe B e C, viene ribadito come una sessione multicast può essere utilizzata, ad esempio, per l'upgrade dei firmware:

> *For example, the multicast session might be used to broadcast a firmware upgrade file. In that case the end-device might end the multicast session has soon as the full file is received without waiting for TimeOut.*

Sebbene specifiche LoRa forniscano un'indicazione su come gestire il Firmware-over-the-Air with tramite LoRaWAN, va precisato che tale funzionalità presenta una serie di difficoltà:

- **le trasmissioni dei Gateway non sono coordinate**, questo significa che se il gateway invia messaggi in Downlink del firmware non può ricevere messaggi in Uplink dai nodi che andranno persi;
- **non esiste un la possibilità a livello MAC di fare in modo che i nodi in classe A possano ricevere frame multicast**, questo dipende dal fatto che il supporto multicast era stato aggiunto per i nodi in classe B e C per consentire applicazioni come il controllo dei lampioni stradali e non per trasferire aggiornamenti firmware;
- **i gateway hanno un duty cycle limitato** ovvero possono trasmettere solo per 1% del tempo, in base alla regolamentazione EU863-870 ISM ETSI (European Telecommunications Standards Institute) come riportato in LoRaWAN Regional Parameters v1.1rB per le bande di frequenza EU863-870 ISM, quindi buona parte delle risorse di trasmissione per i messaggi di Downlink sono usati per gli acknowledgements e i messaggi di controllo MAC e di conseguenza le risorse utilizzabili per il FOTA sono limitate.

La problematica dell'implementazione della funzionalità FOTA è stata anche oggetto dell'articolo Firmware Updates over Low-Power Wide Area Networks che illustra come il Nerwork Server di The Things Network (TTN) ha approcciato il problema concentrandosi su come inviare l'immagine del firmware ottimizzando il duty cycle del dispositivo e il consumo energetico sfruttando il Multicast per l'aggiornamento contemporaneo di più device per ottimizzare il duty cycle del gateway.

Un altro aspetto evidenziato nell'articolo Firmware Updates over Low-Power Wide Area Networks è quello relativo alla sicurezza. Infatti **quando più dispositivi partecipano ad una sessione multicast temporanea in cui tutti i dispositivi condividono le stesse chiavi di sessione ci si espone ad un potenziale rischio per la sicurezza se uno dei dispositivi viene compromesso** in quanto tramite le chiavi di sessione multicast un attaccante potrebbe inviare pacchetti come se provenissero dal server permettendo un attacco di tipo packet injection. Per proteggere il processo di aggiornamento l'implementazione di FOTA fatta da The Things Network (TTN) prevede tre misure di protezione:

1. **quando il file viene ricevuto il dispositivo calcola il checksum dei dati ricevuti e lo invia al server** nella sessione privata del dispositivo, il server confronta il checksum ricevuto con il checksum dei dati inviati, per verificare se i dati sono stati ricevuti correttamente o meno a causa di errori di trasmissione o manomissioni, e risponde ad ogni dispositivo in modo individuale nella sessione privata circa la correttezza del checksum;
2. **quando il server invia al dispositivo la risposta sulla correttezza del checksum invia anche il message integrity code (MIC) per garantire l'integrità del checksum inviato al dispositivo**, il MIC non può essere falsificato da nessuno che non conosca le chiavi di sicurezza della sessione sicure del dispositivo, in questo modo il server controlla il checksum del dispositivo e il dispositivo il MIC del server trasmessi nella sessione privata per convalidare il file;
3. **quando un attaccante inietta pacchetti casuali il dispositivo potrebbe non essere in grado di ricostruire l'immagine originale**, inoltre i dispositivi potrebbero esaurire l'alimentazione perché continuano a ricevere checksum che indicano che i dati ricevuti non sono corretti, **per evitare ciò la sessione multicast ha una durata** ovvero un limite fisso sul numero di messaggi e se il limite viene raggiunto il dispositivo tornerà alla sessione privata eliminando i dati.

Riferimenti

- LoRa Alliance - resource HUB
- The Things Network - Learn