Ordine degli Ingegneri della provincia di Napoli

Sistemi TLC, Sicurezza e Privacy: il ruolo degli Operatori

Napoli, 8 Marzo 2019

Seminario «Le intercettazioni telefoniche: Analisi tabulati e Geolocalizzazione»

Ing. Antonio Cimino - Vice Coordinatore Commissione ICT OIN

Le reti di telecomunicazione sono in continua evoluzione per la sempre crescente domanda di velocità di trasmissione, capacità ed efficienza di trasferimento dell'informazione per unità di banda.

GSM (Global System for Mobile communication) presente in Italia dal 1995 nella gamma 900MHz e dal 1998 nella gamma dei 1800MHz.

UMTS (Universal Mobile Telecommunications System) nella gamma dei 2100MHz con velocità di trasmissione massima in DL di 384 kbit/s, è presente in Italia dal 2003.

HSDPA (High Speed Downlink Packet Access) impiega un canale a pacchetto ad alta velocità condiviso tra più utenti e tecniche trasmissive avanzate, incrementando la velocità e riducendo la latenza. Presente in Italia dal 2006 con velocità in DL via via crescenti da 3,6Mb/s a 7,2Mb/s e 14,4Mb/s. Per finire a 21Mb/s con modulazione 64QAM e a 28Mb/s con trasmissione MIMO 2x2 ed infine 42Mb/s con tecnica Dual Carrier che affascia 2 canali UMTS (2x5MHz).

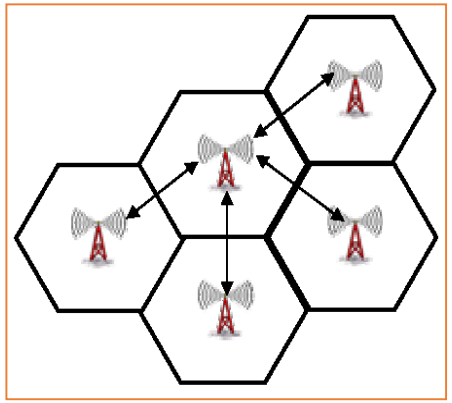
LTE (LongTerm Evolution), che consente con 20 MHz di banda e terminali di categoria 3 velocità fino a 100 Mbit/s in DL e 50 Mbit/s in UL. La latenza migliora e ciò consente servizi ad ampia interattività. Presente in Italia dal 2013 nelle gamme 800MHz, 1800MHz, 2600MHz.

Una rete radiomobile cellulare è costituita da:

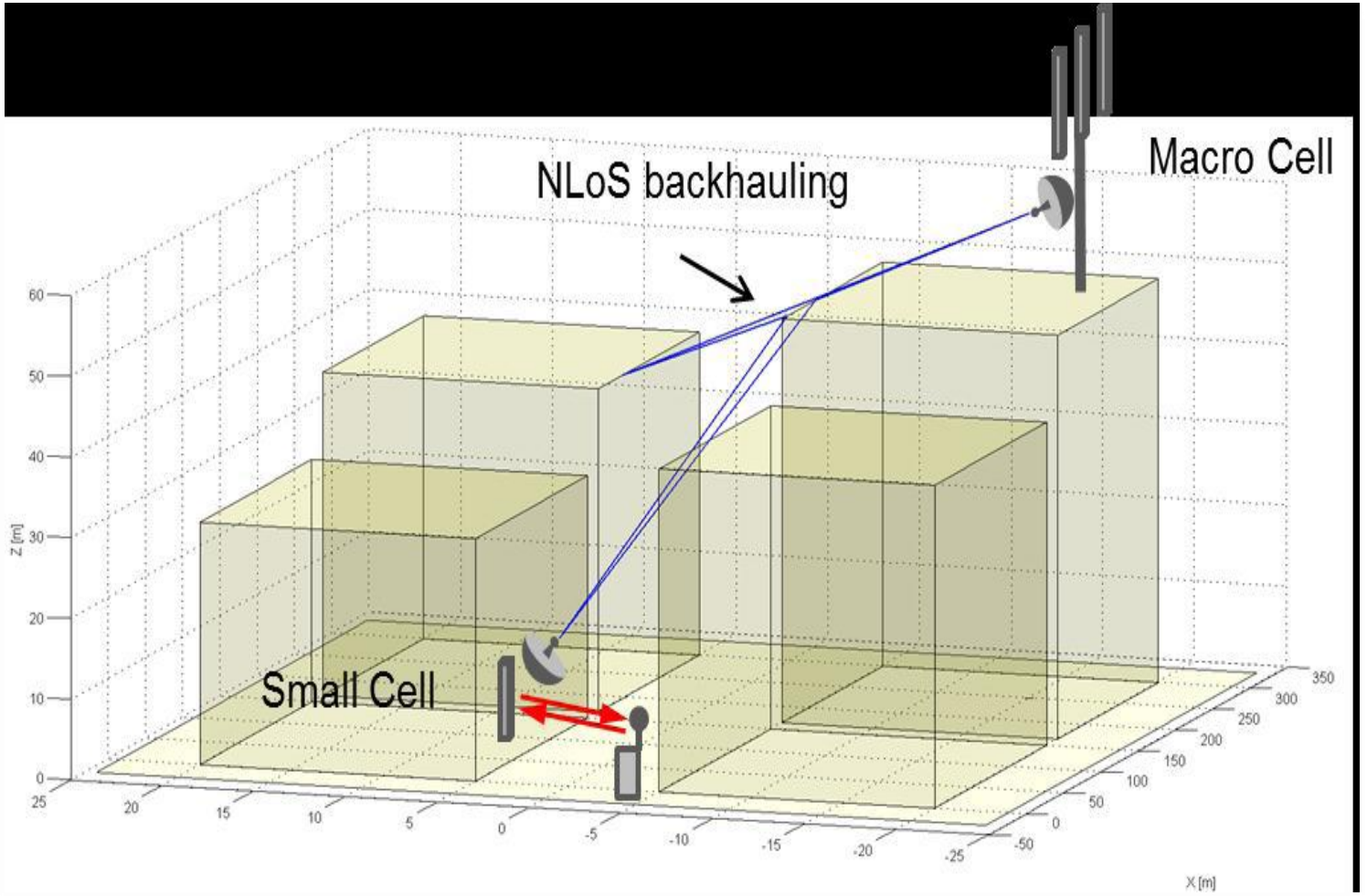
> Nodi di Accesso Radio, che tramite le antenne collegano i terminali

> Nodi di Core Network che svolgono la funzione di commutazione

> Collegamenti Trasmissivi (backhauling) che connettono i Nodi Radio ai nodi di Core.

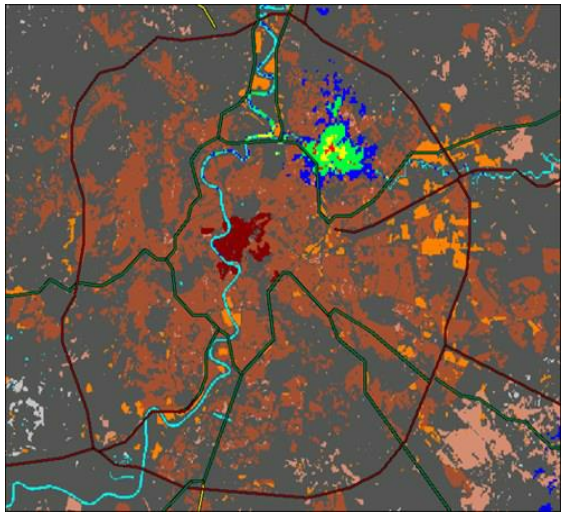


Una cella che copre un territorio ad alta densità di traffico (es. urbana) avrà una superficie minore di quella che ne copre uno a bassa densità (es. rurale) Rif. Macrocella (1-30km) , Microcella, (0,2-2 km), Picocella (20-200mt), Femtocella (10m).


NLoS backhauling
Macro Cell
Small Cell
Z [m]
X [m]
60
50
40
30
20
10
0
25
20
15
10
5
0
-5
-10
-15
-20
-25
-50
0
50
100
150
200
250
300
350

Gli elementi utilizzati per **calcolo della copertura** di un impianto (BTS) sono i seguenti:

> la posizione dell'impianto (coordinate geografiche);
> le principali caratteristiche strutturali (altezza dal suolo, orientamento delle antenne, tipo di antenna, potenza irradiata, etc);
> l'orografia del territorio;
> la classificazione del territorio in base al suo utilizzo (morfoclassi); (es. urba-nizzato denso, suburbano, foresta, area aperta, mare, etc);
> mappa di distribuzione della popolazione;
> poligoni dei confini amministrativi : nazionali, regioni, province, comuni.



Nel simulatore, il territorio è rappresentato come una fotografia digitale in cui ogni pixel è un quadrato di dimensione prestabilita (tipicamente 100m x 100m); per ciascun elemento di territorio conosciamo quindi sia l'altezza sul livello del mare che la sua classificazione.
I più comuni modelli matematici di propagazione del segnale radiomobile considerano di base una legge logaritmica di riduzione della potenza al crescere della distanza dall'impianto, introducendo però dei fattori correttivi per tenere in considerazione la frequenza di trasmissione, l'orografia e la classificazione del territorio.

In base ai criteri di progettazione, che variano per ciascuna tecnologia (2G, 3G, 4G), si sceglie il livello di segnale minimo al di sotto del quale il pixel non si considera più coperto, o meglio, servito.

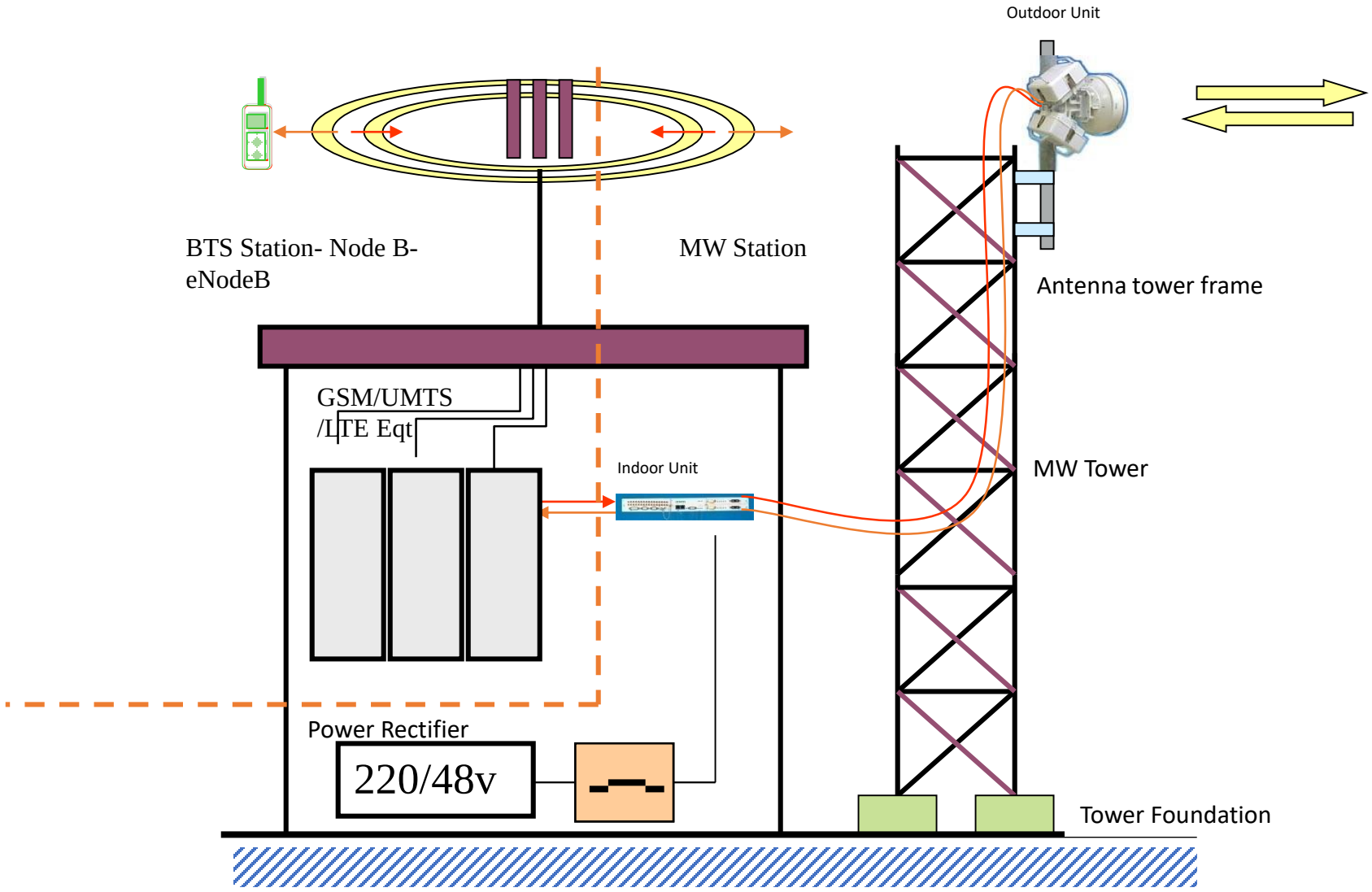
Al termine della simulazione possiamo quindi conoscere la copertura offerta dall'impianto in tutti i pixel circostanti. Vengono impiegati colori diversi per rappresentare le diverse soglie di intensità del segnale ricevuto.

Per l'impostazione dei principali parametri del modello (tuning) ci si basa sui risultati di apposite misurazioni effettuate in campo sui livelli di segnale effettivamente ricevuto.

Una volta ottenuta la copertura di ciascun impianto il software provvede a costruire la mappa complessiva di copertura del territorio prendendo per ciascun pixel il livello massimo tra i segnali ricevuti. La percentuale di territorio coperto si ottiene quindi semplicemente dividendo il numero di pixel coperti per il numero totale di pixel che rappresentano il territorio nazionale.

Per la stima della popolazione coperta occorre infine una mappa della popolazione, che viene costruita a partire dai dati ISTAT relativi all'ultimo censimento. Una volta nota la popolazione presente in ciascun pixel ed i confini amministrativi è sufficiente sommare la popolazione presente nei soli pixel coperti per calcolare le percentuali di copertura di popolazione e territorio.

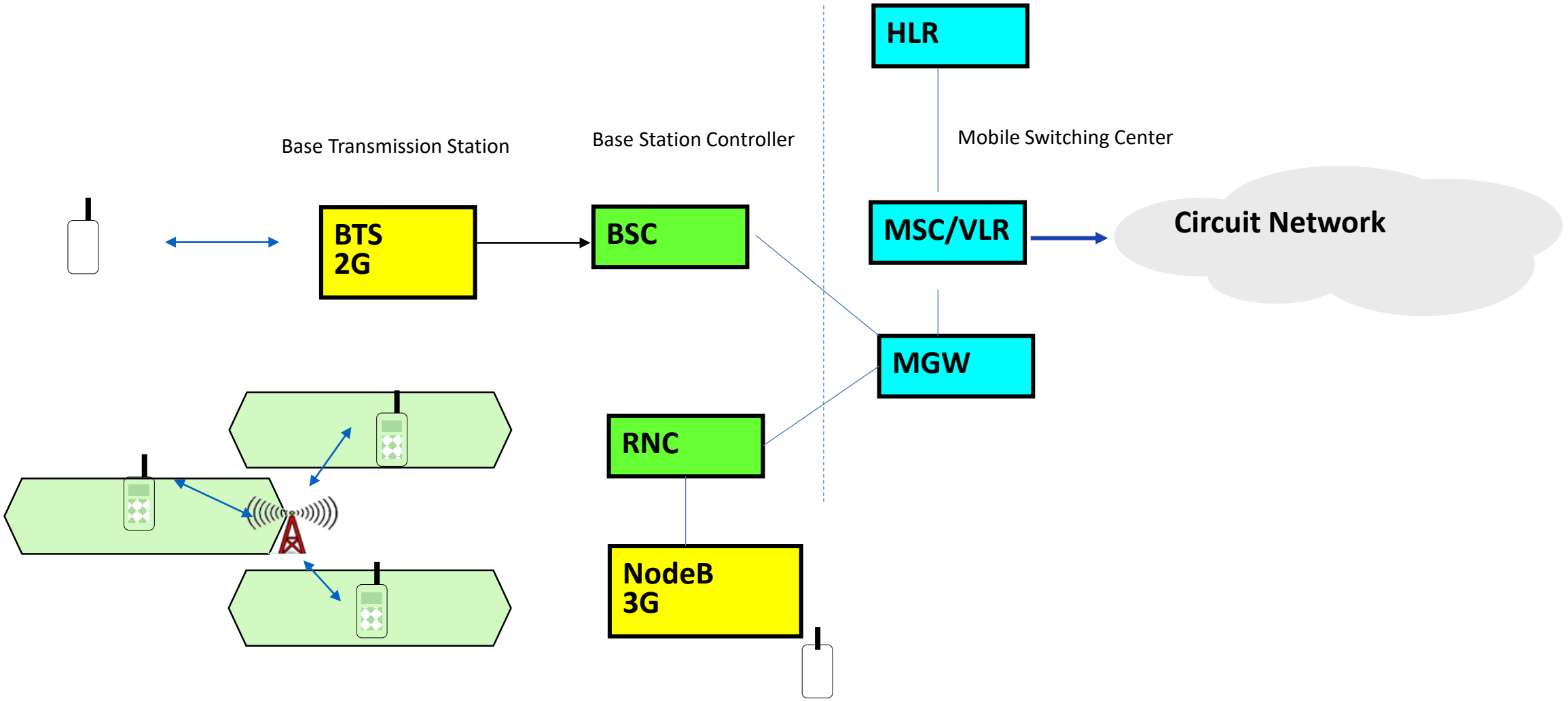
E' corretto parlare di validità statistica: le percentuali di copertura sono tanto più affidabili quanto più si considerano aree estese cioè con un numero di pixel elevato, mentre perdono di affidabilità su analisi puntuali riferite a singoli pixel.


Outdoor Unit
BTS Station- Node B-
eNodeB
MW Station
Antenna tower frame
GSM/UMTS
/LTE Eqt
Indoor Unit
MW Tower
Power Rectifier
220/48v
Tower Foundation

La funzionalità di Controllo della Rete Radio gestisce l'assegnazione iniziale delle risorse radio, la nuova assegnazione per *handover* (trasferimento automatico della connessione sulle risorse radio della cella di destinazione) e il rilascio finale.

Il controllo della rete radio può essere allocato in un nodo interposto fra i nodi di accesso e i nodi di commutazione (GSM e UMTS), oppure distribuito nei nodi di accesso e nei nodi di commutazione (LTE).

La creazione di una connessione fra il terminale radiomobile e un altro terminale, sia radiomobile sia fisso, compete alla funzionalità di Commutazione che provvede all'istradamento, su base selezione, fra sorgente e destinazione.


HLR
Base Transmission Station
Base Station Controller
Mobile Switching Center
BTS
2G
BSC
MSC/VLR
Circuit Network
MGW
RNC
NodeB
3G

BTS *Base Transceiver Station*

Stazione Radio Base 2G deputata alla ricetrasmissione delle comunicazioni d'utente, attraverso i sistemi di antenna e dei messaggi di segnalazione sull'interfaccia radio, alla codifica e cifratura dei segnali per assicurarne rispettivamente l'integrità e la riservatezza, alla raccolta di misure radio e di traffico ed al loro inoltro verso la rete, alla diffusione delle informazioni di sistema in broadcast.

BSC *Base Station Controller*

È il controllore della stazione radio base 2G (BTS). Amministra le risorse radio assegnando i canali per le singole connessioni, raccoglie le misure di qualità e accessibilità ed inoltra i messaggi di segnalazione scambiati tra il terminale ed i nodi più interni della rete. Gestisce poi la mobilità radio tra più stazioni radio (BTS) garantendo la continuità delle chiamate a circuito (meccanismo di handover) o delle connessioni a pacchetto (riselezione di cella)

MSC *Mobile Switching Center-Server*
Gestisce, per la componente a circuito, la mobilità su macro aree dette Location Area (nel numero di qualche unità per MSC).
È coinvolto nelle procedure cosiddette AAA (Authentication - Authorization - Accounting) per l'accesso alla rete ed ai servizi e per la tassazione. L'MSC è anche responsabile per l'handover tra BSC diversi.

RNC *Radio Network Controller*
Controllore 3G delle risorse radio con funzioni analoghe al BSC 2G

MGW e GW MSC *MSC Gateway*

I Nodi GW MSC forniscono le funzioni di instradamento e commutazione ai nodi di livello gerarchico inferiore MGW

HLR *Home Location Register*

Archivio contenente le caratteristiche anagrafiche e i profili di servizio associati a ogni SIM. Contiene anche la posizione attuale del cliente in termini di VLR Visitor Location Register, necessaria per inviare il segnale di paging (segnale di chiamata verso l'accesso radio) nella LA opportuna

La realizzazione della connessione può essere svolta direttamente o attraverso la funzionalità di Transito all'interno della stessa rete dell'operatore e verso altre reti fisse e mobili. La funzionalità di localizzazione dell'utente radiomobile chiamato consente di determinare verso quale cella instradare la connessione.

La commutazione può avvenire secondo due tecniche:

la commutazione di circuito CS (Circuit Switching), dove le risorse impiegate nel percorso da sorgente a destinazione sono assegnate alla connessione per tutta la sua durata;

la commutazione di pacchetto PS (Packet Switching), dove i singoli blocchi di dati impegnano le risorse per il solo tempo d'attraversamento.

Le principali caratteristiche delle bande LTE sono riassunte
di seguito:

Banda 800MHz: garantisce le migliori prestazioni in termini di copertura e penetrazione indoor.

Banda 1800 MHz: offre prestazioni intermedie in termini di copertura e penetrazione indoor. In tale banda è possibile utilizzare anche frequenze prima utilizzate per il GSM a 1800 MHz.

Banda 2600 MHz è la gamma con caratteristiche meno favorevoli in termini di propagazione e penetrazione indoor e può quindi essere impiegata efficientemente in *hot spot*.

La funzionalità di Carrier Aggregation consente di aggregare bande appartenenti a gamme diverse, ottenendo una banda equivalente di larghezza pari alla somma delle bande elementari, con cospicui miglioramenti della velocità trasmissiva.

Nella gamma degli 800 MHz, le bande di frequenza assegnate per il servizio LTE derivano dalla riassegnazione di parte delle frequenze (digital divided) precedentemente in uso per la TV analogica. La vicinanza tra le bande LTE e DVB-T può dar seguito a varie forme di interazione.

Nella gamma dei 2600MHz, le bande assegnate agli operatori mobili per il servizio LTE risultano adiacenti a quelle impiegate per i radar di controllo del traffico aereo civile
e militare. Analogamente a quanto esposto per la gamma a 800 MHz, anche in questo caso si può manifestare un fenomeno interferenziale

Per **scheda ARPA** si intende il progetto radio definitivo che avvia l'iter di presentazione permessi.

In essa viene definita univocamente la configurazione radio che otterrà autorizzazione dall'Arpa Regionale.

Le scelte fondamentali da compiere:

- Le tecnologie da implementare
- Le antenne da utilizzare
- Base antenna, orientamento e tilt delle antenne
- Le potenze da autorizzare

Produzione Dati e parametri di cella

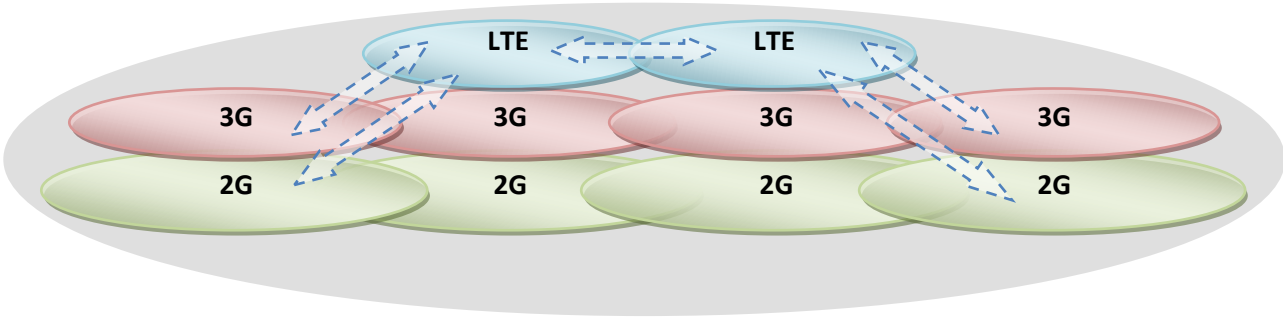
- Una strategia possibile, prevede che gli utenti dotati di terminale LTE dovranno accamparsi “facilmente” alla rete 4G.

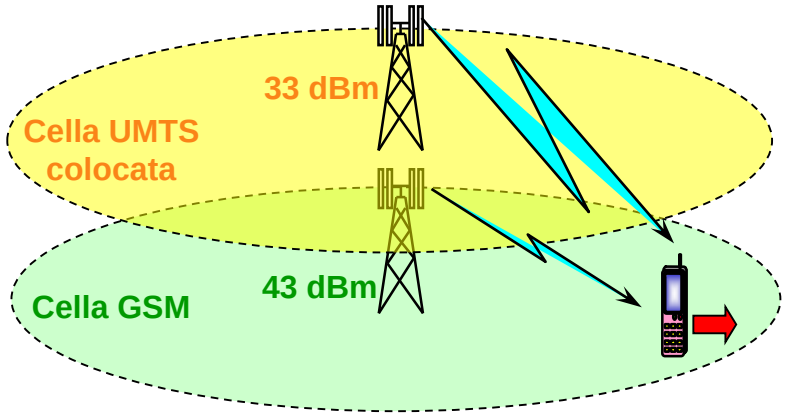
- In Idle Mode gli utenti registrati sulla rete LTE tenderanno a rimanere il più possibile all’interno della rete 4G, selezionando di volta in volta la cella LTE in grado di offrire il miglior livello di copertura (RSRP) e qualità (RSRQ).

- In Connected Mode gli utenti LTE effettueranno le sessioni dati rimanendo il più possibile all’interno della rete 4G e spostandosi, in caso di mobilità, sulla cella in grado di offrire il livello di potenza più elevato. Gli utenti saranno in grado di proseguire le loro sessioni dati anche in aree non coperte da rete LTE in quanto, qualora il livello della servente LTE (RSRP) dovesse scendere sotto una soglia di guardia, il terminale sarà indotto dalla rete LTE a selezionare la miglior cella 3G misurata (o 2G qualora non sia presente la rete 3G).

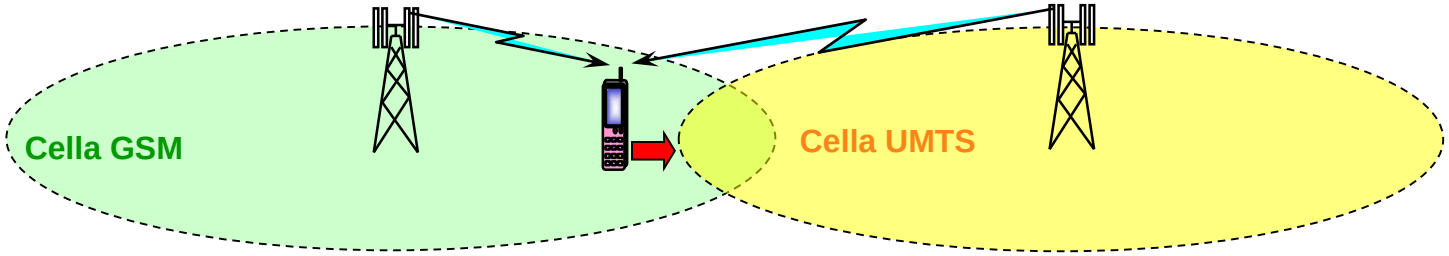
In presenza di copertura LTE, i terminali tenteranno di accamparsi sul layer 2600 fino ad un determinato valore di copertura (RSRP). In assenza di un segnale LTE 2600 sopra determinate soglie, il terminale tenterà di selezionare il layer 800.

In assenza di livelli di segnale LTE 800 e 2600 sopra determinate soglie, il terminale effettuerà la riselezione del 3G (oppure del 2G in caso di copertura 3G non adeguata).





In base al valore impostato, l'UE in Idle Mode esegue sempre le misure delle celle UMTS adiacenti.



Fine copertura GSM ed
inizio copertura UMTS

Dual SIM e eSIM

I device hanno un alloggiamento per una nano-SIM fisica ed integrano la eSIM come seconda SIM. La eSIM è una SIM su chip “riscrivibile” integrata nel device. La eSIM consente all’utente di cambiare operatore senza la necessità di rimuovere la SIM fisica: è sufficiente scannerizzare con il device un QR code, fornito dal nuovo operatore, per far sì che il profilo SIM del nuovo operatore venga scaricato dal device e “scritto” nella eSIM. La tecnologia Dual SIM è realizzata nella modalità Dual-SIM-Dual-Standby (DSDS) avente il seguente comportamento:

Quando entrambe le SIM sono in Idle, entrambe sono in grado di effettuare o ricevere chiamate voce ed SMS

Quando una delle due SIM è in chiamata voce, l’altra non può ricevere chiamate voce o SMS, né effettuare traffico dati

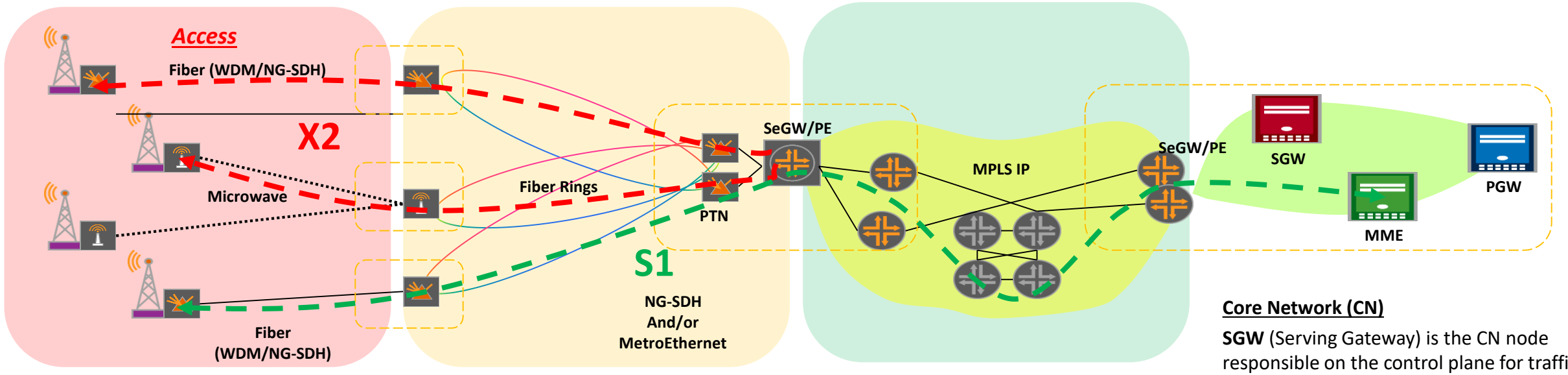
Una sola delle due SIM è in grado di effettuare traffico dati e può essere scelta dall’utente

Valutazione Performance

Accessibilità : Indicazione della probabilità di aggancio di un mobile alla cella in questione relativamente alle varie fasi di segnalazione necessarie : disponibilità di un SDCCH (nessuna congestione), corretta segnalazione sul canale SDCCH impegnato (nessuna caduta sul canale SDCCH), corretto aggancio sul canale TCH relativamente a transazioni di tipo MOC (Mobile Origitened Call) e/o MTC (Mobile Termineted Call) (aggancio del mobile sul canale TCH)

Cadute di conversazione: Indicazione della percentuale di chiamate con rilascio anomalo relativamente a tutte le chiamate che hanno determinato un' assegnazione di un canale TCH della cella vista in termini di utenza ossia includendo gli eventuali handover su tale cella ma escludendo tutte le situazioni di Handover Intracella (si tratta sempre della stessa chiamata in termini di utente).

Il traffico: E' noto che 1 Erlang rappresenta il traffico generato da una conversazione telefonica tra due utenti (voice-path) per un tempo continuo e mai interrotto di un'ora.



Access network (eRAN)

eNodeB (enhanced NodeB) is the access element of the evolved RAN, responsible for radio management and also for paging and handover procedures (formerly in charge of BSC/RNC)

Microwave and NG-SDH are the wireless and fiber-based transport technologies used on last-mile backhauling

Aggregation Network

NG-SDH and Metro-Ethernet are the technologies used to aggregate thousands of access sites towards tenths of IP POPs

SeGW/PE are L2/L3 aggregation devices (switch-router) able to manage access VLANs and IP VPNs towards the transport over IP MPLS, in order to create the any-to-any connectivity required by LTE between the eNodeBs and the core gateways. The same devices must manage the IPSEC encryption of the eNodeB traffic.

IP Backbone

PE (Provider Edge) routers define and transport one or more IP VPN over an IP MPLS backbone. Their scope is to transport many services, either fixed or mobile network, over a single multiservice backbone. PE functionalities may be supported by the same SeGW node.

Core Network (CN)

SGW (Serving Gateway) is the CN node responsible on the control plane for traffic and routing management, including lawful interception

PGW (Packet Data Network Gateway) is the CN node responsible for user traffic management, on data plane, and the Internet gateway

MME (Mobility Management Entity) is the CN node responsible for signaling, tracking and paging, including mobility from LTE to 2G/3G networks

Gli eNodeB richiedono maggiore capacità di banda sulla rete MW/NG-SDH di backhauling

L'architettura LTE è snella senza BSC/RNC tuttavia richiede l'integrazione in rete di apparati L2/L3 capaci di :

- Assicurare l'accesso untrusted (IPSEC tunnel management)
- Fornire L3 routing verso la core network (S1 interface)
- Fornire L3 routing tra i RAN sites (X2 interface)
- Fornire la connessione verso la Management System/DCN

Il ruolo dell' RNC è distribuito sugli eNodeB, core (MME/SGW/PGW) e gli apparati di aggregazione.

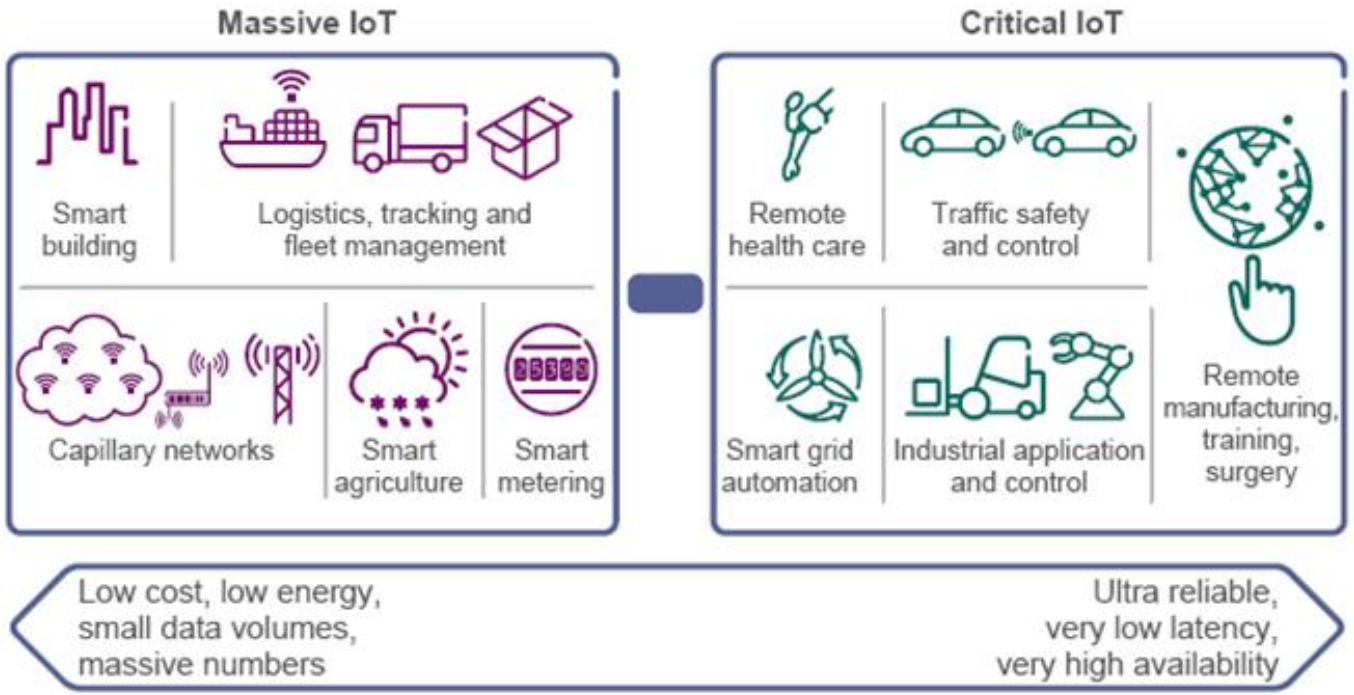
IoT: Internet of Things , scenari di impiego

Il **Massive IoT**, per il quale è necessario gestire grandi quantità di dispositivi a basso costo e consumo energetico; si tratta di applicazioni come Smart Building, Smart Agricolture, Smart Metering e use cases di logistica e trasporto. Si prevede infatti un numero vertiginoso di dispositivi che nel 2021 raggiungerà una quota pari a 28 miliardi nel mondo;

Il **Critical IoT**, i cui requisiti principali sono la bassa latenza, l'alta affidabilità ed un'altissima availability. Fanno parte di questa categoria applicazioni come l'E-Healthcare, il Traffic Control, la Telemedicina e Telechirurgia, la Smart Grid e simili applicazioni industriali.

Molti dispositivi IoT useranno delle tecnologie radio che operano nello spettro senza licenza designate per una connettività a corto raggio con una QoS limitata, come accade per le Machine Type Communication.

In tal caso, la connettività può essere realizzata mediante Wi-Fi, Bluetooth, Zigbee. L'alternativa all'uso dello spettro senza licenza risiede nelle tecnologie cellulari come il GSM, il WCDMA, l'LTE ed il futuro 5G, che hanno uno spettro con licenza ed assicurano quindi un'alta qualità del servizio. In particolare è stata sviluppata una nuova tecnologia di accesso radio a banda stretta, NB-IoT (Narrow Band IoT), creata specificamente come soluzione per le emergenti applicazioni LPWA (Low Power Wide Area).



Bande 5G: 700MHZ* (ideale per copertura mobile e pervasiva anche in indoor) ; 3.6GHz (buona capacità di banda) ; 26GHz (servizi ad altissima capacità su aree geografiche limitate (hot spot)

* Frequenze disponibili per gli operatori mobili a partire da luglio 2022 (ad oggi in uso per la TV digitale terrestre)

“Everything that can be automated, will be automated” (Robert Cannon)

Sicurezza e Privacy in ambienti smart IoT

L'accesso alla rete Internet da parte di innumerevoli oggetti (molto diversi dai tradizionali apparati ICT) che scambiano e comunicano informazioni, amplia le tradizionali minacce (threats) nel contesto della sicurezza e della privacy, sia per effetto dell'enorme allargamento della superficie di attacco che delle peculiarità degli oggetti e degli ambienti smart.

I dispositivi dell'IoT possono, infatti, presentare una serie di vulnerabilità in merito alla sicurezza che possono essere sfruttate in modo fraudolento:

1. consentendo l'accesso non autorizzato e l'uso improprio delle informazioni personali;

2. facilitando attacchi ad altri sistemi;

3. creando rischi per la sicurezza fisica di persone e cose.

Questi rischi sono anche tipici dell'ICT tradizionale ma risultano sicuramente accresciuti dalle specificità della IoT. Ad esempio, i nuovi Smart TV consentono di navigare in Internet, fare acquisti e condividere foto, similmente a un computer portatile o desktop. E, così come avviene per un computer, qualsiasi vulnerabilità di sicurezza in questi televisori potrebbe mettere in pericolo le informazioni personali memorizzate o trasmesse attraverso essi (password, conto corrente, ecc.). Inoltre, esattamente come per un computer, i punti deboli nella sicurezza di un particolare oggetto connesso possono facilitare attacchi contro la rete interna del consumatore a cui è collegato o attivare attacchi verso sistemi esterni.

Per quanto riguarda i rischi per la sicurezza fisica si pensi, ad esempio, alle vulnerabilità potenziali di un sistema di controllo della frenata di una Smart Car che, se sfruttate in maniera fraudolenta, potrebbero causare un incidente e, infine, mettere a rischio la vita del conducente. Oppure si pensi alle vulnerabilità di un dispositivo di controllo della salute: la manomissione delle informazioni trasmesse al centro di controllo potrebbe, anche in questo caso, mettere a rischio la vita dell'utilizzatore.

Ancora, riferendosi alle debolezze nel sistema di sicurezza dei contatori intelligenti di energia in una Smart Home, un ladro che accedesse da remoto ai dati di utilizzo di energia potrebbe determinare che la casa in un certo momento è disabitata e mettere in atto un furto

L'IoT presenta una "superficie di attacco" molto più estesa (si pensi a tal proposito alle previsioni sul numero di oggetti connessi).
Molti dei dispositivi IoT devono essere a basso costo e, pertanto, presentano limitazioni hardware: molti di essi (sensori, attuatori, . . .) sono alimentati con una batteria e dotati di CPU con limitata potenza di calcolo e limitata memoria RAM. Queste limitazioni, in aggiunta al fatto che tali dispositivi utilizzano Sistemi Operativi proprietari, rendono difficile l'utilizzo di sistemi di crittografia (poichè richiedono elevate capacità computazionali) o di sistemi di sicurezza convenzionali (antivirus) che richiedono RAM e hard-disk capienti.

Limitazioni software: il sistema operativo (semplice per essere adattato alle capacità hardware) spesso non consente di ricevere dinamicamente nuovo codice per l'aggiornamento della sicurezza.

Le aziende produttrici di dispositivi IoT (ad esempio quelle di elettrodomestici intelligenti) non hanno ancora esperienza e "mindset" per trattare con specifica competenza le tematiche legate alla sicurezza dei sistemi.

La molteplicità dei dispositivi connessi rende complicata l'adozione di un unico schema di sicurezza che sia applicabile sia dal dispositivo più semplice che da quello più complesso.

Inoltre i diversi mezzi con cui i dispositivi sono connessi alla rete rende complesso l'uso di un protocollo di sicurezza che consideri sia le caratteristiche dei mezzi wired che di quelli wireless allo stesso tempo.

Oltre ai rischi per la sicurezza, nell'IoT vi sono anche rischi per la **privacy**. Alcuni di questi rischi sono determinati dalla raccolta diretta di informazioni personali sensibili come la geo-localizzazione, i numeri del conto corrente o informazioni sanitarie - rischi già presentati dall'Internet tradizionale e dal m-commerce. Altri rischi nascono dalla raccolta indiretta di informazioni relative alle abitudini personali: si tratta di informazioni che possono essere dedotte dall'enorme mole di dati raccolti relativi, ad esempio, ai consumi energetici della casa, ai canali televisivi preferiti, ai luoghi maggiormente frequentati, eccetera.

Appare chiaro che, da parte di tutti gli “addetti ai lavori”, occorre considerare **sicurezza** e **privacy** come essenziale elemento progettuale, al fine di evitare che le aspettative degli early adopters delle nuove tecnologie smart dell’IoT vengano deluse su queste tematiche fondamentali, con conseguente ritardo o, addirittura, fallimento delle possibilità di adozione in larga scala.

Il ruolo degli Operatori

Gli Operatori di reti TLC, da sempre abituati a un contesto ampiamente regolato da leggi e regolamenti (ad es. per la tutela della privacy) e ad implementare soluzioni tecnologiche fortemente standardizzate, potranno portare un contributo di valore all'intero ecosistema IoT, concorrendo al rispetto dei principi fondamentali della sicurezza: **confidenzialità, integrità, disponibilità, non-ripudio.**

Ad esempio, per quanto riguarda la **confidenzialità**, l'Operatore di Rete può spendere e far valere il suo ruolo di "intermediario" tra i dispositivi smart e le piattaforme di servizio, facendo ricorso alle soluzioni che già implementa per la tutela dei dati personali e sensibili dei propri clienti: identità dell'utente, informazioni commerciali, informazioni bancarie.

Può garantire l'**integrit**à dei dati, ovvero che l'informazione non sia manipolata senza il consenso o all'insaputa dell'utente, ricorrendo a tecniche di "tunneling" o creando delle reti private virtuali (VPN) specifiche per i servizi IoT, minimizzando così il transito di informazioni su reti pubbliche che non adottano meccanismi di cifratura.

Grazie all'attitudine consolidata ad adottare tutte le policy necessarie a garantire la **disponibilità** dei propri apparati di rete (esecuzione di test di conformità, monitoraggio di performance, uso di spettro licenziato per minimizzare fenomeni interferenziali….), può mettere in campo la propria capacità tecnica ed organizzativa per monitorare da remoto anche le prestazioni dei dispositivi smart IoT, verificandone, ad esempio, il rispetto degli standard e adottando opportune azioni correttive nelle situazioni problematiche (es. aggiornamento del firmware da remoto o nei casi più estremi, qualora il dispositivo rappresenti una minaccia per la rete, l'esclusione del dispositivo).

Può, infine, garantire il corretto svolgimento delle procedure di **autenticazione** (ovvero la verifica dell'identità digitale dell'utente e del dispositivo) che già implementa nell'ambito, ad esempio, delle reti radiomobili. Se l'autenticazione è robusta ed è dimostrabile che l'autenticità non è stata violata, si rispetta inoltre il principio del **non-ripudio**, inteso come la garanzia che il mittente/destinatario di un messaggio non possa negare di averlo inviato/ricevuto.

Il ruolo fondamentale degli operatori di rete per garantire la sicurezza dell'intero ecosistema IoT è evidenziato anche dalla GSMA (associazione che rappresenta gli operatori di telefonia mobile) che, riconoscendo il ruolo di sicurezza e privacy come fattore "abilitante" dell'ecosistema IoT, ha pubblicato una serie di linee guida rivolte ai player del settore e, una in particolare, rivolta proprio agli operatori di rete (IoT Security Guidelines for Network Operators).

Ordine degli Ingegneri della provincia di Napoli

Grazie per l’attenzione