UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Ingegneria Modena
Dipartimento di Ingegneria "Enzo Ferrari"

SFIDE E VULNUS DEL 5G

Prof. Ing. Maurizio Casoni

- Sommario -

5G – Introduzione

- Protocolli e Reti Cellulari
- Bande di Frequenza
- Latenze, Architetture e Ottimizzazioni
- Applicazioni Chiave

5G – Vulnerabilità e Sicurezza

- DDoS e Radio Jamming
- Attacchi Informatici, Privacy e Minacce
- Principi di Funzionamento del 5G e Sicurezza
- Network Slicing e Analisi di Sicurezza Architetturali

5G – Consumi Energetici

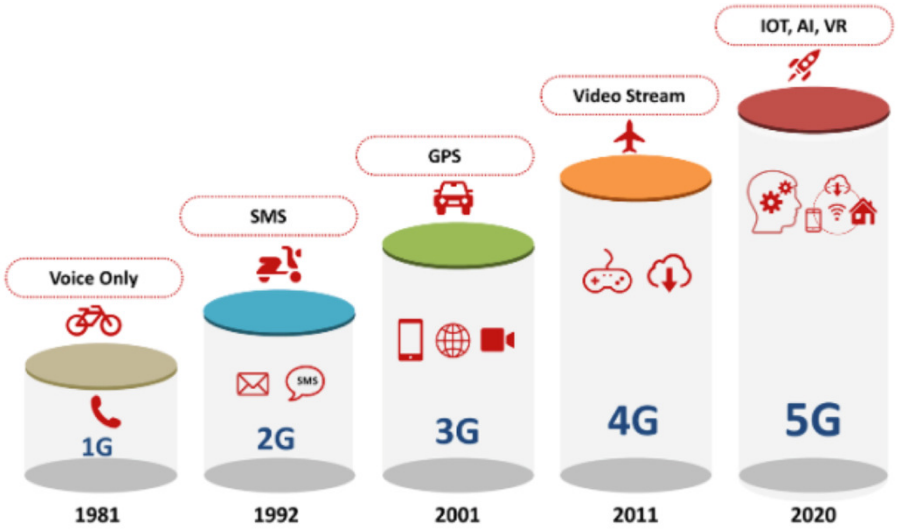
- Tecnologie Multi-Radio
- Evoluzione Architetturale delle reti cellulari
- Impatto Energetico Architetturale
- Impatto Energetico Operazionale

- Introduzione -

5G

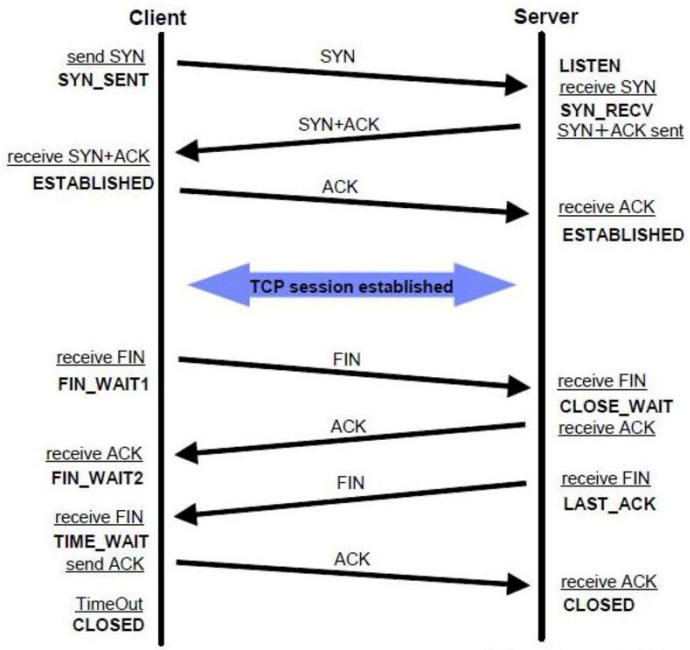
Cos’è il 5G

5G È L’ACRONIMO DI *FIFTH GENERATION*, OVVERO LA *QUINTA GENERAZIONE* DEL ***PROTOCOLLO*** DI COMUNICAZIONE ***CELLULARE***



5G

Che cos'è un protocollo



5G È L'ACRONIMO DI *FIFTH GENERATION*, OVVERO LA *QUINTA GENERAZIONE* DEL ***PROTOCOLLO*** DI COMUNICAZIONE CELLULARE

UN PROTOCOLLO È UN INSIEME DI REGOLE DI DIALOGO PER TRASMETTERE DATI, PER FORMATTARE E PROCESSARE DATI

SPECIFICA COME DUE O PIÙ DISPOSITIVI DEVONO OPERARE E INTERAGIRE PER COMUNICARE

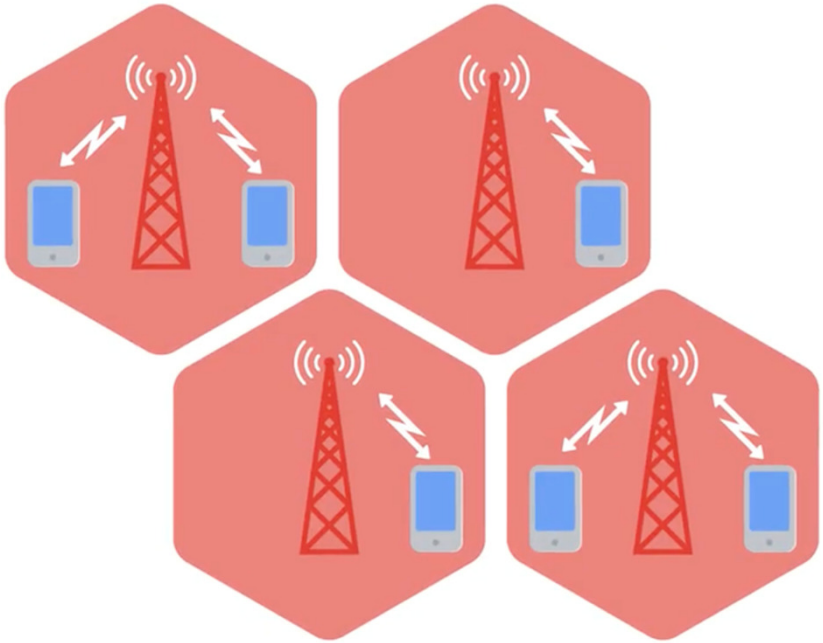
RISPETTO AL LINGUAGGIO NATURALE LA COMUNICAZIONE ELETTRONICA SEGUE SEMPRE REGOLE BEN PRECISE, MA A GRANDI LINEE È MODELLATA SUL MODO IN CUI NOI COMUNICHIAMO IN MODO FORMALE

IL NOSTRO 'FORMATO' È LA LINGUA CHE PARLIAMO, MENTRE USIAMO LA NOSTRA MENTE PER 'PROCESSARE' LE INFORMAZIONI, TRASFORMANDO INPUT SONORI O VISIVI IN CONCETTI E PENSIERI

TUTTAVIA, UN PROTOCOLLO IN UN SISTEMA RADIOMOBILE 5G SPECIFICA ANCHE COME I DISPOSITIVI DEVONO ACCEDERE AL MEZZO TRASMISSIVO (DI NORMA L'ARIA)

5G

Che cos'è una rete cellulare



5G È L'ACRONIMO DI *FIFTH GENERATION*, OVVERO LA *QUINTA GENERAZIONE* DEL PROTOCOLLO DI COMUNICAZIONE ***CELLULARE***

LE RETI CELLULARI SONO PROGETTATE SULLA BASE DEL CONCETTO DI 'CELLE', OVVERO ZONE GEOGRAFICHE CIASCUNA COPERTA DAL SEGNALE GENERATO DA UNA TORRE RADIO

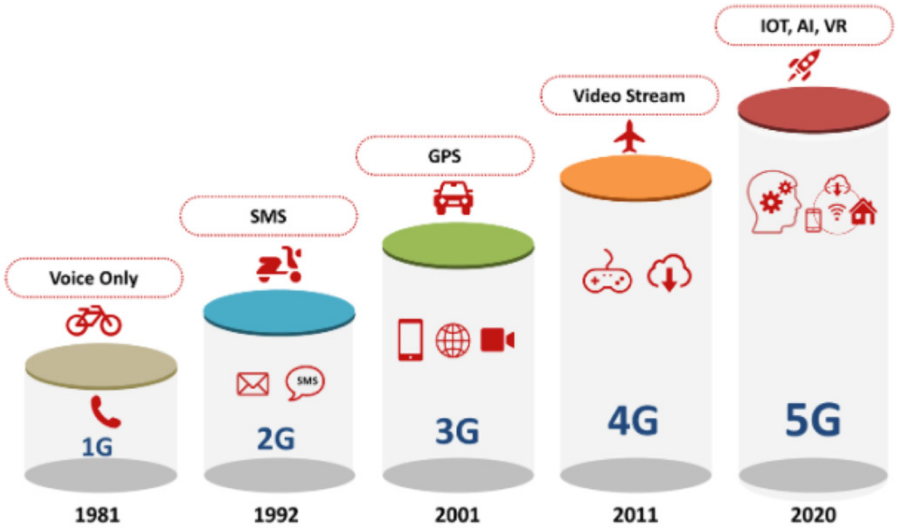
QUESTE OPERANO GENERANDO E RICEVENDO ONDE RADIO A DETERMINATE FREQUENZE

STORICAMENTE, AD OGNI CELLA È ASSEGNATA UNA CERTA BANDA DI FREQUENZE. AD ESEMPIO, SE A UNA CELLA VIENE ASSEGNATA LA BANDA 2.4-2.5 GHZ, POTRÀ TRASMETTERE E RICEVERE A 2.46 COME A 2.48 GHZ, MA NON A 2.75 GHZ

I SISTEMI CELLULARI MODERNI SONO IL RISULTATO DI DECADI DI INNOVAZIONI TECNOLOGICHE IN CUI GLI INGEGNERI HANNO SPERIMENTATO DIVERSI MODI PER CONDIVIDERE IL MEZZO TRASMISSIVO O, POTREMMO DIRE, L'ARIA

5G

Cos’è il 5G



5G È L’ACRONIMO DI *FIFTH GENERATION*, OVVERO LA *QUINTA GENERAZIONE* DEL PROTOCOLLO DI COMUNICAZIONE CELLULARE

IL 5G PUÒ OPERARE SU DUE PRINCIPALI BANDE DI FREQUENZA:

- SUB - 6 GHZ
- ONDE MILLIMETRICHE (MILLIMETER WAVE, O MMWAVE), ~40 GHZ

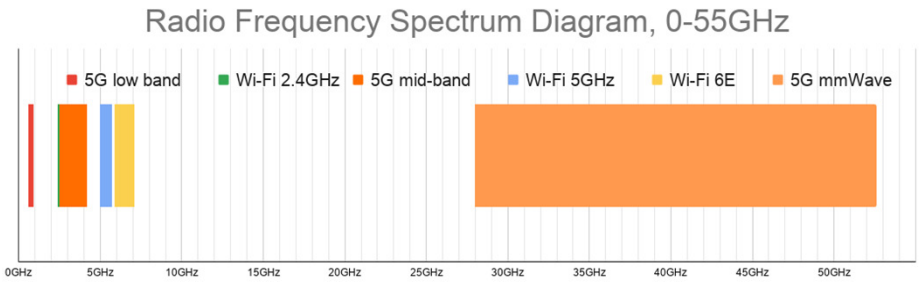
LE FREQUENZE ESATTE ALL’INTERNO DI QUESTE BANDE CHE I DISPOSITIVI ANDRANNO AD UTILIZZARE VARIANO DA OPERATORE AD OPERATORE E DA PAESE A PAESE

LE PROMESSE DEL 5G IN TERMINI DI ALTISSIME VELOCITÀ DI TRASFERIMENTO E BASSISSIME LATENZE SONO APPANNAGGIO DELLE FREQUENZE PIÙ ALTE

TENDENZIALMENTE, PIÙ È ALTA LA FREQUENZA, MAGGIORI SARANNO LE PRESTAZIONI, MA MINORE SARÀ LA COPERTURA GEOGRAFICA E LA PENETRAZIONE DI OSTACOLI

5G

Bande di frequenza: sub – 6 GHz



Le frequenze sotto i 6 GHz usate dal 5G non sono una novità, sono infatti analoghe a quelle già usate con 4G / LTE

La banda sub – 6 GHz è spesso ulteriormente divisa in:

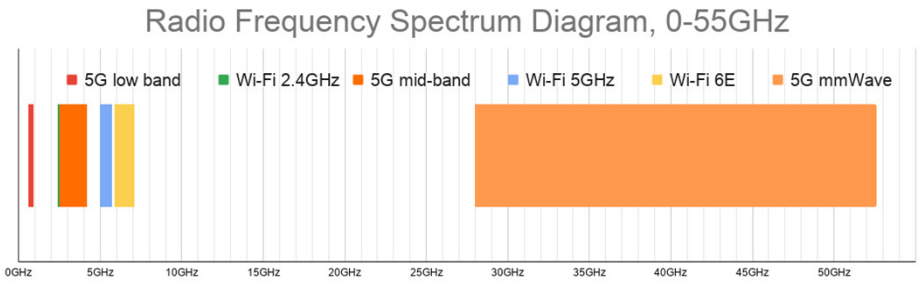
- Banda bassa (sub – 1 GHz)
- Banda media (2.5 GHz – 3.5 GHz)

A meno di 1 Ghz, la banda bassa è quasi ininfluenzata dagli ostacoli. Tipicamente, serve qualcosa come il fianco di una montagna tra torre radio e dispositivo per impattare in modo significativo la qualità della connessione. La portata geografica è ampia, ma la larghezza di banda disponibile è ristretta, limitando significativamente la velocità massima

La banda media è un buon compromesso per aree urbane. Non penetra muri e ostacoli facilmente quanto la banda bassa, il che rende però più facile per poche torri radio servire un'alta concentrazione di dispositivi in qualche chilometro quadrato senza interferire tra loro

5G

Bande di frequenza: sub – 6 GHz



UNA PORTATA PIÙ LIMITATA NON È QUINDI NECESSARIAMENTE UN MALE!

PIÙ AMPIA È LA PORTATA DI UNA TORRE RADIO, PIÙ UTENTI POTRANNO CONNETTERSI CONTEMPORANEAMENTE DIVIDENDOSI LE RISORSE RADIO E OTTENENDO QUINDI VELOCITÀ PIÙ BASSE E LATENZE MENO STABILI

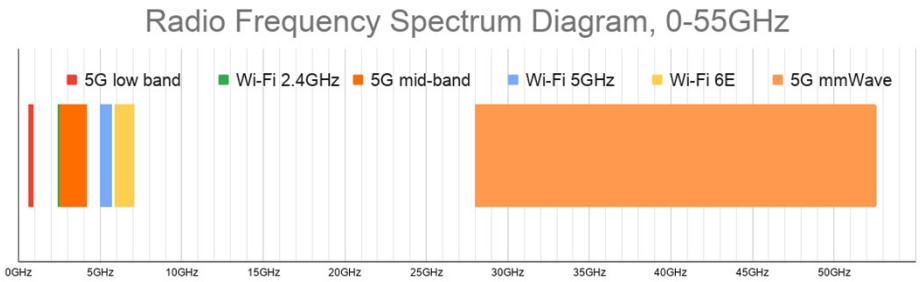
SEBBENE SIANO LE ONDE MILLIMETRICHE QUELLE CHE CARATTERIZZANO IL 5G, L'OPERATIVITÀ SOTTO I 6 GHZ È STATA ULTERIORMENTE AFFINATA RISPETTO AL PASSATO. RISPETTO AL 4G, CI SI ASPETTANO SIGNIFICATIVI MIGLIORAMENTI ANCHE IN QUESTA BANDA

PER QUANTO RIGUARDA LE FREQUENZE PIÙ BASSE, AD OGGI È POSSIBILE USUFRUIRE DI VELOCITÀ COME 100 MBPS O ADDIRITTURA 200 MBPS DA UNA CONNESSIONE 5G A BANDA BASSA! TUTTAVIA, QUANDO L'ADOZIONE DEL 5G SARÀ PIÙ AMPIA, QUESTI VALORI CALERANNO QUASI CERTAMENTE IN MODO SIGNIFICATIVO

LA BANDA MEDIA DEL 5G OPERA INVECE A FREQUENZE LEGGERMENTE PIÙ ALTE RISPETTO AL 4G, OFFRENDO DA 125 MBPS A 500 MBPS A SECONDA DEI CASI

5G

Bande di frequenza: mmWave

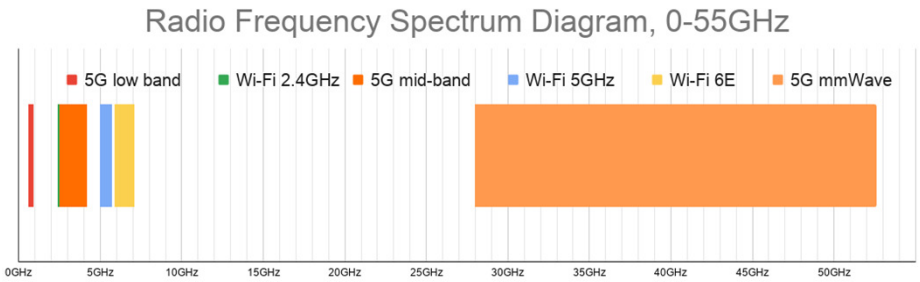


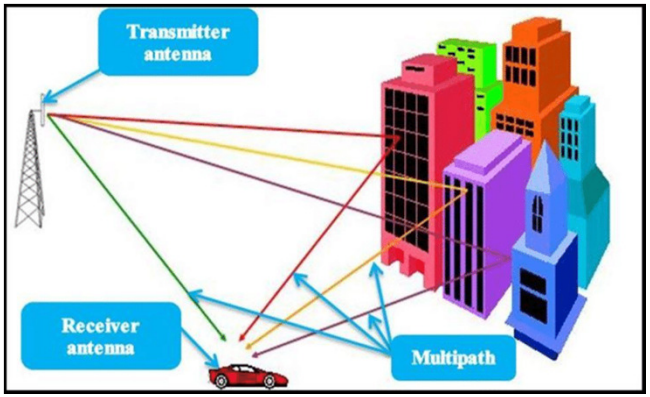
L'AMMONTARE DI BANDA A DISPOSIZIONE CON LE ONDE MILLIMETRICHE (MMWAVE) È ENORME.
LE SPECIFICHE DEL 5G PREVEDONO CANALI INDIVIDUALI LARGHI 800 MHZ, CHE SI TRADUCONO IN VELOCITÀ DI TRASFERIMENTO **AI MARGINI** DI UNA CELLA DI 400 MBPS

IL PROBLEMA PRINCIPALE DELLE MMWAVE È CHE NON SONO IDONEE A PENETRARE OSTACOLI E MURI. ALLE FREQUENZE DEFINITE PER IL 5G, GLI EDIFICI RIFLETTONO LE ONDE RADIO

5G

Bande di frequenza: mmWave





L'AMMONTARE DI BANDA A DISPOSIZIONE CON LE ONDE MILLIMETRICHE (MMWAVE) È ENORME.
LE SPECIFICHE DEL 5G PREVEDONO CANALI INDIVIDUALI LARGHI 800 MHZ, CHE SI TRADUCONO IN VELOCITÀ DI TRASFERIMENTO **AI MARGINI** DI UNA CELLA DI 400 MBPS

IL PROBLEMA PRINCIPALE DELLE MMWAVE È CHE PENETRANO CON DIFFICOLTÀ OSTACOLI SOLIDI. ALLE FREQUENZE DEFINITE PER IL 5G, GLI EDIFICI RIFLETTONO LE ONDE RADIO

IL FATTO CHE LE ONDE MMWAVE RIMBALZINO SU SUPERFICI SOLIDE HA PORTATO A SFRUTTARE MOLTO PIÙ CHE IN PASSATO LA PROPAGAZIONE MULTI-PERCORSO (MULTI-PATH). QUESTA RENDE LE MMWAVE IDONEE PER APPLICAZIONI ESTERNE

LA PORTATA È DECISAMENTE PIÙ LIMITATA RISPETTO ALLE FREQUENZE A BANDA MEDIA, CHE COMPORTA LA NECESSITÀ DI PIÙ CELLE MA, AL TEMPO STESSO, SI VENGONO AD AVERE MENO UTENTI PER CELLA E QUINDI MENO INTERFERENZE E PIÙ PRESTAZIONI

POSSIBILE IDEA È QUINDI QUELLA DI UTILIZZARE LE MMWAVE PER L'ESTERNO E BANDA MEDIA PER L'INTERNO

5G

Latenze: lo stato attuale



Ora come ora, un utente urbano con una buona connessione 4G a banda media può aspettarsi latenze nell'ordine dei 40-50 ms

Circa la metà di questi risultano da 'latenze aeree', ovvero il tempo che serve ad ogni pacchetto per essere trasferito da un dispositivo alla torre radio associata

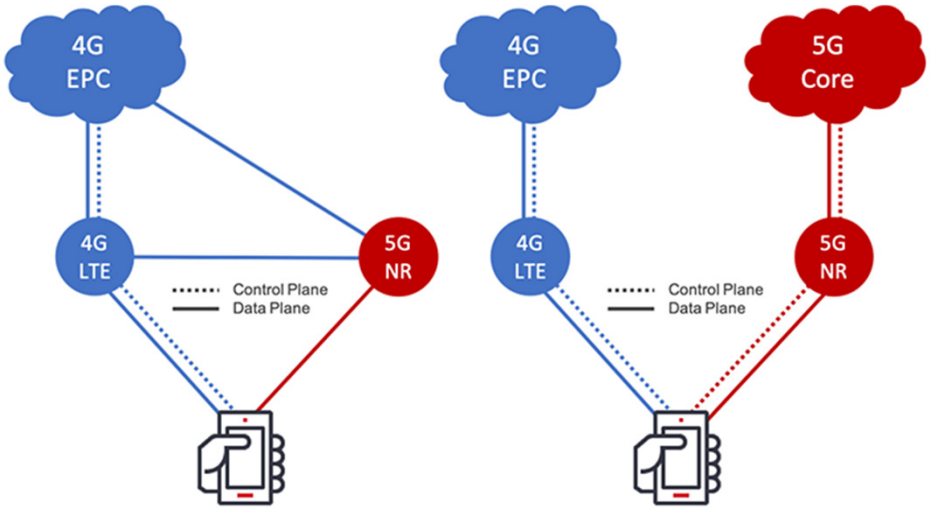
L'altra metà è 'latenza di rete', ovvero causata dai dispositivi nel percorso complessivo (e.g., router) dalla torre radio al server Internet di interesse

Le latenze aeree sono così *alte* non per via della propagazione ma per questioni di comunicazione e controllo

Come per il WiFi, le connessioni cellulari devono dividere il tempo trasmissivo tra più dispositivi. Inoltre, se due dispositivi comunicano contemporaneamente, le collisioni di pacchetti che ne risultano implicano la necessità di ritrasmettere i dati

5G

Latenze: Non Stand-Alone Architecture



A differenza del WiFi, i protocolli cellulari sono rigidi e controllati centralmente per assicurare un'equa allocazione di risorse ai dispositivi

Per poterlo fare, nei protocolli è previsto del tempo 'cuscinetto' per includere casi in cui i dispositivi o le torri radio abbiano bisogno di più tempo del previsto per codificare, decodificare e notificare la ricezione di ogni pacchetto inviato

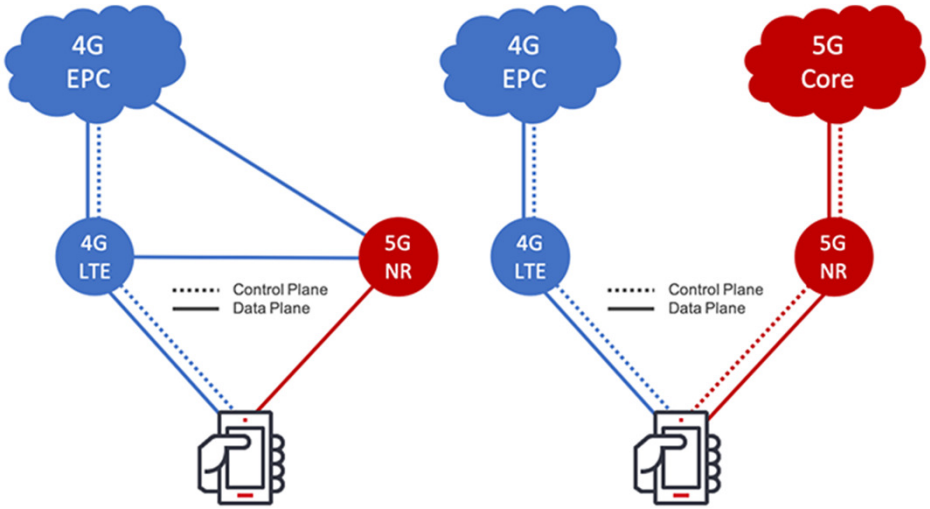
Con i miglioramenti recenti in termini di potenza di calcolo e quindi di tempi di elaborazione di dispositivi e attrezzature nelle torri radio, questi slot 'cuscinetto' possono essere ristretti in modo significativo

Ad oggi, gli operatori cellulari hanno implementato il 5G secondo l'architettura di transizione chiamata NSA, che sta per 'Non Stand-Alone architecture', ovvero *architettura non autonoma*

In sostanza, le operazioni di comunicazione e controllo sono ancora gestite dalla rete 4G, solo i dati vengono trasferiti da dispositivi a torri radio con velocità 5G

5G

Latenze: Stand-Alone Architecture



Di conseguenza, un dispositivo utente si connette contemporaneamente ad elementi radio multipli su frequenze diverse, con latenze limitate dallo standard 4G

Gli utenti 5G rurali hanno oggi latenze attorno agli 80 ms, mentre gli utenti 5G a banda media possono beneficiare di latenze sui 20-30 ms, rispetto agli stessi utenti 4G per cui le latenze si attestano nell'ordine dei 40-50 ms

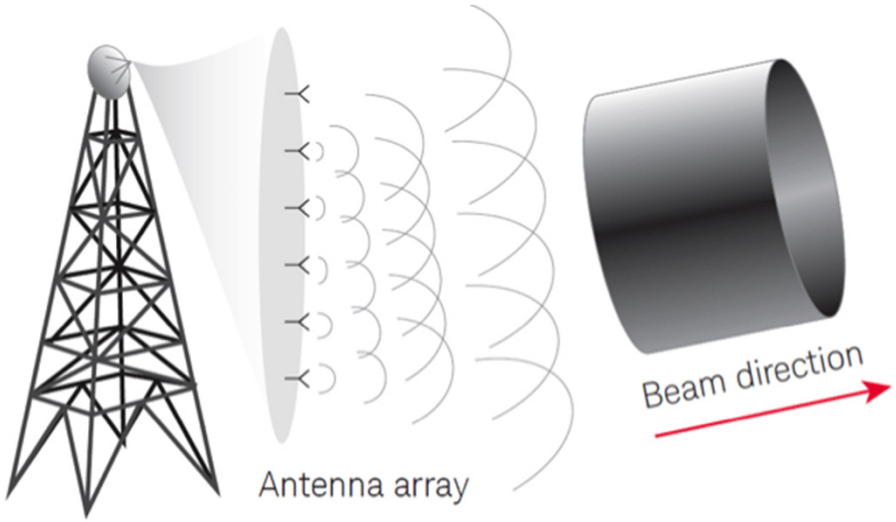
Bisogna però tenere presente che la maggior parte di questa differenza è dovuta alla relativa scarsità di utenti 5G. Nel tempo, questo vantaggio è destinato a scomparire

La buona notizia è che man mano che i canali 5G diventeranno più popolati, ci si aspetta che gli operatori di rete comincino a dispiegare reti 5G ad architettura SA, che sta per 'Stand-Alone', ovvero ad *architettura autonoma*

In questa architettura la rete 5G può funzionare autonomamente dalle reti 4G, gestendo anche le operazioni di comunicazione e controllo con tempistiche molto più stringenti

5G

Direzionalità



Il 5G è tipicamente dispiegato con antenne dette Massive MIMO (Multiple-Input Multiple-Output), ovvero composte da un numero elevato (e.g., 256) di elementi di antenna trasmittenti e riceventi con controllo elettronico dell'ampiezza e della fase dei segnali

Anche se gli smartphone avranno tipicamente array 2x2 o 4x4, gli array massivi degli elementi radio possono essere usati dagli operatori cellulari per formare dei fasci di onde direzionali (beamforming)

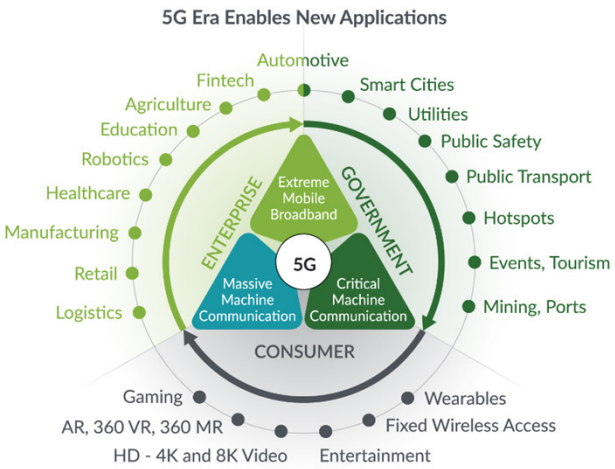
In generale, questi fasci vengono generati controllando la direzione di un fronte d'onda attraverso la manipolazione di fase e altre caratteristiche dei segnali individuali

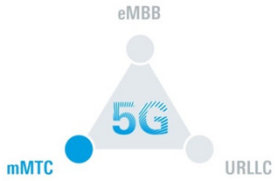
In sostanza, lo stesso segnale viene mandato da antenne multiple e il ricevitore ottiene quindi diverse copie dello stesso segnale. A seconda della sua posizione, i segnali possono arrivare con fase opposta (distruggendosi a vicenda), con fase uguale (aggiungendosi in modo costruttivo).

Il beamforming migliora notevolmente il rapporto segnale-rumore e incrementa le risorse temporali disponibili per i dispositivi connessi

5G

Le applicazioni per eccellenza





Il 5G intende supportare tre grandi categorie di casi d'uso:

- Enhanced Mobile Broadband (eMBB): servizi a larghezza di banda elevata per la connettività wireless
- Ultra-Reliable Low Latency Communication (URLLC): comunicazione ultra affidabile e a bassa latenza per requisiti critici
- Massive Machine Type Communication (mMTC): comunicazione affidabile per miliardi di sensori e dispositivi di monitoraggio

eMBB: l'obiettivo finale del 5G è quello di fornire fino a 10 Gb/s di picco di throughput, 1 Gb/s di throughput in mobilità elevata e fino a 10.000 volte il traffico di rete totale rispetto al 4G

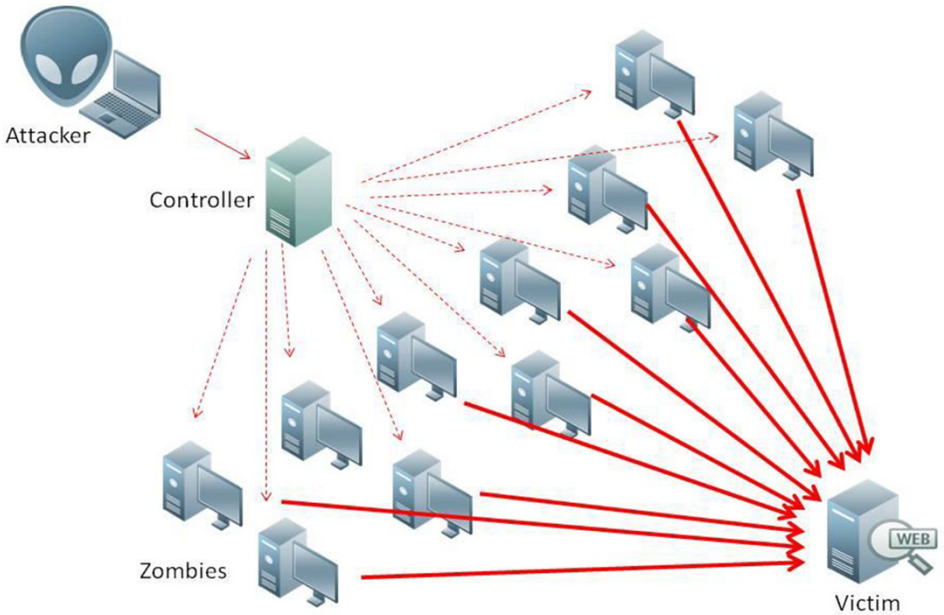
URLLC: una famiglia di casi d'uso completamente nuovi per rendere possibili comunicazioni ultra-affidabili a bassa latenza, supportando i requisiti più avanzati richiesti da alcuni settori, tra cui la guida autonoma per il settore automobilistico, la chirurgia remota, la robotica e le soluzioni cloud per l'industria 4.0. Spesso all'acronimo URLLC è associato il termine **Tactile Internet** o **Internet Tattile**

mMTC: connessione robusta di *miliardi* di dispositivi alla rete

- Vulnerabilità e Sicurezza -

5G: Vulnerabilità

DDoS, IoT e Botnet



I meccanismi di sicurezza definiti nello standard 3GPP garantiscono comunicazioni cifrate e integrità dei messaggi

Riguardo la disponibilità dei servizi, lo standard garantisce collegamenti affidabili in caso di cattive condizioni radio che non dipendono da azioni dolose, ma non protegge da tutte le possibili minacce come attacchi **DDoS** o **Radio Jamming**

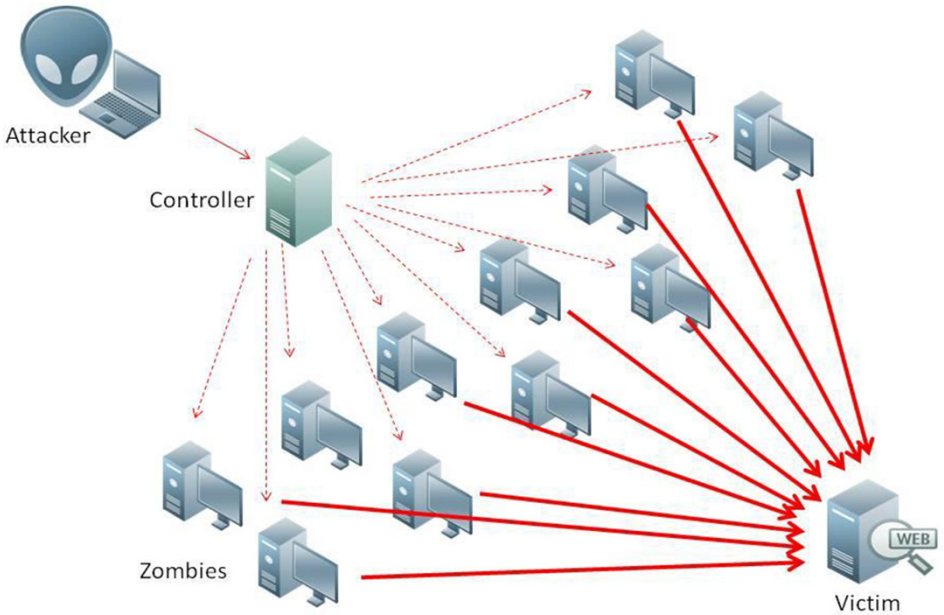
DDoS sta per Distributed Denial of Service e consiste in un attaccante che, preso il controllo di un certo numero di dispositivi 'zombie', li usa per inondare di richieste un dispositivo target che, di conseguenza, può trovarsi talmente oberato che non ha più la possibilità di rispondere alle richieste legittime provenienti dagli utenti

Il DDoS, benchè estremamente semplice, è un attacco efficace e difficile da contrastare, usato anche da entità governative

L'implementazione delle infrastrutture cellulari 5G e la proliferazione di dispositivi Internet of Things (IoT) sta creando una superficie di attacco allarmante per attacchi DDoS

5G: Vulnerabilità

DDoS, IoT e Botnet



Date le frequenze elevate, saranno necessari diversi elementi radio per coprire aree piuttosto piccole

Al tempo stesso, come premesso in precedenza, una delle applicazioni chiave del 5G è mMTC, che prevede un aumento esponenziale del numero di dispositivi potenzialmente connessi contemporaneamente, specialmente in riferimento al paradigma Internet of Things (IoT) e Industria 4.0

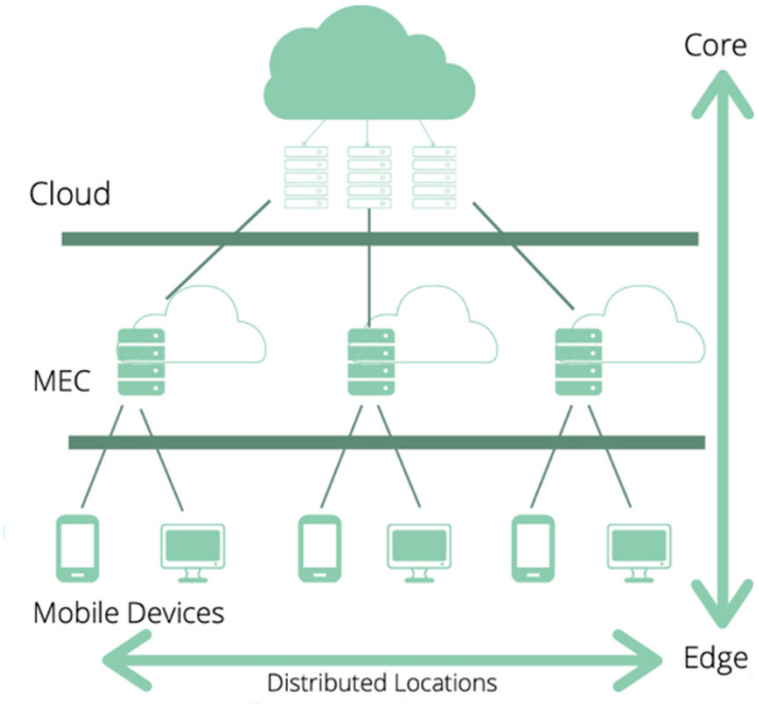
Questo rende molto concreto il rischio di trovarsi connesse reti di dispositivi (botnet) comandati a distanza da un attaccante

Inoltre, eMBB implica che botnet future potrebbero non aver bisogno di sfruttare un enorme numero di dispositivi mobili o IoT per paralizzare i propri obiettivi in quanto le stesse botnet saranno in grado di generare traffico a un tasso molto più alto dell'attuale!

La protezione contro attacchi DDoS è responsabilità degli operatori di rete, che possono utilizzare meccanismi per tentare di identificare e scalare selettivamente il traffico in entrata

5G: Vulnerabilità

URLLC



La minaccia è particolarmente preoccupante per le comunicazioni ultra-affidabili e a bassa latenza (URLLC). URLLC è considerata l'aggiunta più promettente alle prossime funzionalità 5G, ma **sarà anche la più difficile da proteggere** in quanto, analogamente a molti device IoT, richiede di essere 'posizionata' nei pressi della rete di accesso

In particolare, per le applicazioni URLLC che richiedono latenze nell'ordine di qualche millisecondo, il ruolo del Mobile Edge Computing (MEC, il dislocamento di piccoli data center nei siti radio per calcolo a bassa latenza e accesso diretto ai dati) sarà critico

MEC estende ancor di più la superficie di attacco delle reti 5G, soprattutto se si considera l'adozione di infrastrutture massicciamente distribuite come Fog ed Edge computing, e gli attacchi DDoS contro i server MEC potranno avere un impatto diretto su servizi e applicazioni critiche

Queste si estendono a diversi settori e industrie e includono le applicazioni che ricadono sotto il termine Internet Tattile, come giochi online, interfacce aptiche, automazione industriale e veicoli intelligenti/ guida autonoma.

5G: Vulnerabilità

Radio Jamming



Il **Radio Jamming** consiste nel disturbare volutamente le comunicazioni radio in modo da incrementarne il rumore.
Si esegue piazzando dispositivi di disturbo vicino alle torri radio.
Questi dispositivi trasmettono dati fasulli sulla stessa frequenza e utilizzando la stessa modulazione del segnale che si vuole disturbare

Analogamente a quanto accade per gli attacchi DDoS, l'eventuale protezione è compito dell'operatore di rete

È possibile monitorare lo stato delle proprie stazioni radio per tentare di rilevare eventuali elementi vittime di jamming in 3 modi:

- Rilevando cambiamenti improvvisi nelle prestazioni di un canale o monitorandone l'energia in eccesso
- Con metodi statistici
- Con tecniche di IA basate su machine e deep learning

Se viene rilevato jamming, si può tentare di aggirarlo re-direzionando il traffico di rete attraverso altre stazioni radio

Ad ogni modo, In un contesto 5G è piuttosto improbabile subire jamming su frequenze come le mmWave, perché richiede molta energia da parte del jammer

5G: Vulnerabilità

Attacchi informatici



Ad oggi, le barriere tecnologiche per eseguire con successo cyber attacchi sono quasi inesistenti

Diversi tipi di malware e vere e proprie suite di attacco sono vendute come Software-As-A-Service, con opzioni come periodi di prova, supporto utenti 24/7, forum di discussione dedicati e documentazione multi-lingua

Questa ampia e semplice disponibilità di malware ha contribuito ad un incremento sostanziale nella frequenza di cyber attacchi, che oggi portano con sé bassi rischi a fronte di guadagni potenzialmente alti

Al tempo stesso, l'alto tasso di digitalizzazione di industrie e servizi pubblici ha anche portato all'aggravamento dell'impatto che tali attacchi possono avere

Ad esempio, recentemente si è assistiti ad un netto incremento di attacchi detti *RANSOMWARE*, che consistono nel blocco delle funzionalità di un servizio a scopo di ottenere denaro in cambio della ripresa della sua operatività

5G: Vulnerabilità

Privacy



Le minacce alla privacy degli utenti finali vengono mitigate con meccanismi che proteggono gli identificativi utente

Rispetto agli standard cellulari precedenti, il 5G aumenta la frequenza con cui gli identificativi utente temporanei vengono aggiornati

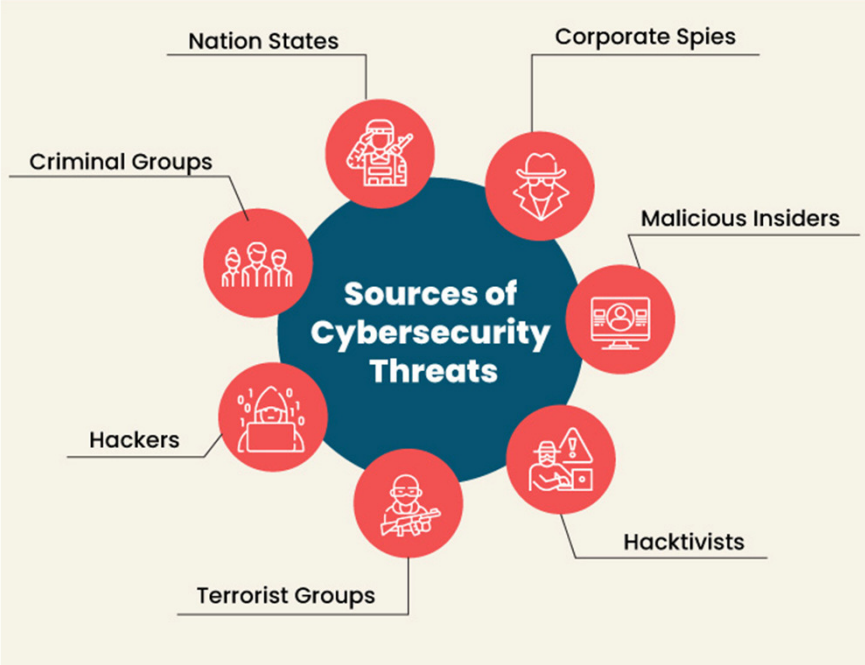
Tuttavia, similmente a quanto detto in precedenza, lo standard 5G protegge la privacy solo all'interno dell'operatività della rete cellulare

Ad esempio, un messaggio mandato da un utente in una rete sociale è protetto dallo standard 3GPP mentre attraversa la rete cellulare, ma è compito della rete sociale assicurarsi che il messaggio sia protetto dall'inizio alla fine del percorso, dato che attraverserà numerosi altri nodi Internet una volta uscito dalla rete 5G

Inoltre, è sempre responsabilità della rete sociale assicurare la privacy dei dati dell'utente elaborati ed immagazzinati nei loro server

5G: Vulnerabilità

Minacce



Possibili minacce possono essere rappresentate da criminali esterni ma anche da attori interni ad un'organizzazione

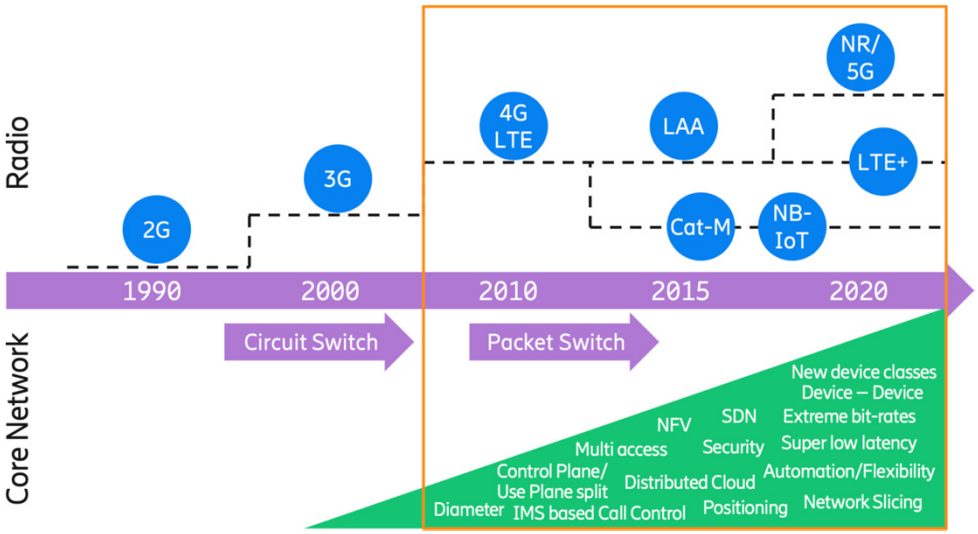
Classi di attaccanti comuni includono infatti dipendenti che cercano un guadagno personale (e.g., un dipendente che, avendo accesso ad un sistema di fatturazione e pagamento in locale o raggiungibile attraverso la rete, commette una frode) ed ex dipendenti scontenti che intendono vendicarsi di un danno subito

Altre minacce sono rappresentate da 'hacktivisti', sabotatori motivati politicamente o ideologicamente che attaccano con l'intenzione di interrompere servizi, compromettere siti web, o rubare informazioni sensibili per causare danni finanziari o mandare segnali politici

Sebbene gli stessi gruppi che minacciano qualsiasi industria possono attaccare anche gli operatori di rete, questi ultimi hanno caratteristiche uniche che li rendono un bersaglio interessante per attacchi sponsorizzati da stati o a fine di spionaggio industriale.
Le reti di telecomunicazioni, infatti, immagazzinano e trasferiscono dati, posizionamento e informazioni sensibili come messaggi e conversazioni, anche tra soggetti di alto profilo

5G: Sicurezza

I nuovi principi di funzionamento



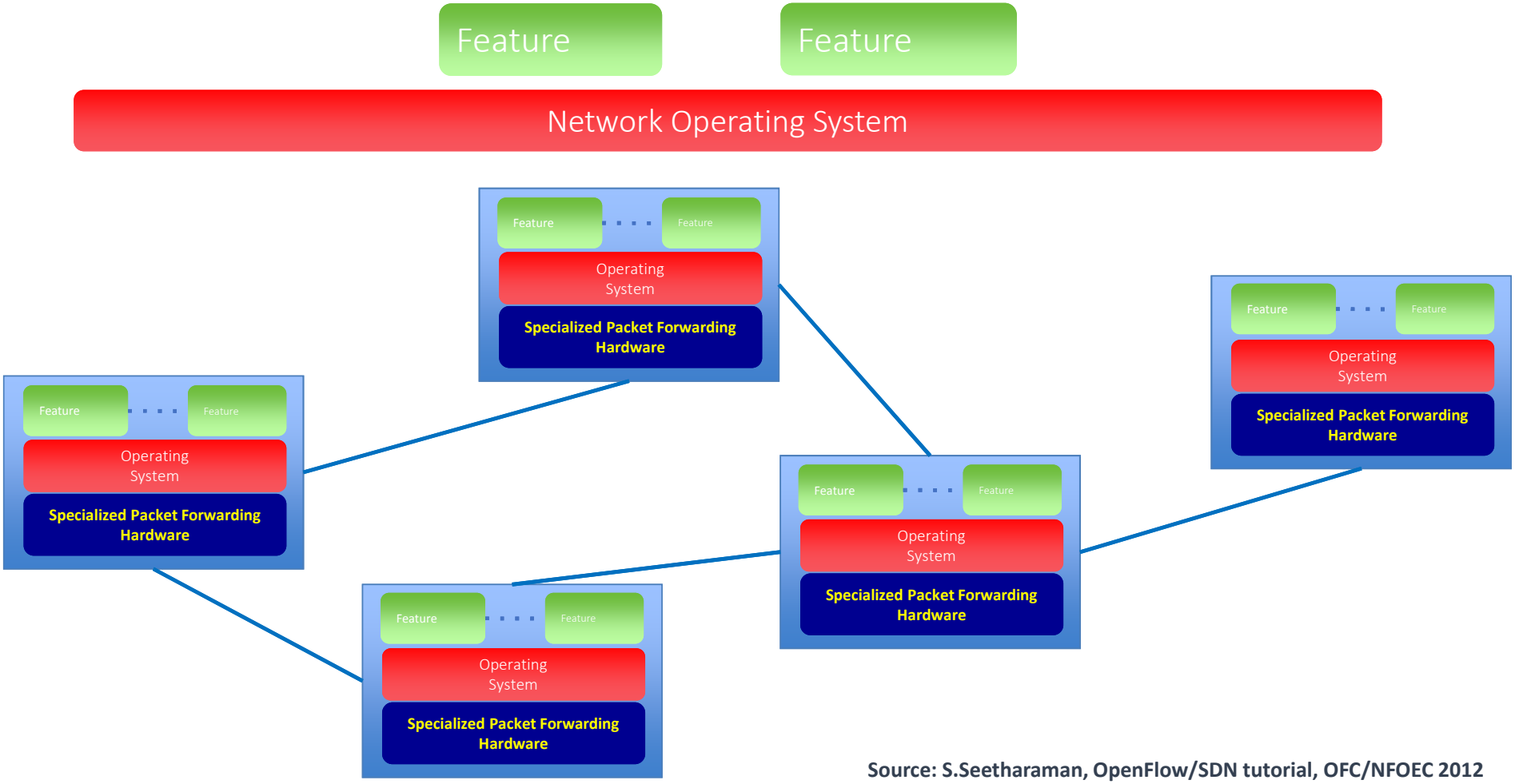
Il 5G può apparire 'semplicemente' come una tecnologia radio più veloce e versatile rispetto agli standard precedenti, ma è in realtà un'evoluzione ben più profonda

Il 5G è la prima generazione progettata a partire da tecnologie come il cloud-computing e la virtualizzazione. Tramite esse, l'esecuzione software può essere disaccoppiata dall'hardware fisico, rimuovendo il bisogno di funzioni dipendenti da hardware specifico. Questo è reso possibile da tecnologie come Software-Defined Networking (SDN) e Network Function Virtualization (NFV)

L'introduzione dell'IA e di computer sempre più potenti assieme alle tecnologie cloud sta portando ad un aumento dell'automazione nella configurazione delle reti, con una tendenza verso vere e proprie 'Self-Organizing Networks', ovvero reti capaci di configurarsi in autonomia e rispondere automaticamente a cambiamenti ad es. topologici

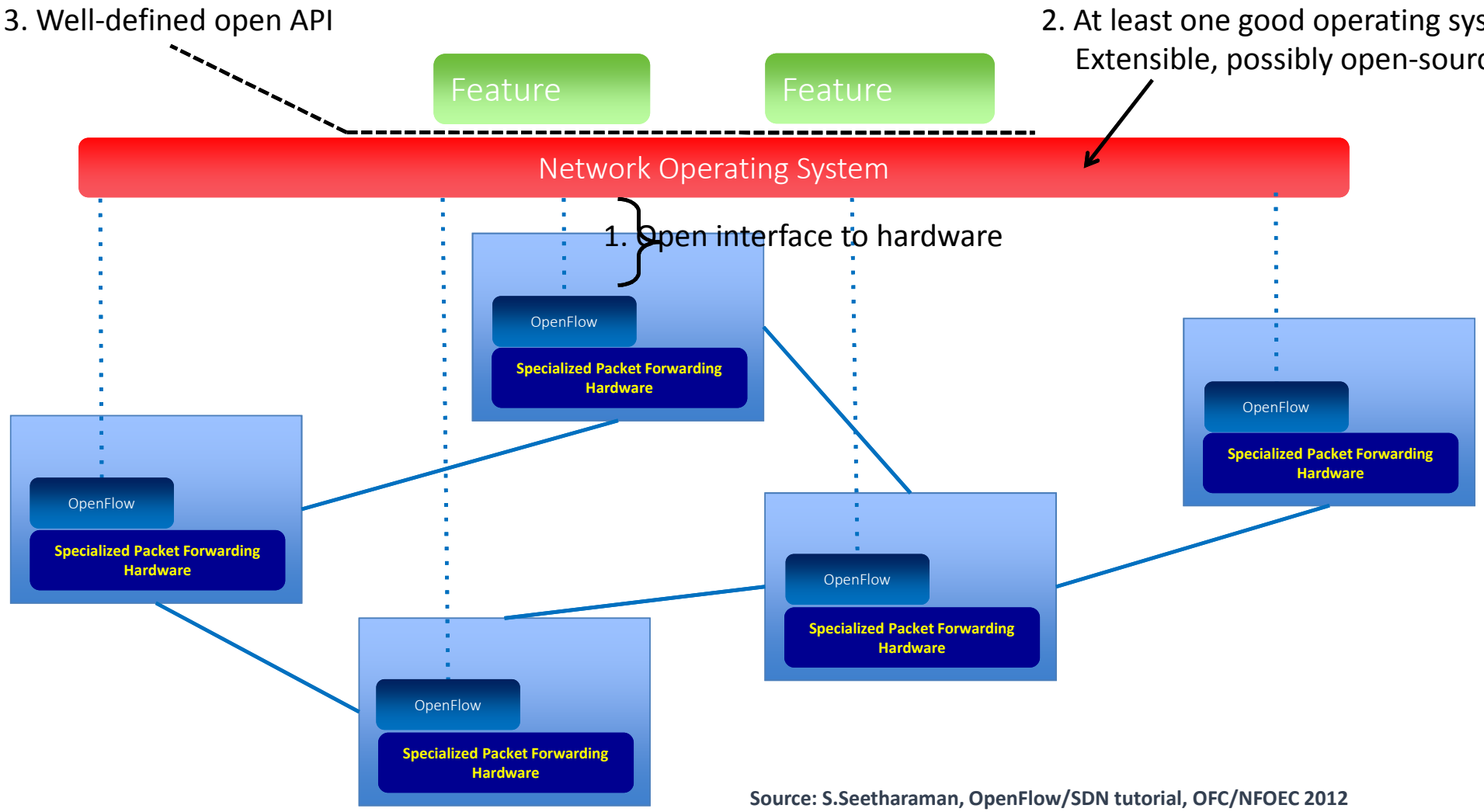
Inoltre, la tendenza dominante che si sta già palesando per le reti 5G è quella di reti sempre più basate su software. Tutto ciò porta un sistema 5G a non essere statico o completamente definito a priori, e.g., una rete core 5G potrà fornire servizi anche via 4G, WiFi, o via cavo

The OpenFlow Network Innovation



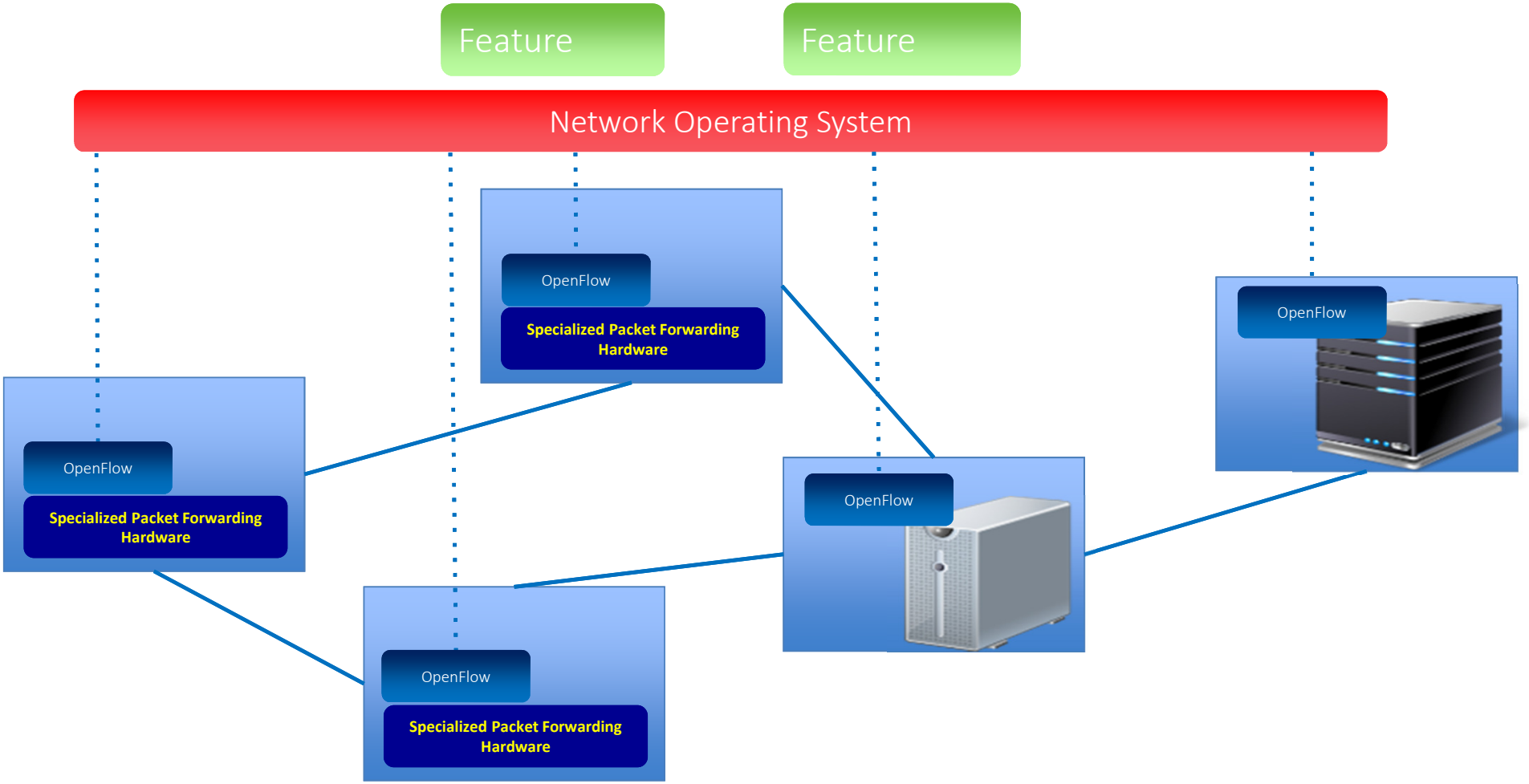
Source: S.Seetharaman, OpenFlow/SDN tutorial, OFC/NFOEC 2012

The OpenFlow Network Innovation

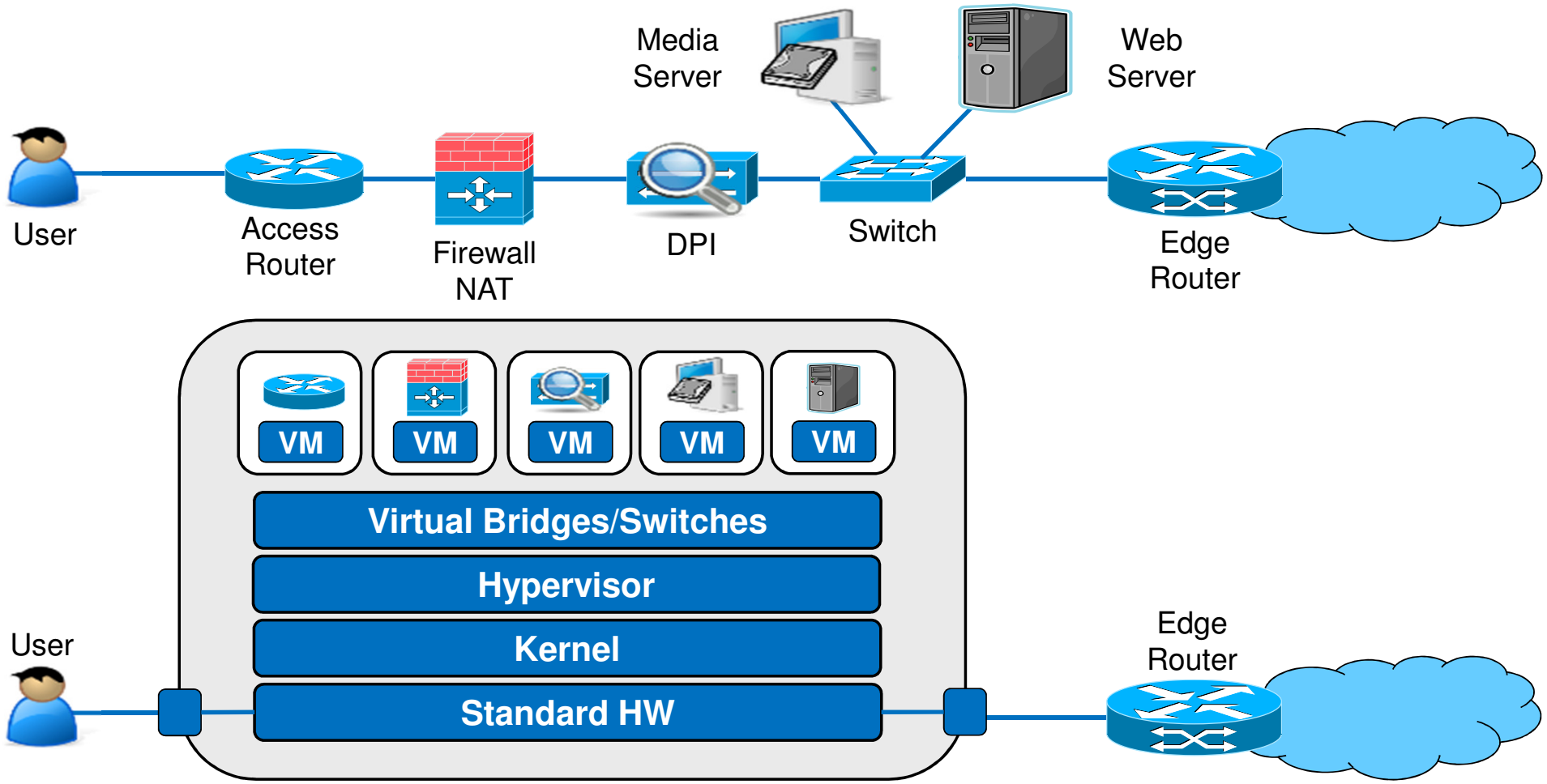


Source: S.Seetharaman, OpenFlow/SDN tutorial, OFC/NFOEC 2012

The OpenFlow Network Innovation

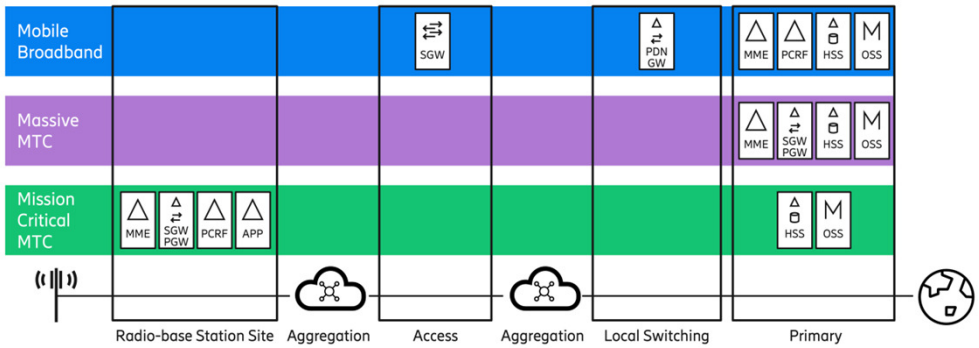


Network Function Virtualization (NFV):



5G: Sicurezza

Network Slicing



UNA RETE BASATA SU CLOUD INTRODUCE PERÒ NUOVI VETTORI DI ATTACCO CONTRO LA RETE, SPECIALMENTE SE LA SICUREZZA NON È CONSIDERATA IN FASE DI PROGETTAZIONE E INTEGRATA DALL'INIZIO

AL TEMPO STESSO, IL CLOUD RENDE POSSIBILE CREARE PARTIZIONAMENTI PER AUMENTARE LA RESILIENZA DELLA RETE E MIGLIORARE LE LATENZE, RENDENDO ANCHE POSSIBILE POSIZIONARE MECCANISMI DI SICUREZZA VICINO ALLE FONTI DI ATTACCO E QUINDI ISOLANDO LA PORTATA DEGLI ATTACCHI AD UN'AREA LOCALE

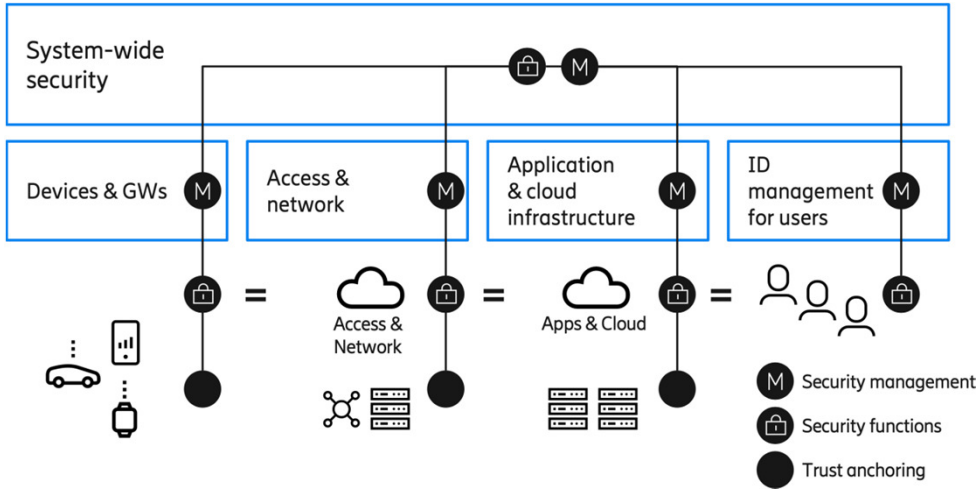
UNA SUDDIVISIONE DELLA RETE 'IN FETTE' (NETWORK SLICING) PERMETTE DI SEPARARE DIVERSI TIPI DI TRAFFICO UTENTE E DI CREARE AD-HOC RETI CORE DEDICATE A FACILITARE CASI D'USO SPECIFICI

IN SOSTANZA, TALE SUDDIVISIONE DELLA RETE PERMETTE DI CREARE SOTTO-RETI SPECIFICHE PER TIPO DI DISPOSITIVO, INDUSTRIA, O CLIENTE, SEPARANDO RUOLI E ISOLANDO SUPERFICI D'ATTACCO

OGNI 'FETTA', INFATTI, PUÒ AVERE LE PROPRIE POLITICHE DI SICUREZZA, CUCITE SU MISURA IN BASE ALLE NECESSITÀ E AI RISCHI SPECIFICI

5G: Sicurezza

Architetture di sicurezza



I MECCANISMI DI SICUREZZA DEFINITI NELLO STANDARD 3GPP SI FOCALIZZANO SU ELEMENTI FUNZIONALI E INTERFACCE, OVVERO GLI ELEMENTI SOTTO DIRETTA RESPONSABILITÀ DELLO STANDARD

CONSIDERAZIONI ADDIZIONALI DI SICUREZZA RELATIVE A DIVERSI TIPI DI IMPLEMENTAZIONE E DISPIEGAMENTO GEOGRAFICO VANNO AFFRONTATI A PARTE

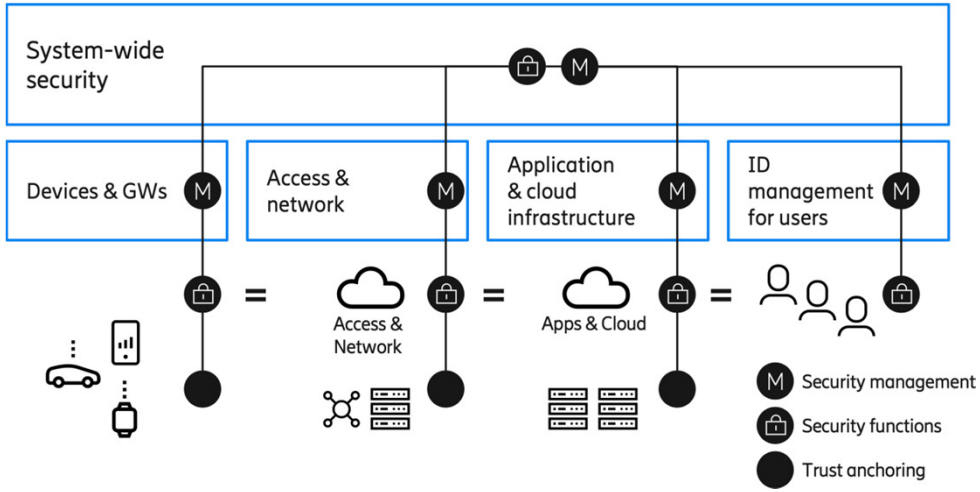
LA SICUREZZA COMPLESSIVA DI UNA RETE PUÒ ESSERE LETTA PRINCIPALMENTE CON DUE TIPI DI APPROCCIO: ORIZZONTALE E VERTICALE

LA *SICUREZZA ORIZZONTALE* PUÒ ESSERE DEFINITA COME **SICUREZZA DI SISTEMA** E VIENE OTTENUTA COMBINANDO E COORDINANDO UNA MOLTITUDINE DI CONTROLLI DI SICUREZZA TRA DIVERSI DOMINI, COME ACCESSO RADIO, RETI DI TRASPORTO, CORE, SERVIZI DI SUPPORTO (E.G., DNS, DHCP), CLOUD E SISTEMI DI GESTIONE (E.G., RETE, ESPERIENZA UTENTE)

IL COORDINAMENTO TRA TUTTI QUESTI DOMINI È ESSENZIALE PER POTER GARANTIRE OPERATIVITÀ DEI SERVIZI, CONFIDENZIALITÀ, INTEGRITÀ E PRIVACY

5G: Sicurezza

Architetture di sicurezza



LA *SICUREZZA VERTICALE* PUÒ INVECE ESSERE DEFINITA COME **SICUREZZA DI DISPIEGAMENTO**, OVVERO CI SI FOCALIZZA SULLA SICUREZZA DELLE FUNZIONI DI RETE DA DISPIEGARE

LO STANDARD 3GPP SPECIFICA FUNZIONI DI RETE E COME QUESTE DEVONO INTERAGIRE, MA NON SPECIFICA COME DEVONO ESSERE IMPLEMENTATE IN SISTEMI EMBEDDED O IN AMBIENTI VIRTUALI

TRADIZIONALMENTE, L'EQUIPAGGIAMENTO RADIO È SVILUPPATO SULLA BASE DI PIATTAFORME HARDWARE DIPENDENTI DA UN SINGOLO COSTRUTTORE, SIA NELLA RETE DI ACCESSO CHE NELLA RETE CORE. QUESTE PIATTAFORME SONO STATE PROGETTATE PER SODDISFARE STRINGENTI REQUISITI DI SICUREZZA

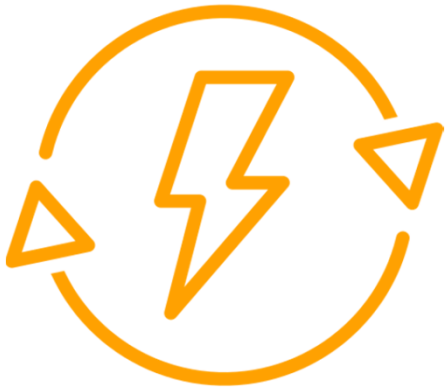
IN AMBIENTI VIRTUALIZZATI, LA SITUAZIONE È DIVERSA IN QUANTO SONO COINVOLTI FORNITORI MULTIPLI, CIASCUNO FOCALIZZATO SU UNA PARTE SPECIFICA DELLA RETE

DI CONSEGUENZA, LE STRATEGIE DI SICUREZZA TRADIZIONALMENTE SVILUPPATE IN UN'UNICA SUITE HARDWARE VANNO ORA IMPLEMENTATE CONSIDERANDO L'INTERA CATENA SOFTWARE CHE VA A COMPORRE I SERVIZI DI RETE VIRTUALIZZATI

- Efficienza Energetica -

5G: Efficienza Energetica

Tecnologie Multi-Radio



Le infrastrutture dei grossi operatori di rete hanno consumi annui nell'ordine dei 5 TWh, avvicinando al *miliardo* di EUR/USD i costi energetici complessivi all'anno *per operatore.* Nonostante la stragrande maggioranza dell'energia provenga dalle reti elettriche, dove queste mancano i soli combustibili fossili usati dagli operatori si attestano tra le decine e le centinaina di *milioni* di litri l'anno

Tradizionalmente, l'introduzione di una nuova tecnologia cellulare comportava il dispiegamento di nuove torri radio e reti core **a fianco** delle infrastrutture già esistenti

Gli operatori di rete hanno utilizzato questa strategia per fornire nuova connettività ai propri clienti senza interrompere servizi avviati in precedenza e per coprire le aree geografiche ancora non coperte dai nuovi standard

Sebbene questa strategia spalmi la spesa capitale nel tempo ed estenda il ritorno degli investimenti fatti per le vecchie infrastrutture, essa presenta anche un maggior costo operativo, dovuto alla manutenzione di più strutture e ad un consumo energetico complessivo via via più elevato

5G: Efficienza Energetica

Tecnologie Multi-Radio



Durante il consolidamento delle reti 4G, alcuni grossi operatori di rete hanno iniziato a sostituire le infrastrutture 2G e 3G esistenti con stazioni base capaci di fornire servizi 2G, 3G e 4G da singole torri radio

Ci sono diversi metodi per co-localizzare le attrezzature che permettono di fornire servizi a partire da diversi standard

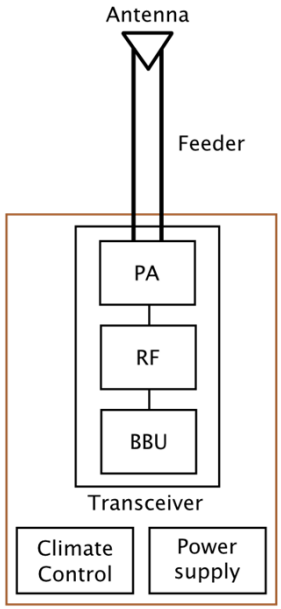
Se questi operano sulle stesse bande di frequenza è possibile usare un unico sistema di antenne, che però implica la condivisione di azimuth e orientamenti tra tutte le tecnolofie

Nel caso più generale, invece, ogni tecnologia usa frequenze diverse e, conseguentemente, va utilizzata un'antenna a banda singola o multipla per ogni standard

L'evoluzione di questa architettura nel tempo, chiamata Multi-Radio Access Technology (M-RAT), può essere suddivisa in quattro step principali, corrispondenti alla diffusione di diverse architetture di rete

5G: Efficienza Energetica

Stazioni base monolitiche



(a) Monolithic BS

Le tradizionali stazioni base sono composte da una cabina con l'attrezzatura elettronica posta sul suolo, una o più antenne montate su un palo ad un'altezza di diverse decine di metri, e cavi detti *feeder* che collegano la cabina al suolo con le antenne

I principali componenti di rete dell'attrezzatura elettronica sono l'alimentatore (Power supply), il condizionatore (Climate Control) e un Transceiver

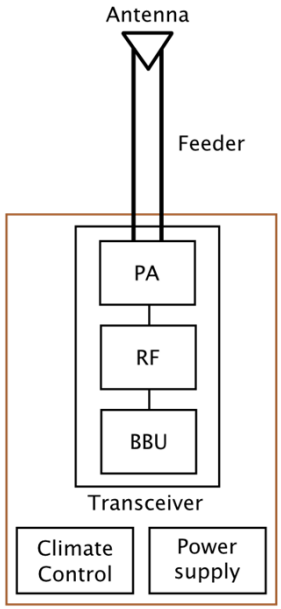
Ciascuno di questi consuma una porzione significativa dell'energia utilizzata dalla stazione base e presenta, pertanto, opportunità per risparmi energetici

L'alimentatore converte corrente alternata in corrente continua per fornire energia al sistema

Il condizionatore mantiene la temperatura dei componenti all'interno di un range operativo appropriato. Attenzione, condizionatore non significa necessariamente 'raffrescatore'. Climi molto freddi hanno bisogno di equipaggiamento che **riscalda** l'attrezzatura

5G: Efficienza Energetica

Stazioni base monolitiche



(a) Monolithic BS

Il transceiver gestisce i segnali in ingresso e uscita, ed è a sua volta composto da tre sotto-elementi:

- BBU, ovvero BaseBand Unit, l'unità che elabora i segnali in banda base
- RF, ovvero Radio Frequency module, l'unità che modula i segnali dati da banda base a radiofrequenza, e viceversa
- PA, ovvero Power Amplifier, l'unità che amplifica il segnale per la trasmissione a radiofrequenza.

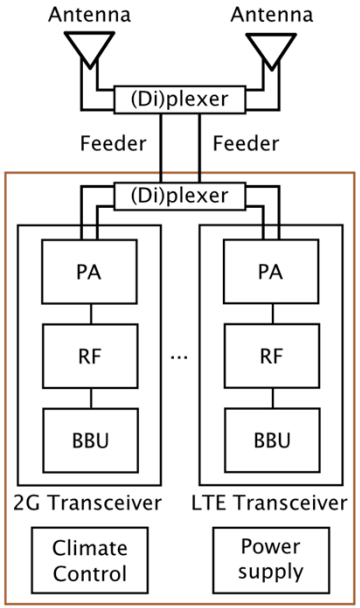
L'amplificatore di potenza è spesso il componente che viene riportato come il più esoso in termini di dispendio energetico, fino al 50% del totale

I feeder sono un altro elemento molto inefficiente. Sono lunghi cavi coassiali che trasportano i segnali analogici tra la cabina al suolo e l'antenna

Se questa è posizionata lontano dal transceiver, le perdite subite dal segnale attraversando i feeder sono significative, richiedendo un segnale maggiormente amplificato e, di conseguenza, più energivoro

5G: Efficienza Energetica

Stazioni base M-RAT



(b) Multi-RAT BS
(M-RAT BS)

Le stazioni base a tecnologie multi-radio modularizzano i propri transceiver, permettendo la coesistenza di standard multipli e introducendo una certa flessibilità nell'aggiunta o rimozione di funzionalità

Ogni stazione base M-RAT ha un unico alimentatore e un unico condizionatore, e permette risparmi di energia significativi

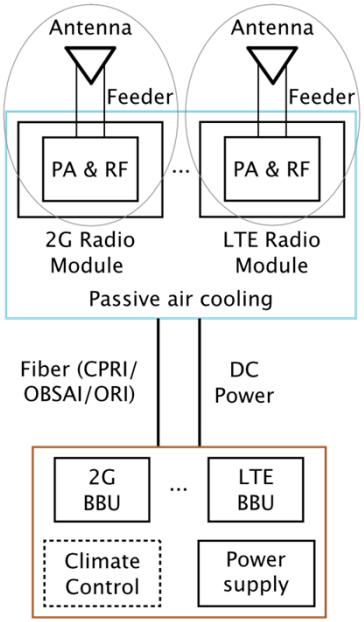
Dovendo fornire energia a più transceiver contemporaneamente, un singolo alimentatore modulare può in media operare ad un regime di efficienza più alto (tendenzialmente, più è alto il carico di un alimentatore all'interno del suo range di operatività, più è alta la sua efficienza)

Lo stesso si può dire per il condizionatore, dato che un sistema di climatizzazione centralizzato è tipicamente più efficiente di uno distribuito

In aggiunta, è anche possibile sfruttare dei bi-accoppiatori (Di-plexers) per ridurre della metà il numero di feeder

5G: Efficienza Energetica

M-RAT Remote Radio Heads



(c) Multi-RAT RRH (M-RAT RRH)

L'evoluzione delle stazioni base si è avuta negli elementi radio, chiamati *Remote Radio Heads (RRHs)*

Gli RRH sono stazioni base che disaccoppiano i propri elementi BBU dalle unità radio, tipicamente mantenendo i primi al suolo e integrando le seconde vicino alle antenne

Questo posizionamento permette ulteriori risparmi energetici in quanto, essendo l'attrezzatura dei transceiver integrata con le antenne, si possono sostanzialmente azzerare le perdite dovute ai feeder

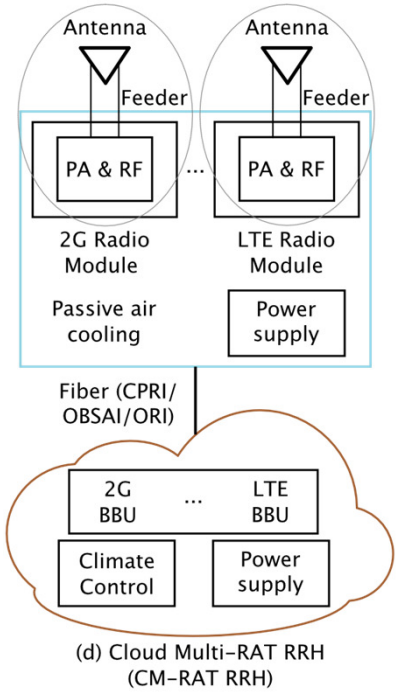
Solamente questo permette di risparmiare fino al 30% dell'energia, riducendo una delle principali fonti di spreco

In celle abbastanza piccole, entrambi gli elementi possono essere posizionati con le antenne

Inoltre, spesso un condizionamento climatico passivo è sufficiente, diminuendo ancor di più l'impatto energetico

5G: Efficienza Energetica

Cloud-RAN e Cloud M-RAT RRH



(d) Cloud Multi-RAT RRH (CM-RAT RRH)

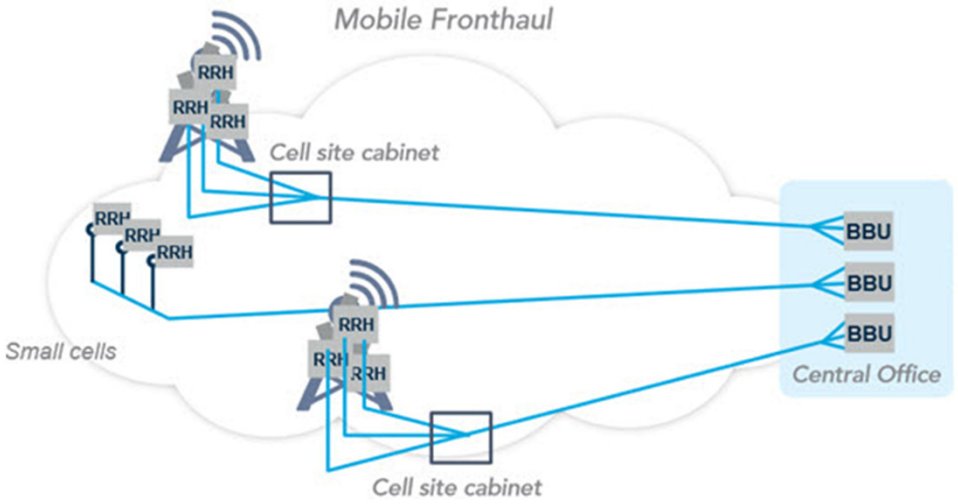
Recentemente ha preso piede il paradigma Cloud-Radio Access Network (C-RAN), per cui le unità BBU vengono aggregate all'interno di server remoti centralizzati in cloud

Centralizzare gli elementi BBU elimina il bisogno di avere sistemi di condizionamento energivori in ogni stazione base o RRH. Assieme alla complessiva semplificazione architetturale degli elementi radio, questo può ridurre fino al 50% le spese operative per nuovi siti

Il paradigma permette inoltre di aumentare l'efficienza energetica generale, le risorse computazionali disponibili per gli algoritmi di elaborazione dei segnali, il bilanciamento del carico tra celle, e rende anche possibile l'implementazione di algoritmi multi-celle

5G: Efficienza Energetica

Cloud-RAN e Cloud M-RAT RRH



Recentemente ha preso piede il paradigma Cloud-Radio Access Network (C-RAN), per cui le unità BBU vengono aggregate all'interno di server remoti centralizzati in cloud

Centralizzare gli elementi BBU elimina il bisogno di avere sistemi di condizionamento energivori in ogni stazione base o RRH. Assieme alla complessiva semplificazione architetturale degli elementi radio, questo può ridurre fino al 50% le spese operative per nuovi siti

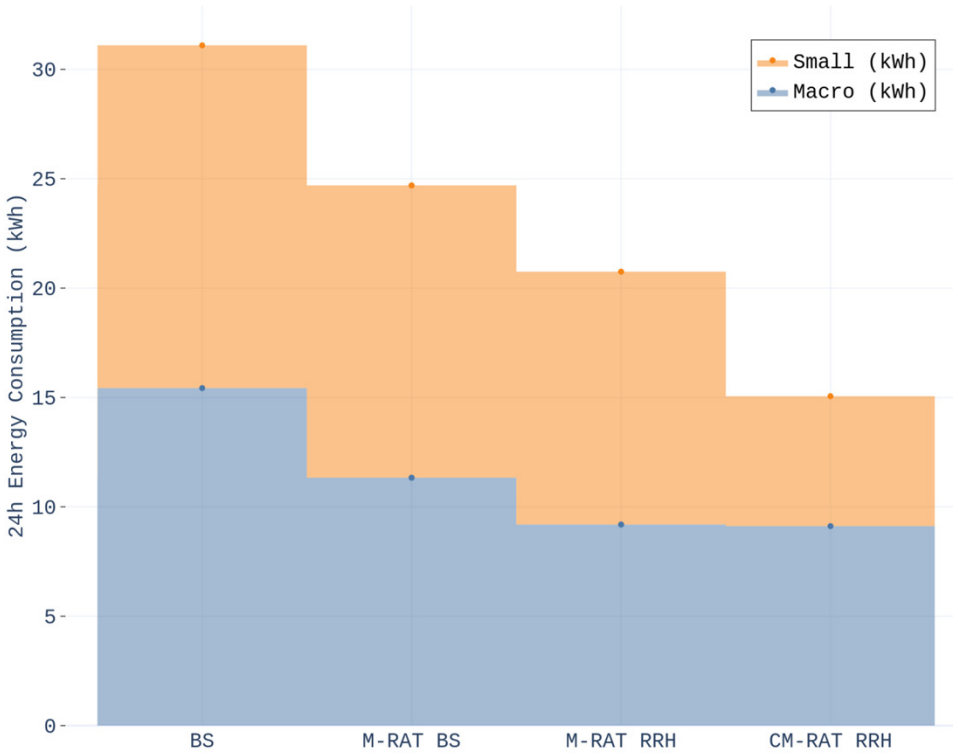
Il paradigma permette inoltre di aumentare l'efficienza energetica generale, le risorse computazionali disponibili per gli algoritmi di elaborazione dei segnali, il bilanciamento del carico tra celle, e rende anche possibile l'implementazione di algoritmi multi-celle

Purtroppo, centralizzare gli elementi di elaborazione dei segnali aumenta enormemente il carico del *fronthaul*, il canale fisico che collega le stazioni radio al cloud

Se il bilanciamento viene implementato in modo inopportuno, questo può addirittura invertire i vantaggi a livello energetico risultanti dalla centralizzazione

5G: Efficienza Energetica

Impatto energetico architetturale



Nel complesso, le architetture multi-radio garantiscono in modo consistente significativi risparmi energetici

Eliminare le inefficienze e aggregare in modo accorto le operazioni risulta in benefici tangibili anche grazie a virtuosi effetti a cascata, per cui il miglioramento dell'efficienza di un componente si ripercuote su altri componenti, moltiplicandone così l'impatto positivo in termini di risparmio energetico

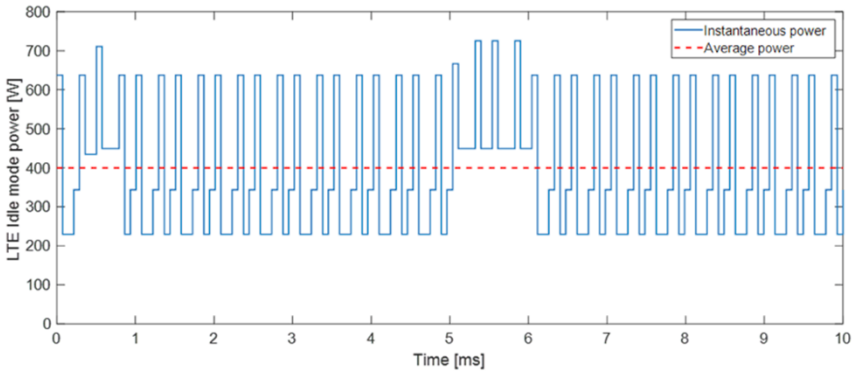
Ad ogni modo, i requisiti dello standard 5G rendono non banale l'integrazione di questa tecnologia in architetture multi-radio, soprattutto a causa della maggiore pressione esercitata sui collegamenti fronthaul di trasporto

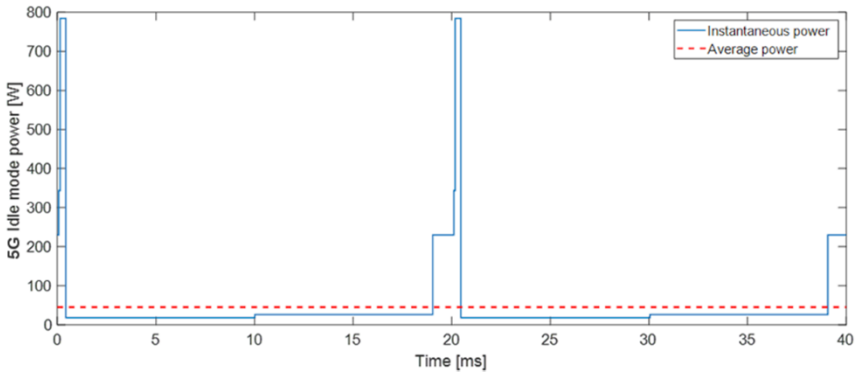
Per ovviare a questo limite, è necessario progettare con accuratezza la dislocazione dell'attrezzatura, rendendo necessarie analisi molto accurate per avere efficienza e flessibilità

Grazie alla flessibilità architetturale dello standard 5G, si possono ripensare le infrastrutture cellulari sulla base di una filosofia carico-centrica, implementando architetture completamente basate sui servizi

5G: Efficienza Energetica

Impatto energetico operazionale





Un altro significativo miglioramento in termini di consumi energetici è dato dalle ottimizzazioni del traffico di rete a basso carico in seno allo standard 5G

Il 5G ottimizza il funzionamento dell'attrezzatura impostando velocemente i componenti in modalità a basso consumo durante qualsiasi gap di traffico nelle trasmissioni dati

Questa funzionalità viene chiamata **MICRO-SLEEP TRANSMISSION**, ed è stata notevolmente espansa rispetto allo standard 4G, che prevedeva gap della durata massima di 0.2 ms

Nel 5G in architettura SA, questo intervallo può arrivare fino a 20 ms, quindi due ordini di grandezza in più.

È stato possibile ampliare in modo così marcato questi tempi massimi per via di un'altra caratteristica del 5G chiamata **ULTRA-LEAN DESIGN**, che permette di mandare segnali di controllo e di sincronizzazione molto meno frequentemente che con il 4G senza inficiare la qualità del servizio

- Conclusioni -

Il 5G rappresenta un'evoluzione significativa delle reti cellulari, in cui il software gioca un ruolo preminente. Software-Defined Networking, Network Function Virtualization e tecnologie Cloud sono alla base dello standard, aumentando la flessibilità delle reti e permettendo di ripensare in modo innovativo la loro infrastruttura per offrire velocità prima riservate a reti in fibra ottica, comunicazioni ultra affidabili, latenze minime ed elevata connettività

Per quanto lo standard includa meccanismi di sicurezza per garantire comunicazioni cifrate e integrità dei messaggi, rimangono purtroppo aperte una serie di vulnerabilità, anche in virtù del sostanziale abbassamento delle barriere tecnologiche presenti per l'accesso a malware e strumenti relativi

Attacchi DDoS, Radio Jamming, Ramsonware, e contro la privacy richiedono l'accorta implementazione di politiche di network slicing e la considerazione della sicurezza sia con un approccio orizzontale che verticale

Il 5G è anche frutto dell'innovazione portata avanti nel tempo con gli standard precedenti, ed un punto chiave della nuova tecnologia è la sua potenzialità di migliorare notevolmente l'efficienza energetica

Architetture multi-radio, micro-sleep transmissions, ed ultra-lean design permettono marcati risparmi energetici, aspetto fondamentale per le implicazioni sia economiche che sociali