di Giovanni Nazzaro

LE SFIDE DEL 5G PER L'AUTORITÀ GIUDIZIARIA E LE FORZE DI POLIZIA

Giovanni NAZZARO, *Lawful Interception Consultant* e *Security Manager*, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni, esperto in *security*, *legal* e *compliance* in tali ambiti. Dal 2001 si occupa della progettazione dei sistemi d'intercettazione e di data retention in uso agli operatori di telecomunicazioni mobili, fisse, wifi, satellitari. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della"*Lawful Interception Academy*" dal 2014, è promotore della *LIA Certification* per la certificazione degli apparati LEMF e dei processi aziendali della funzione Judicial Authority Services, secondo i criteri della LIA. Si occupa di formazione ed è docente a contratto per il Ministero di Giustizia, in Master Universitari di I e II livello.

Council of the European Union, Law enforcement and judicial aspects related to 5G - Brussels, 6 May 2019

Il 5G è molto più che un'evoluzione del 4G ma porta con sé problematiche d'interesse per l'Autorità Giudiziaria e per le forze di polizia che il Consiglio Europeo ha elencato nel suo documento del 6 maggio 2019. A differenza di quanto invece riportato da alcuni organi di stampa italiana che hanno commentato il documento di Bruxelles, molte di queste problematiche non sono ostacoli insuperabili ma sfide che possono essere affrontate e superate a livello nazionale mediante un'opportuna legislazione da sviluppare, sebbene il nostro paese non sia riuscito a farlo per tutte le precedenti tecnologie dal 2G al 4G.

1. *Introduzione*

Il 5G è molto più che un'evoluzione del 4G perché prospetta velocità di trasferimento significativamente più elevate mediante connessioni a banda larga mobile migliorate, tempi di risposta (latenza) più brevi, connessioni ultra-affidabili e un Internet of Things (IoT) sicuro.

Il 5G diventerà la spina dorsale di una varietà di modelli di business come la guida interconnessa e autonoma, la telemedicina, smart grids, smart cities ecc., più in generale tutta la gamma delle applicazioni IoT. Il mercato dei 5G sarà un business da mille miliardi di dollari.

Attualmente a livello mondiale solo 5 aziende forniscono la rete di accesso radio al 5G, due delle quali europee (Ericsson e Nokia), due cinesi (Huawei e ZTE) e una sudcoreana (Samsung), quindi non ci sono aziende americane. Ecco perché la UE sta sostenendo l'autonomia tecnologica e la leadership delle aziende europee nel 5G.

2. *Architettura del 5G*

L'Internet of Things richiederà una progettazione delle reti mobile differente rispetto al passato, quando le comunicazioni erano solo di tipo HTC (Human Type Communication) cioè di tipo umano. L'aspetto più caratteristico che emergerà in questo passaggio tecnologico si basa sul fatto che oggi il numero di utenti mobili è piccolo se paragonato a quello che ci sarà a breve con l'avvento dello IoT, inoltre la quantità di dati scambiati è superiore rispetto alle trasmissioni sporadiche che faranno le macchine. Cambiando il paradigma da pochi utenti (umani) con molto traffico ciascuno a molti utenti (umani e macchine) con poco traffico ciascuno, alla fine la quantità di dati scambiati sarà enormemente superiore ma soprattutto distribuita.

La nuova core network del 5G è stata progettata non da una singola nazionale o un singolo produttore ma a livello mondiale dal 3GPP, che ha completato a fine 2016 lo studio di fattibilità. I risultati della nuova Core Network 5G (5GC) sono stati documentati a seguire e nel 2017 - 2018 c'è stata la completa attività normativa di specifica dell'architettura, delle procedure, degli aspetti protocollari e di radio 5G, fino ad arrivare a giugno 2018 con specifiche tecniche implementabile da parte dei costruttori di reti.
E' cambiato molto ma non tutto rispetto al passato: come il 4G Evolved Packet Core (EPC) il 5GC aggregerà il traffico dati dei dispositivi finali. Il 5GC riuscirà anche ad applicare politiche personalizzate di gestione della mobilità dei dispositivi prima di instradare il traffico verso i servizi del rispettivo Operatore o verso Internet.

Le differenze, invece, sono importanti in quanto il 5GC è scomposto in un numero di elementi Service-Based Architecture (SBA) ed è progettato da zero per il controllo completo e la separazione del livello utente. Il 5GC comprendrà funzioni di rete (o servizi) virtualizzati, basati su software, e potrà quindi essere stanziato all'interno di infrastrutture cloud di tipo Multi-access Edge Computing (MEC) conosciuto come Mobile Edge Computing. Il cuore della nuova architettura del 5G è proprio la progettazione di software cloud nativo.

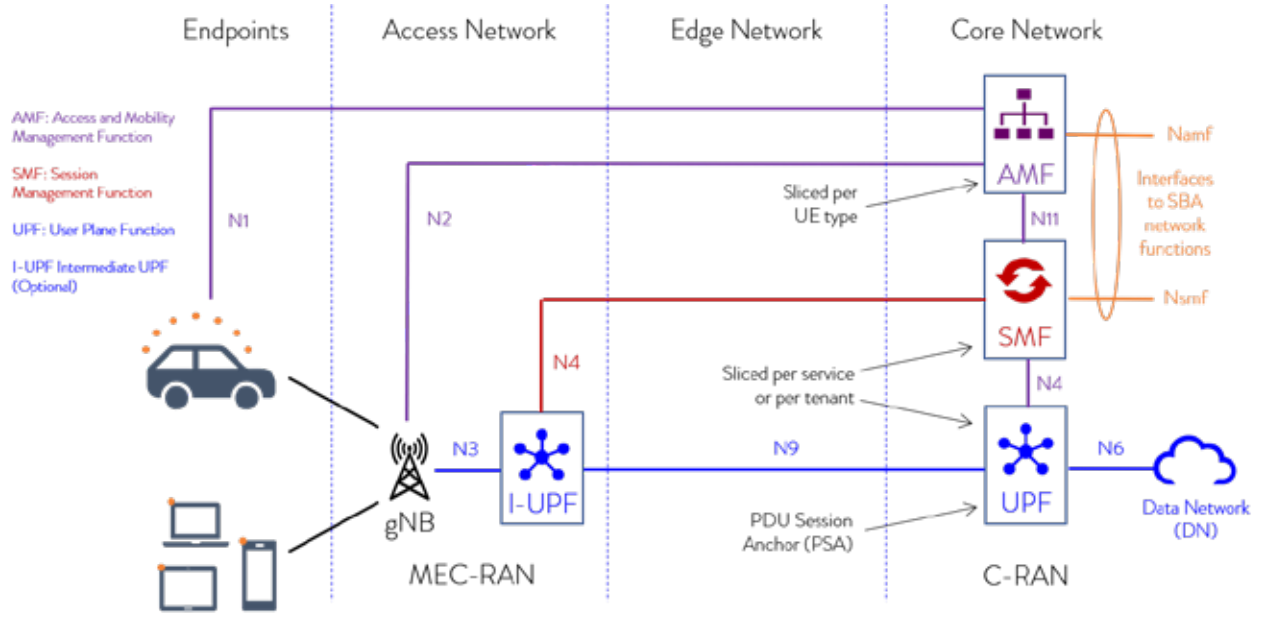

Figura 1 - Architettura del 5GC con il dettaglio della funzionalità di User Plane Function (UPF) (Fonte Metaswitch)

Elenchiamo di seguito le principali nuove funzioni di rete del 5G:

a) **User Plane Function (UPF)**. Nella separazione del piano di controllo delle sessioni dati da quello dei dati d'utente, l'UPF del 5GC rappresenta l'evoluzione della funzione del Packet Gateway (PGW) svolta sul piano dati. Questa separazione consentirà l'inoltro e il ridimensionamento dei dati in modo indipendente, in modo che l'elaborazione dei pacchetti e l'aggregazione del traffico possano essere distribuiti sulla rete. Per Le UPF e le piattaforme di servizio potranno essere così dispiegate quanto più possibile vicino ai dispositivi da controllare. UPG quindi rappresenta il punto di ancoraggio della sessione Protocol Data Unit (PDU) per fornire mobilità all'interno e tra le tecnologie di accesso radio (RAT), incluso l'invio di uno o più pacchetti di marcatori finali al gNB. A differenza di quanto accade nelle reti 4G, dove tutte le sessioni dati dell'utente sono ancorate al nodo SGW, nella 5GC diverse sessioni di dati d'utente possono essere ancorate ad UPF diverse.
UPG rappresenta il punto di interconnessione tra l'infrastruttura mobile e la rete dati (DN) ed effettua l'incapsulamento e la decapsulazione del GPRS Tunneling Protocol per il piano utente (GTP-U). Per tale motivo UPG può effettuare un rilevamento delle applicazioni mediante modelli di filtro del traffico SDF (Service Data Flow) ed un rapporto sull'utilizzo del traffico per la fatturazione. Infine, UPG si interfaccia con i sistemi di Lawful Interception (LI).

b) **Session Management Function (SMF)**. Componente fondamentale dell'architettura SBA, SMF è responsabile dell'interazione con il piano dati disaccoppiato, creando, aggiornando e rimuovendo le sessioni di Protocol Data Unit (PDU) e gestendo il contesto di sessione all'interno dell'UPF. SMF svolge anche il ruolo di server DHCP (Dynamic Host Configuration Protocol) e di sistema per l'IP Address Management (IPAM). Per soddisfare i requisiti architetturali del 5G, SMF deve essere interamente progettato e fornito come una funzione di rete Cloud-Native.

c) **Access and Mobility Management Function (AMF)**. Con la 4G EPC mobility Management Entity (MME) scomposta in due elementi funzionali, l'AMF riceve tutte le informazioni relative alla connessione e alla sessione dall' User Equipment (UE) ma è responsabile solo per la gestione delle attività di connessione e della mobilità. Tutto ciò che riguarda la gestione delle sessioni viene inoltrato alla Session Management Function (SMF) visto in precedenza. Una rete mobile comprende molte istanze AMF,

quindi viene utilizzato un identificatore AMF (GUAMI) globalmente univoco. L'UE specifica il proprio identificativo GUAMI nel primo messaggio NAS (Non-Access Stratum) che invia, che viene instradato all'AMF richiesto dalla rete di accesso radio (RAN). L'identificativo GUAMI è applicabile sia all'accesso 3GPP sia all'accesso non-3GPP, quindi garantisce anche che i messaggi provenienti da una UE, registrati attraverso entrambe le reti di accesso, vengano inoltrati allo stesso AMF.

Essendo il punto di accesso al 5GC, terminando così il piano di controllo RAN e il traffico UE che origina dall'interfaccia di riferimento N1 o N2, AMF implementa gli algoritmi di cifratura e integrità della NAS. Dopo il messaggio NAS iniziale con il GUAMI, l'AMF invia una richiesta di Authentication and Key Agreement (AKA), in modo equivalente all'MME nelle infrastrutture Evolved Packet Core (EPC). Tuttavia, a differenza dell'MME, l'AMF inoltra alla SMF in modo trasparente la segnalazione relativa alla creazione ed alla gestione delle sessioni dati d'utente. Infine, al fine di inviare informazioni sugli eventi, l'AMF si collega ai sistemi Lawful Intercept (LI).

Queste sono solo alcune delle nuove funzioni di rete dell'architettura basata sul servizio 5G Core. Vediamo altre:

- **Uplink Classifier**: una UPF può selezionare determinati flussi di traffico nell'ambito di una sessione dati d'utente e ridirigerli verso una rete locale dove, ad esempio, possono essere collocate piattaforme di MEC (Mobile Edge Computing).
- **Branching Point**: una UPF può anche distribuire una sessione dati verso altre UPF, tutte agganciate alla stessa rete dati, e abilitare uno dei nuovi schemi di gestione della mobilità Session Service Continuity (SSC) introdotti nella rete 5G.

- **Session e Service Continuity (SSC)**: le modalità SSC possono essere tre: la prima è quella più tradizionale (SSC 1), in cui l'ancoraggio dell'IP è stabile, cioè la connessione dati viene spostata da un punto di aggancio alla rete ad un altro preservando l'indirizzo IP, per fornire un supporto continuo alle applicazioni e per la manutenzione del percorso verso l'UE man mano che la posizione viene aggiornata. Le altre due modalità break-before-make (SSC 2) e make-before-break (SSC 3) consentono di riposizionare l'ancoraggio IP, cioè l'indirizzo IP può variare al cambiare del punto di aggancio alla rete della connessione dati.

- **Mobile Initiated Connection Only (MICO)**: è una funzionalità del tutto nuova rispetto al 4G, orientata al settore dei device che devono poter funzionare con bassissimo consumo della batteria, affinché questa non venga sostituita per molti anni. Un device in modalità MICO si trova nello stato IDLE e quindi non controlla il canale radio di paging. L'AMF lo considera irraggiungibile e differisce la consegna del traffico terminato fino a quando non passa dallo stato di IDLE a CONNECTED per trasmettere, ad esempio, i dati relativi ad una segnalazione.

I cambiamenti sono piuttosto radicali rispetto al 4G ed uno dei fattori più importanti che farà decollare la nuova architettura sarà la progettazione Cloud-Native e le relative metodologie di implementazione ovvero la virtualizzazione delle funzioni di rete (Network Functions Virtualisation - NFV).

3. *Il Multi-access Edge Computing (MEC)*

Il Multi-access Edge Computing (MEC) è una specifica dell'ETSI Industry Specifications Group (ISG) definita all'inizio del 2016. In origine era stato definito come Mobile Edge Computing, ma il primo termine è stato cambiato dopo qualche mese per comprendere tutte le tipologie di accesso (wireless e wireline). I documenti ETSI MEC ISG in evoluzione sono disponibili a questo link https://www.etsi.org/technologies/multi-access-edge-computing (oggetto di un prossimo articolo su questa rivista).
Le infrastrutture Multi-Access Edge Computing consentono l'implementazione di funzionalità della rete mobile solo software o di applicazioni SaaS (Software-as-a-Service) che operano all'interno di una piattaforma di virtualizzazione standardizzata vicino ai bordi della rete.
L'architettura di riferimento MEC è composta da due aree funzionali, Host e Management. La combinazione di questi elementi funzionali fornisce le basi necessarie per la scalabilità di applicazioni e servizi mobili in modo altamente granulare e dinamico. Il Virtualization Infrastructure Manager (VIM) è il componente più importante dell'architettura ETSI NFV ISG, essendo responsabile per l'allocazione, la gestione e il rilascio di risorse di elaborazione, storage e networking virtualizzate.
Il livello di Management comprende le entità amministrative sia dell'host che quelle di sistema. Il cuore dell'Host per dispositivi mobili è l'infrastruttura di virtualizzazione, che fornisce alle applicazioni mobili risorse di elaborazione, storage e di rete. La funzionalità del piano dati, all'interno dell'infrastruttura di virtualizzazione, applica le regole e le liste di controllo dell'accesso durante il routing del traffico tra servizi di rete e applicazioni mobili. Questi possono essere locali all'Host o esterni, su Host residenti in altre reti anche estere.

4. *Aspetti di interesse per l'Autorità Giudiziaria e le Forze di polizia*

Il 22 marzo 2019 il Consiglio Europeo ha espresso il proprio sostegno a un approccio concertato alla sicurezza delle reti 5G. Nella sua raccomandazione, adottata il 26 marzo, la Commissione stabilisce una serie di misure operative, al fine di valutare le vulnerabilità delle reti 5G e una migliore gestione di tali rischi, sia a livello nazionale che europeo. Secondo un programma rigoroso 2019 (per le date del programma si veda "Reti mobili 4G e 5G: siamo proprio sicuri?" di Giovanni Nazzaro, su "Sicurezza e Giustizia" numero I del MMXIX, https://www.sicurezzaegiustizia.com/reti-mobili-4g-e-5g-siamo-proprio-sicuri/), le valutazioni nazionali dei rischi dovrebbero essere completate entro la fine di giugno. L'obiettivo è la definizione di un insieme di strumenti per la sicurezza informatica (requisiti di certificazione, test, controlli, identificazione di prodotti non sicuri) da utilizzare a livello nazionale dagli Stati membri.

Il 6 maggio 2019 il Consiglio Europeo, prendendo anche spunto dal *position paper* 8268/19 sul 5G dell'Europol, ha evidenziato alcune problematiche dal punto di vista dell'Autorità Giudiziaria e delle forze di polizia. E' importante subito sottolineare, a differenza di quanto invece riportato da alcuni organi di stampa italiana, che molte di queste problematiche sono in realtà sfide che possono essere affrontate a livello nazionale, non solo europeo o internazionale, mediante un'opportuna legislazione da sviluppare. Parte di questa disinformazione è comunque servita per alzare l'attenzione sul tema, considerando che nel nostro paese non si è mai riusciti a regolamentare tecnicamente le modalità di intercettazione o, più in generale, l'erogazione delle prestazioni obbligatorie ex art. 96 del Codice delle Comunicazioni italiano, come lo dimostrano le attuali problematiche sul VoLTE. Il riferimento è al decreto interministeriale del 28 dicembre 2017, che all'art. 7 istituiva presso il Ministero della giustizia un tavolo tecnico permanente di cui tutt'oggi si ignora l'esistenza, la composizione e le attività (nell'ipotesi positiva che si sia costituito).
In linea con il nostro CCE anche il Codice europeo delle telecomunicazioni elettroniche del 2018 stabilisce che le autorità nazionali di regolamentazione possono rilasciare qualsiasi approvazione relativa al 5G in base alla capacità dei fornitori di rete di effettuare il monitoraggio delle comunicazioni.

5. *Le sfide correlate al 5G*

Per quanto sopra esposto, sarà necessario regolamentare i requisiti funzionali d'intercettazione legale delle comunicazioni sull'architettura frammentata e virtualizzata del 5G, altrimenti si perderà l'accesso a dati preziosi. In particolare, gli aspetti evidenziati dal documento del Consiglio Europeo sono legati ai seguenti specifici ambiti:

1) la crittografia
2) l'architettura frammentata e virtuale
3) l'autenticità delle prove
4) la disponibilità della rete dal punto di vista delle forze dell'ordine

5.1. *La crittografia*

Il 5G offrirà standard di sicurezza molto elevati. Sebbene la crittografia end-to-end non sia ancora impostata come obbligatoria negli standard 5G, non si può escludere che sarà inclusa nel processo di standardizzazione che sarà completato nel dicembre 2019. La crittografia end-to-end renderebbe impossibile accedere ai contenuti nelle comunicazioni elettroniche, anche attraverso intercettazioni legali.
La crittografia del numero IMSI (è il numero individuale della scheda del telefono cellulare) renderebbe impossibile – per le forze dell'ordine e le autorità giudiziarie – identificare i dispositivi mobili o la posizione di coloro che rappresentano una seria minaccia per la sicurezza nazionale, nonché delle potenziali vittime che si trovano di fronte a tale minaccia. Senza accesso al numero IMSI, le intercettazioni legali che si basano su questo parametro non saranno possibili.
Il 5G avrà rigorosi processi di autenticazione (per identificare un utente prima che gli venga concesso l'accesso) che renderà più difficile alle forze dell'ordine effettuare l'indagine senza essere rilevati (ad esempio non potranno essere usati gli attuali IMSI-catcher necessari per la rilevazione di dispositivi mobili e la localizzazione dei sospetti).

5.2. *L'architettura frammentata e virtuale*

Diversi fornitori di reti e servizi potrebbero essere in grado di operare sulla stessa infrastruttura fisica. Ogni fornitore di servizi utilizzerà un livello virtuale personalizzato della stessa infrastruttura fisica, con specifiche tecniche diverse. Le informazioni derivanti dal monitoraggio delle comunicazioni potrebbero, pertanto, non essere disponibili in ogni sezione della rete. In pratica, con la rete 5G, i fornitori di servizi e di rete non possono – se non sono obbligati a farlo – avere una copia completa delle informazioni disponibili, che renderebbe impossibile l'intercettazione legale.
Il Multi-access Edge Computing (MEC) consentirà alle reti di telefonia mobile di archiviare ed elaborare contenuti in cloud decentralizzati in prossimità degli utenti della rete, che potranno comunicare direttamente tra loro. Le informazioni non saranno necessariamente dirette tramite nodi centrali , dove oggi l'intercettazione è implementata.
Abbiamo visto che gli elementi dell'architettura frammentata potrebbero essere fisicamente all'estero, quindi per monitorare le comunicazioni, in futuro, si potrebbe richiedere la cooperazione di numerosi fornitori di rete sia in Italia che all'estero, sotto diverse giurisdizioni. L'instaurazione di una cooperazione internazionale può allargare il periodo temporale tra richiesta e implementazione dell'intercettazione, con un rischio non trascurabile di perdere un copia completa delle informazioni.

5.3. *L'autenticità delle prove*

Data la moltitudine di attori coinvolti nel fornire le reti 5G, potrebbe essere più difficile stabilire l'autenticità delle prove e distinguere le prove false da quelle reali.

5.4. *La disponibilità della rete dal punto di vista delle forze dell'ordine*

Nel campo della cybersicurezza, l'utilizzo del 5G richiede di menzionare le comunicazioni mission critical (MCC), definite come la capacità di fornire mezzi di comunicazione in cui le reti convenzionali non possono soddisfare la richiesta, tipicamente in aree colpite da disastri o incidenti di sicurezza pubblica in cui le reti mobili convenzionali non funzionano, lasciando i primi soccorritori sul posto senza alcun mezzo di comunicazione.
L'aumento globale della minaccia del terrorismo sta spingendo i governi a migliorare la sicurezza pubblica attraverso il coordinamento tempestivo tra diverse forze di polizia, vigili del fuoco, servizi medici di emergenza ecc.
Con la sua alta affidabilità e bassa latenza, il 5G offre grandi potenziali per sostituire le vecchie reti, ma deve essere tenuto al sicuro dagli attacchi informatici e da altri fattori esterni di interferenza. ©