L'aumento del traffico dati può portare alla congestione delle risorse radio per l'accesso alle reti mobili cellulari. Per ovviare a tale problema gli operatori mobili possono ricorrere al "*WiFi offloading*" che richiede tuttavia una particolare attenzione sotto il profilo delle intercettazioni mobili richieste dall'Autorità Giudiziaria.

Armando FRALLICCIARDI possiede un'approfondita conoscenza sulla tecnologia delle reti fisse e mobili. Ha partecipato a gruppi di lavoro per la definizione di metodi e sistemi d'intercettazione conformi agli standard ETSI e 3GPP e in diversi casi ha fornito la sua collaborazione in importanti indagini a supporto del'AG. È Vice Presidente dell'associazione ELISS.

Giovanni NAZZARO, ing. delle telecomunicazioni, opera nell'*information technology* e nelle reti di telecomunicazioni ed è esperto in *security* e *compliance* in tali ambiti, con particolare riferimento alle c.d. "Prestazioni obbligatorie per l'AG". Nel 2005 ha fondato l'associazione *Experts of Lawful Interception and Security Standards* (ELISS), di cui è Presidente. È Direttore responsabile delle riviste tecnico-giuridiche "Sicurezza e Giustizia" e "Il Documento Digitale". Docente a contratto, autore di monografie e numerosi articoli, direttore di corsi di formazione, è ospite di seminari e convegni in qualità di relatore o moderatore.

WIFI OFFLOAD OF MOBILE DATA: L'INTERCETTAZIONE DELLE COMUNICAZIONI DI RETE MOBILE CON ACCESSO WIFI

di Armando FRALLICCIARDI e Giovanni NAZZARO

Negli ultimi anni il traffico dati sulle reti mobili è cresciuto costantemente, soprattutto a causa della diffusione dei dispositivi mobili intelligenti come *smartphone* e *tablet*, i cui utilizzatori chiedono connettività ad alta velocità in ogni momento ed appunto in mobilità. Le reti 3G UMTS con accesso HSDPA e le reti 4G LTE soddisfano questa esigenza, ma spesso i dispositivi hanno già applicazioni preinstallate ed attive per diversi tipi di servizi e questo aumenta ulteriormente la richiesta di banda creando situazioni di potenziale congestione sull'accesso radio.
Secondo uno recente studio di Cisco (*Cisco VNI Global Mobile Data Traffic Forecast Update 2013–2018*)[(1)] il traffico dati sulle reti mobili nel 2013 è aumentato dell'81% a livello globale e del 34% in Italia rispetto al 2012. Il suddetto rapporto stima che nel 2018 il volume di dati scambiati al mese dai dispositivi mobili sarà di 15,9 Exabyte (1 Exabyte equivale ad a 1 Trilione di byte).

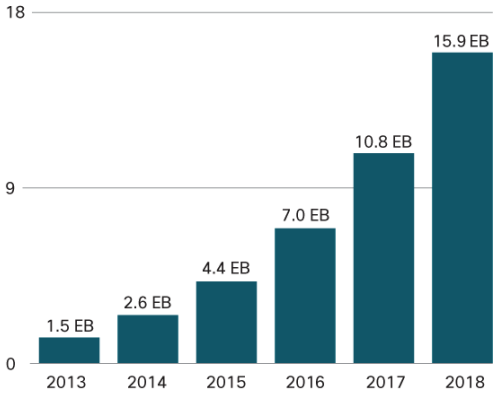

Figura 1: Cisco Forecasts 15.9 Exabytes per Month of Mobile Data Traffic by 2018 (fonte CIsco).

La disponibilità di accessi radio Wi-Fi in ambienti di lavoro o in aree pubbliche fornisce un soluzione per decongestionare l'accesso radio UMTS e LTE. Gli Operatori mobili sempre più spesso seguono strategie di *WiFi offloading* per ridurre la richiesta di banda sulle proprie reti radio di accesso 3G e 4G.

In generale con l'espressione "*Mobile Data Offloading*" si intende infatti l'uso di tecnologie di rete complementari (come ad esempio il Wi-Fi, il WiMAX o le Femtocelle) per fornire dati originariamente destinati alle reti cellulari. Le regole che innescano l'utilizzo di una rete di accesso di questo tipo possono essere impostate sia dall'utente finale (l'utente mobile) sia dallo stesso operatore.

Il rapporto della Cisco prevede che nel 2018 il 52% del traffico dati originato da dispositivi mobili sarà del tipo *Offload* contro il 48% di tipo cellulare.

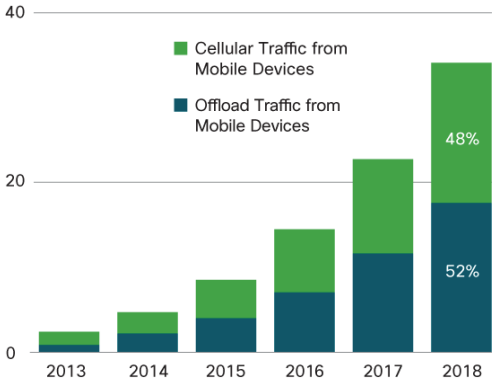

Figura 2: 52 Percent of Total Mobile Data Traffic Will Be Offloaded by 2018 (fonte CIsco).

Per quanto attiene i servizi che produrranno questi eccezionali valori di scambio dati, il rapporto della Cisco indica che il 69,1% sarà dovuto al *download* di video.

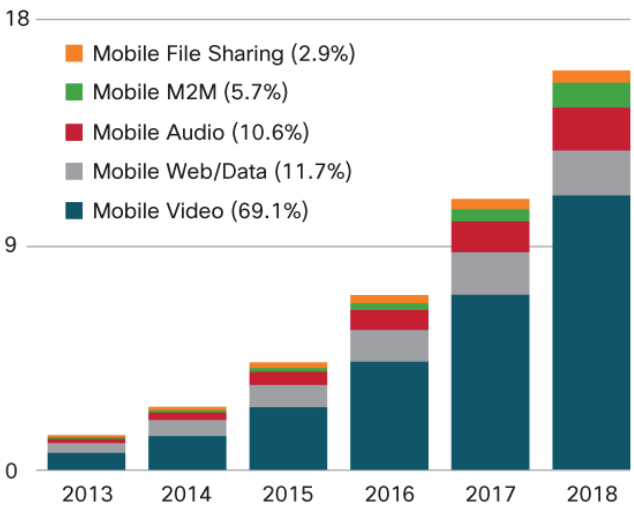

Figura 3: Mobile Video Will Generate Over 69 Percent of Mobile Data Traffic by 2018 (fonte CIsco).

La decongestione della rete si realizza, quindi, dando la possibilità agli utenti di accedere alla *Mobile Core Network* mediante *hotspot* Wi-Fi, anche di operatori diversi da quello di rete mobile, ogni volta che queste sono disponibili. Il vantaggio dell'utente è un costo minore per l'occupazione della banda a fronte però di una riduzione della mobilità. La strategia è efficace per l'operatore di rete mobile se il fenomeno è controllato, per evitare che l'utilizzo del WiFi da parte dell'utente possa prevalere, minacciando i propri ricavi da accesso UMTS/LTE.

In figura 4 è rappresentato il modello di architettura di accesso Wi-Fi ad una rete mobile. I dati provengono dalla Internet verso il dispositivo mobile, e viceversa, attraversando un segmento di architettura dove è applicata la cifratura degli stessi dati (*tunnel*), in particolare dal *Wi-Fi Gateway* (Wi-Fi GW) al *Packet Gateway* (P-GW). In merito alle architetture di accesso tramite rete Wi-Fi, è doveroso precisare che la 3GPP (*Third-Generation Partnership Project*) ha specificato una serie di tipologie definite appunto "*non-3GPP IP access*" (vedi specifica 3GPP TS 23.402[2]) che si divono in:

- ***non attendibile (Untrusted)***: comprende qualsiasi tipo di connessione Wi-Fi che o non è sotto il controllo dell'operatore (*hotspot* pubblico aperto, WLAN domestica dell'abbonato, ecc) o che non fornisce sufficiente sicurezza (autenticazione, crittografia, ecc.);
- ***attendibile (Trusted)***: si riferisce generalmente all'operatore di rete mobile che ha integrato l'accesso Wi-Fi con crittografia *over-the-air* e un metodo di autenticazione sicura. Questo tipo di accesso è nativamente integrato in LTE.

Ai fini dell'erogazione delle prestazioni obbligatorie per l'Autorità Giudiziaria (AG), che coinvolgono l'operatore mobile, con particolare attenzione alle intercettazioni delle comunicazioni, l'identificazione dell'utente che accede ad una rete mobile da Wi-Fi e la sua localizzazione sono i punti di attenzione che presentano la maggiore criticità. L'accesso agli *hotspot* Wi-Fi richiede agli utenti un'identificazione per la rete locale. Quando l'utente da Wi-Fi accede alla rete mobile il terminale deve ripetere il processo di autenticazione per simulare l'accesso UTRAN o E-UTRAN. In pratica l'architettura I-WLAN stabilisce un tunnel direttamente dal terminale d'utente al P-GW, attraverso il Wi-Fi Gateway, di conseguenza l'utente deve autenticarsi nuovamente quando accede alla rete mobile.
La ri-autenticazione con protocollo EAP avviene con trasferimento delle credenziali d'accesso tra i rispettivi sistemi di autenticazione (AAA) dell'*hotspot* e rete mobile come rappresentato in figura 4.

La figura 4 evidenzia anche che le funzioni d'intercettazione del traffico dati sono implementate nel *Packet Data Gateway* (P-GW) attraverso cui l'utente accede a Internet. Le funzionalità d'intercettazione duplicano il traffico (*payload*) in modo integrale inviandolo ai sistemi dell'Autorità Giudiziaria attraverso l'architettura ***ETSI standard*** che prevede le interfacce HI (1,2,3).
Nel flusso del *payload* è inserito l'*header* con le informazioni di correlazione per associare in modo univoco il traffico intercettato al determinato *target*. Lo standard 3GPP ha specificato un nuovo parametro, il ***Radio Access Technology*** (RAT), per consentire ai sistemi di ricezione dell'AG di riconoscere che la comunicazione intercettata proviene da un accesso Wi-Fi piuttosto che dalla tradizionale rete cellulare UTRAN. Il ***RAT type*** è definito in accordo allo standard

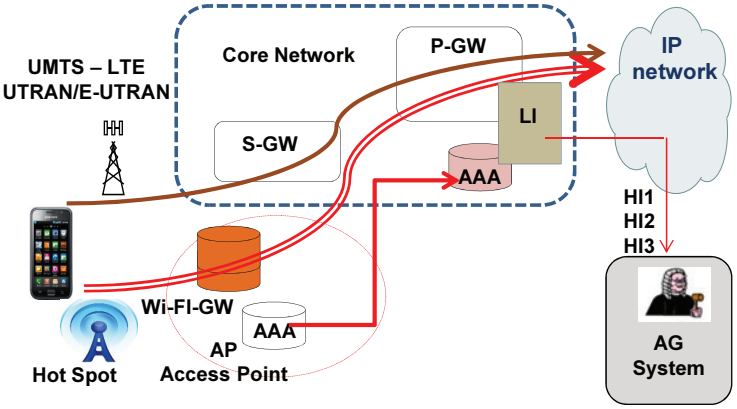

Figura 4: Modello di architettura di accesso Wi-Fi ad una rete mobile. Le funzioni d'intercettazione del traffico dati sono implementate nel Packet Data Gateway (P-GW).

3GPP TS 29.274[3] e può presentare, tra gli altri, i valori di "UTRAN" (*UMTS Terrestrial Radio Access Network*) e comunemente indicato come 3G, "GERAN" (*GSM EDGE Radio Access Network*), "WLAN" (*Wireless LAN*) come nel caso di Wi-Fi.

L'accesso Wi-Fi determina eventi che producono IRI con informazioni diverse rispetto all'accesso canonico UTRAN/E-UTRAN. Ad esempio l'informazione di localizzazione del target riporta l'informazione "*WLAN access point name*" in sostituzione della cella. Gli eventi che identificano un accesso Wi-Fi sono indicati nella seguente tabella.

Evento	Nota esplicativa
I-WLAN Access Initiation	Tentativo di accesso
I-WLAN Access Termination	Autenticazione
I-WLAN Tunnel Establishment (successful)	Connessione alla rete IP con successo
I-WLAN Tunnel Establishment (unsuccessful)	Connessione alla rete IP fallita
I-WLAN Tunnel Disconnect	Chiusura della connessione alla rete IP
Start of intercept with I-WLAN Communication Active	Attivazione dell'intercettazione con la connessione del target già attiva

Gli IRI prodotti dagli eventi indicati in tabella contengono le informazioni necessarie all'AG per rilevare che si tratta di un accesso Wi-Fi e quindi anche le informazioni contenute sono corrispondenti al tipo di accesso. **Le informazioni rilevanti che obbligatoriamente devono essere inviate ad AG, oltre a quelle che identificano il target e quelle di correlazione con il *payload*, sono il nome dell'*hotspot* e il parametro *"WLAN access point name"* per localizzare il *target***.
In conclusione, la diffusione delle architetture di *Wi-Fi offloading* rende complesse o critiche le operazioni d'intercettazione. La conformità agli *standard* delle funzionalità d'intercettazione degli operatori mobili e Wi-Fi, nonché dei sistemi di ricezione dell'AG, è la strada obbligata che permette di superare ogni criticità.©

NOTE

1. "*Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018*", *White paper, released February* 5, 2014.
2. 3GPP TS 23.402 "*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses*".
3. 3GPP TS 29.274 "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; (EPS); (GPRS); Tunnelling Protocol for Control plane (GTPv2-C); Stage 3". ◊