La sicurezza nell’era del 5G, Edge e Fog Computing

Author : Antonio Manzalini

Date : 23 Ottobre 2019

Il settore delle telecomunicazioni sta attraversando una rapida trasformazione, determinata dalla convergenza di una serie di tendenze tecnico-economiche, quali: il rapido progresso delle tecnologie dei semiconduttori (e delle relative capacità elaborative e di memoria) a costi sempre più bassi, la capillare penetrazione della banda ultra-larga, l’accelerazione delle prestazioni dell’informatica e dei sistemi di Intelligenza Artificiale. Inoltre, il progressivo sviluppo di Internet come rete globale sta conducendo a una digitalizzazione pervasiva in molti settori industriali (ad es. Industria 4.0, agricoltura di precisione, etc.), sociali (ad es. Smart City, media e servizi digitali).

Il 5G rappresenta una profonda trasformazione digitale e assume il ruolo di punto di convergenza di numerosi filoni di innovazione di rete e servizi. Tra questi filoni, si ricorda: la **softwarizzazione** delle reti, che ha come obiettivo principale la virtualizzazione delle piattaforme di rete e servizi digitali, per aumentarne flessibilità di dispiegamento e gestione; lo **sviluppo dell’accesso wireless** al fine di raggiungere, in opportune condizioni, prestazioni paragonabili a quelle dell’accesso fisso; l’**innovazione delle reti di trasporto, con accesso trasparente fisso-mobile,** basate su un utilizzo sempre più integrato e flessibile delle tecnologie IP su ottico; l’**evoluzione del Cloud Computing verso l’Edge ed il Fog Computing**.

Software Defined Network (SDN) e Network Function Virtualization (NFV) sono due delle principali tecnologie del 5G, abilitanti, rispettivamente, il disaccoppiamento del software dai sistemi hardware e la virtualizzazione delle funzionalità di rete e servizi (figura 1). Queste tecnologie conferiranno al 5G alti livelli di flessibilità e programmabilità (ad es. attraverso API). L’infrastruttura di rete acquisterà così una nuova “plasticità” tale da renderla capace di adattarsi rapidamente, e in maniera efficace, alle richieste del marcato: da un’architettura di rete relativamente statica e chiusa si passa dunque ad un’architettura che ha due livelli di definizione, quello hardware e quello software.

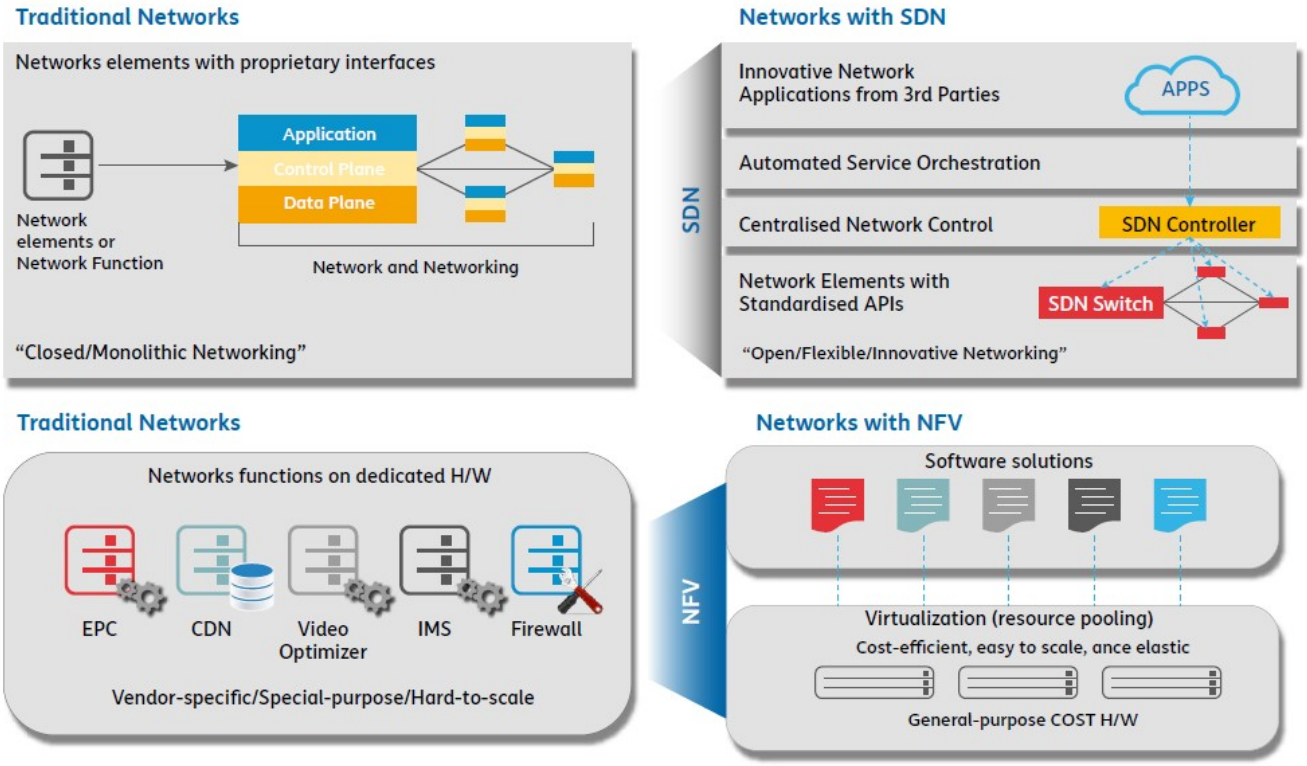

Figura 1: Il cambio di paradigma portato dall'introduzione di tecnologie come SDN e NFV (fonte: GSMA)

L'evoluzione del Cloud Computing verso l'Edge e Fog Computing contribuirà ad alimentare lo spostamento delle risorse fisiche, logiche e quindi dell'intelligenza di rete e servizio, verso le zone più periferiche della rete, più vicine agli utenti, addirittura fino ai terminali. È dimostrato infatti che l'integrazione dei sistemi di Edge e Fog Computing [1], [2] nell'infrastruttura 5G costituirà un fattore essenziale per abbassare i tempi di latenza richiesti dai servizi digitali del futuro, e quindi aumentarne le prestazioni. L'Edge Computing, inoltre permetterà di abilitare nuovi scenari servizi, difficilmente realizzabili solo con infrastrutture di Cloud Computing (ad es. *smart road* e *connected car, multi-media entertainment, drone remote piloting*, etc).

In tale contesto evolutivo, la sicurezza è un tema centrale: la sofwarizzazione, la sempre maggior penetrazione delle connessioni a banda ultra-larga e il dispiegamento pervasivo di risorse IT (Information Technology) più vicine agli utilizzatori sono fattori che aumentano i potenziali punti di vulnerabilità e attacco informatico.

In particolare, i tre principali punti di attenzione riguardano: i sistemi IT, la rete ed i terminali. Com'è noto, infatti, già oggi molti servizi digitali sono gestiti e controllati da sistemi IT e anche per il 5G si prevede una sempre maggiore migrazione verso infrastrutture Cloud-Edge Computing, ampliando così la possibile superficie di attacco informatico. Inoltre, la rete è di fatto

una delle Infrastrutture Critiche alla base del funzionamento di numerose industrie (energia, *utilities*, servizi pubblici, finanza, etc): le minacce sono molteplici e riguardano la resilienza (attacchi DDoS), intercettazione delle comunicazioni, difficoltà individuazione e blocco del traffico malevolo. Il terzo contesto, quello dei terminali (ad es. gateway, PC, cellulari, dispositivi intelligenti dell'Internet delle Cose, etc), è per sua natura capillare e quindi largamente vulnerabile a diversi tipi di attacchi, anche attraverso la creazione e diffusione di botnet.

I **requisiti di sicurezza (riservatezza, disponibilità e integrità) si riflettono inevitabilmente anche negli ambiti della privacy** (protezione dei dati delle persone) **e della resilienza** (garanzia del servizio erogabile anche in caso di degrado della rete). In tal senso, le due principali dimensioni di protezione da attacchi riguardano la **protezione preventiva e protezione reattiva**: la prima è volta a proteggere i sistemi e la rete mediante analisi del rischio e l'implementazione di contromisure (security by-design e monitoraggio continuo); la seconda ha l'obiettivo di minimizzare gli impatti a seguito di un attacco e quindi si basa su tutta una serie di misure adeguate per reagire a un eventuale incidente di sicurezza.

Un esempio sul ruolo chiave dell'Intelligenza Artificiale

Le contromisure preventive e reattive della sicurezza possono oggi contare sulla disponibilità di un'enorme quantità di dati di rete, che vanno dal numero dei possibili allarmi, agli eventi, dai log al minuto ai pattern di traffico. Questa ricchezza di dati, d'altro canto, rende impossibile un'analisi efficace con soli operatori umani: le metriche di utilizzo a disposizione sono molteplici, e soprattutto, l'efficacia di un intervento richiede un'attuazione decisionale molto rapida. Stanno così nascendo diverse soluzioni basate su metodi di big data analitycs e Intelligenza Artificiale.

A.I.^{2} rappresenta un interessante esempio di come l'analisi, da parte di un operatore umano di situazioni a possibile rischio di sicurezza, viene complementata, in fase elaborativa e decisionale, da rapidi sistemi di Intelligenza Artificiale (da cui il nome Artificial Intelligence al quadrato). Come riportato in figura 2 il sistema A.I.^{2} integra le capacità analitiche di un operatore umano, esperto nel rilevare le situazioni a rischio, con una piattaforma di big data analytics in grado di apprendere (*supervised* e *unsupervised learning*) [3] e proporre decisioni.

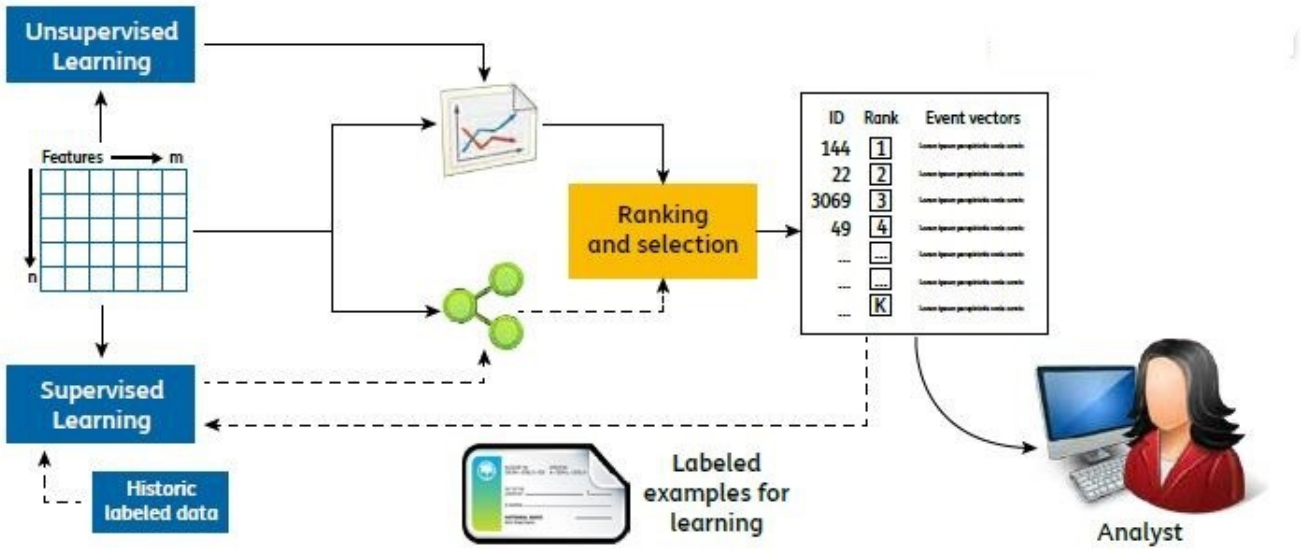

Figura 2 – AI2 : esempio di sistema di sicurezza basato su Intelligenza Artificiale (Fonte [1])

Conclusioni

Il 5G sarà molto di più di una evoluzione lineare della rete mobile LTE con nuovi sistemi di accesso e *core*, maggiore banda, migliori prestazioni e di ridotti consumi. **Il 5G si preannuncia, infatti, come un'innovativa piattaforma di rete e servizi digitali capace di soddisfare le future richieste dell'industria e della Società Digitale.**

La sofwarizzazione, la sempre maggior penetrazione delle connessioni a banda ultra-larga e il dispiegamento pervasivo di risorse IT più vicine agli utilizzatori sono fattori che aumentano i potenziali punti di vulnerabilità ed attacco informatico. La sicurezza *end-to-end* dei servizi assume un ruolo di fondamentale importanza e richiede il coinvolgimento di diversi stakeholder con l'impiego di un framework di processi e tecnologie in grado di mitigare le diverse minacce presenti sull'intera catena.

I **principali punti di attenzione per lo sviluppo di soluzioni di protezione preventiva e protezione reattiva riguardano: i sistemi IT, la rete e i terminali.** Entrambe queste direzioni possono contare su avanzati metodi di *big data analitycs* e Intelligenza Artificiale.

Bibliografia

[1] ETSI MEC - http://www.etsi.org/index.php/news-events/news/1078-2016-04-etsi-mobile-edge-computing-publishes-foundation-specifications;

[2] Industrial Internet Consortium - https://www.iiconsortium.org/index.htm;

[3] Veeramachaneni, Kalyan, et al. "AI^ 2: Training a Big Data Machine to Defend." Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016.

Articolo a cura di **Antonio Manzalini**