WP1: Servizi Big Data in rete 5G

Ernesto Damiani

Premessa

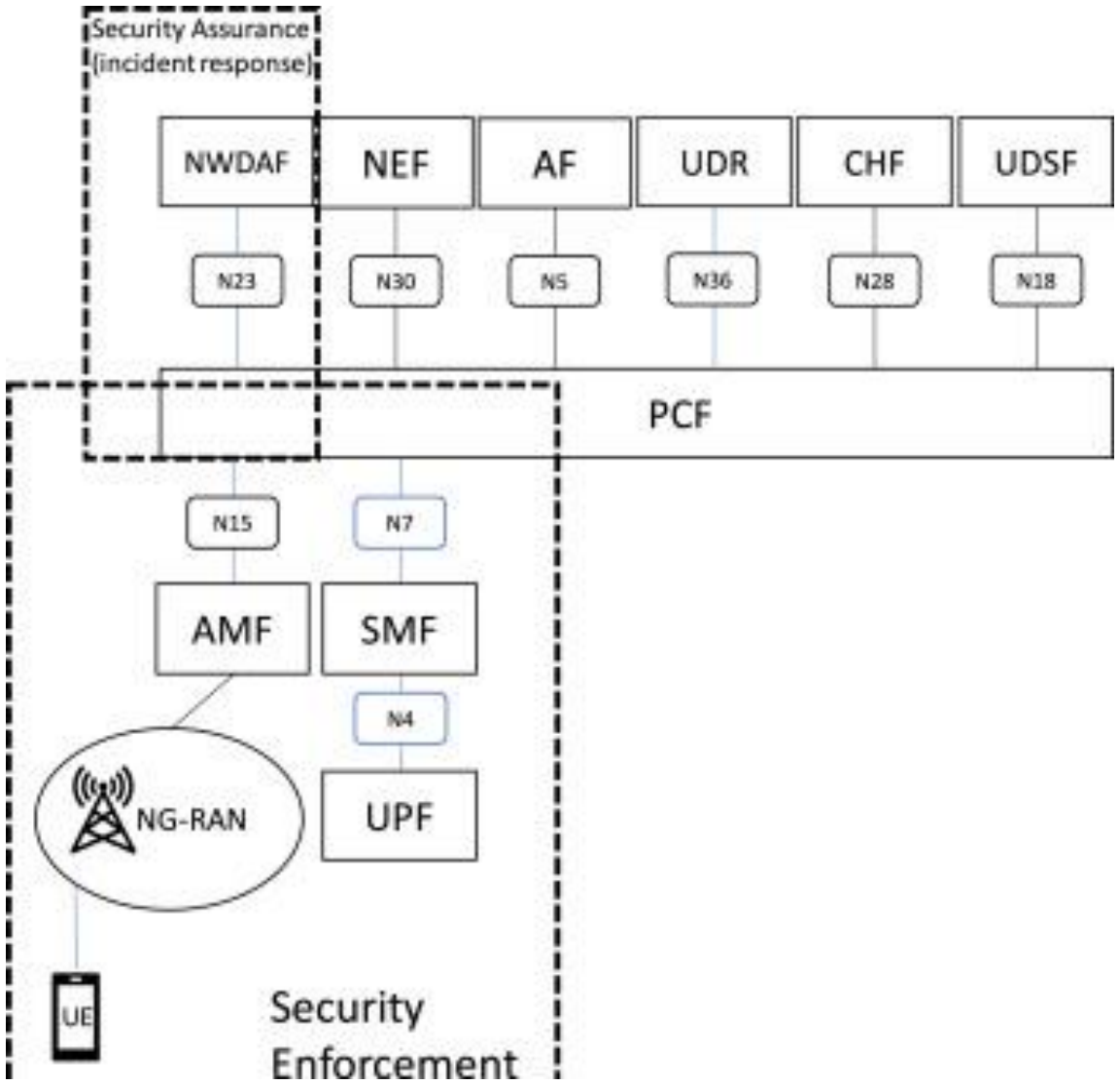
- C'è un vasto consenso nel settore sulla necessità di costruire reti di quinta generazione (5G) intrinsecamente sicure nel senso più ampio.
- Precauzioni sulla privacy e la riservatezza dei dati
- Obiettivi: protezione generale della rete da qualsiasi tipo di attacco informatico che possa compromettere la disponibilità e l'integrità della sua infrastruttura, applicazione e servizi.

5G e sicurezza

- Il 5GS è definito da 3GPP in TS 23.501 come un sistema composto da 5G Access Network (AN), 5G core network e User Equipment (UE). L'architettura del sistema è orientata ai servizi e comprende più Network Functions (NFs)
- La sicurezza della rete riguarda la definizione e l'applicazione delle politiche di sicurezza nell'intera rete, il cosiddetto 5G System (5GS) dagli standard 3rd Generation Partnership (3GPP).
  - Esistono diversi organismi chiave di standardizzazione e forum di settore che stanno contribuendo allo sviluppo dell'architettura 5G, e in particolare dei suoi aspetti di sicurezza, come ITU, ETSI, IETF, NGMN, 5G-PPP, NIST, GSMA, ecc.
- Alcuni di questi enti si concentrano su infrastrutture specifiche come le infrastrutture critiche e altri sviluppano standard di sicurezza per casi d'uso specifici (ad es. healthcare e mission critical) [4].
- Il gruppo di standardizzazione che definisce gli aspetti di sicurezza end-to-end nella rete 5G nel suo insieme è il gruppo di lavoro SA3 di 3GPP.

Principi

- Lavori di ricerca accademica come il progetto 5G-ENSURE nell'ambito del 5G-PPP (5G Infrastructure Public Private Partnership) hanno contribuito all'architettura di sicurezza 5G, fornendo una serie di principi di progettazione della sicurezza e un insieme di funzioni e meccanismi di sicurezza per attuare i controlli di sicurezza necessari per raggiungere gli obiettivi di sicurezza desiderati.
- La Policy Control Function (PCF) è la Network Function (NF) che costituisce, all'interno dell'architettura 5G, un framework completo per definire le policy nella rete e consegnarle ad altre NF del piano di controllo.



Network Data Analytics

L'architettura 5GS è stata estesa per supportare i servizi di analisi dei dati di rete tramite una nuova entità denominata NWDAF (Network Data Analytics Function) [11].

NWDAF si concentra sulle informazioni sul livello di carico, sull'esperienza del servizio, sulle prestazioni della rete e sul comportamento anomalo.

La sicurezza potrebbe iscriversi alle notifiche di analisi di rete e utilizzarle per i calcoli e gli aggiornamenti delle politiche, ma questo non è attualmente standardizzato.

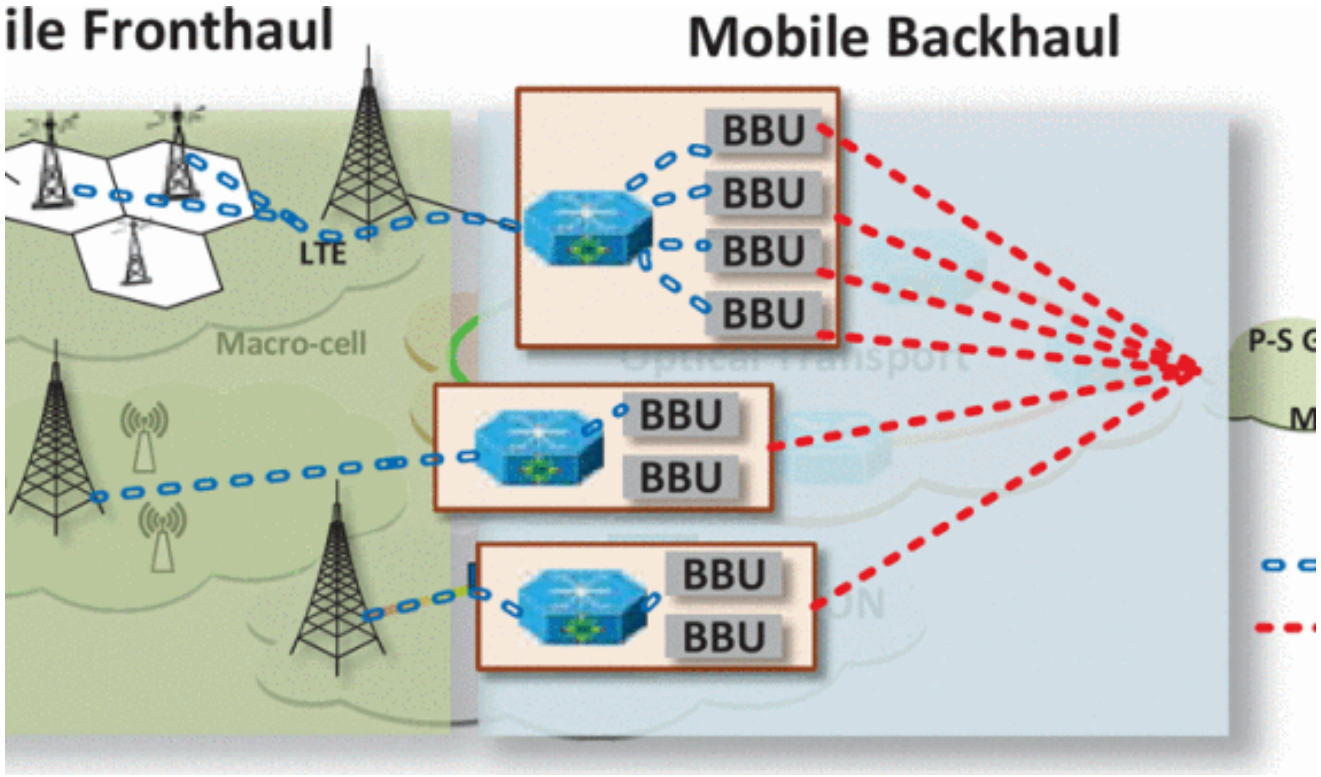
Network data Analytics (2)

Abbiamo studiato il potenziale utilizzo della nuova funzione di analisi di rete per scopi di garanzia della sicurezza. La garanzia di sicurezza della rete richiederà strumenti di monitoraggio sofisticati e specifici per la sicurezza, come i sistemi SIEM (Security Incident and Event Management).

La nostra ricerca mostra che possiamo anche ottenere informazioni rilevanti dal comportamento della rete per creare approfondimenti sulla sicurezza. Un incidente rilevato da NWDAF o SIEM può innescare una modifica della politica nella rete, gestita dal PCF.

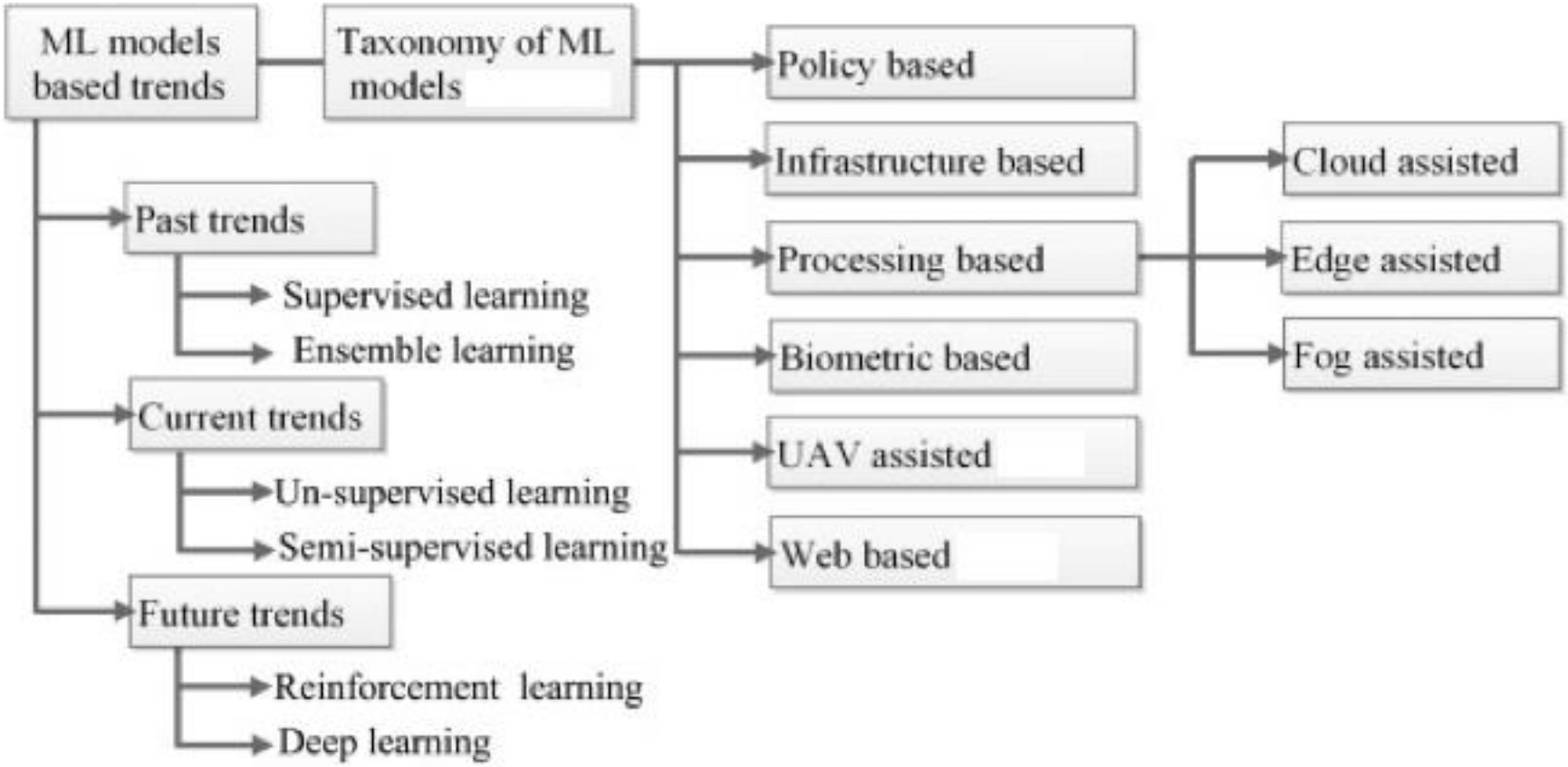
- Per esempio, lo spostamento di un utente da una sezione compromessa per la sicurezza a una sezione di quarantena.

Il nostro User Data Plane



- Definizione di servizi di edge computing per il <u>pre-trattamento sicuro</u> dei dati
  - Funzioni: Digitization/storage, Anonimizzazione/crittografia, sparsity reduction, early fusion, feature extraction, transformer verso latent data space
  - Interfacce:
    - Edge on prem: apparati presso i punti di acquisizione, gestiti dallo spoke
    - Edge on network: servizi nella (sotto)rete operatore gestita dallo spoke

Servizi Dati sullo User Data Plane



Sicurezza UDP

- Nell'attuale architettura 5GS i casi d'uso relativi all'applicazione della sicurezza del piano utente sono limitati alle politiche di sicurezza nei confronti della NG-RAN (NG Radio Access Network), basate sull'attivazione della protezione dell'integrità e/o della riservatezza nell'interfaccia aerea tra l'UE e la Stazione Base.
- Tali politiche di sicurezza possono essere parte delle informazioni sull'abbonato archiviate nell'Unified Data Repository (UDR) e recuperate dalla funzione Unified Data Management (UDM) o, in alternativa, configurate localmente.
    - Poiché attualmente le politiche di sicurezza del piano utente (UP) sono basate a livello globale, il controllo da parte delle politiche locali nel SMF può sembrare a priori sufficiente.
- Un nuovo approccio è però necessario per affrontare i nostri Service Level Agreement, relativi a servizi e funzionalità di sicurezza richiesti da clienti e tenant healthcare (ìverticali che gestiscono un'infrastruttura critica) , che richiedono livelli di sicurezza diversi e personalizzati con clausole di sicurezza sempre crescenti.

Il Nostro Approccio

- I requisiti di un'infrastruttura critica in termini di sicurezza differiranno da quelli dalla generica banda larga mobile potenziata standard dedicata all'IoT.
- Riteniamo che funzionalità come la protezione dell'integrità dell'UDP debbano essere attivate selettivamente.
  - In generale, le sezioni di rete che servono diversi tipi di servizi possono avere requisiti di sicurezza diversi e adottare protocolli e meccanismi di sicurezza distinti. Pertanto, è un punto chiave fornire diversi livelli di protezione della sicurezza per sezioni di rete differenziate.
- Anche gli algoritmi di sicurezza utilizzati per la crittografia dei dati devono essere scelti in modo selettivo (ad es. crypto-suite, lunghezza della chiave) in base al profilo del cliente.
- La nostra tesi è che la sicurezza deve essere parte del profilo utente dello spoke, memorizzato in UDR e PCF recupererà quei nuovi attributi per applicare le politiche corrispondenti.