vayu

Deep Dive nei KPI della Telefonia

Modelli Matematici e Architetture Dati per la Fraud Detection e la Revenue Assurance

EMANUELA BEVILACQUA
Head of Voice Engineering

Bologna - ITNOG - 21 Aprile 2026

Agenda

Modelli di Anomaly Detection

Implementazione di algoritmi di Anomaly Detection basati su analisi comportamentale del traffico (User Behavior Analytics) per il contrasto a fenomeni di IRSF (International Revenue Share Fraud) e Robocalling

Architetture di Monitoraggio Real-Time

Progettazione di pipeline di dati che integrano log di segnalazione SIP e flussi di billing per ridurre il time-to-detect, minimizzando l'esposizione al rischio economico e tecnico

Integrità del Dato e Revenue Assurance

Studio dei meccanismi di riconciliazione tra i nodi di bordo (SBC/Gateway) e i sistemi di rating. Si analizzerà come le discrepanze nei metadati dei CDR (Call Detail Records) agiscano da indicatori precoci di leakage finanziario o di vulnerabilità infrastrutturale

vayu

KPI DI FONIA

Key Performance Indicator
sono per definizione istantanee della qualità del servizio

Opportunamente correlati, rappresentano anche metriche utili in Sistemi predittivi di Anomaly & Fraud Detection o di Revenue Leakage

L’obiettivo garantire la resilienza operativa e la sostenibilità del margine degli operatori Telco

vayu

KPI ATOMICI

Sono metriche valide per singola chiamata

PDD (Post Dial Delay)

Talert - Tattempt

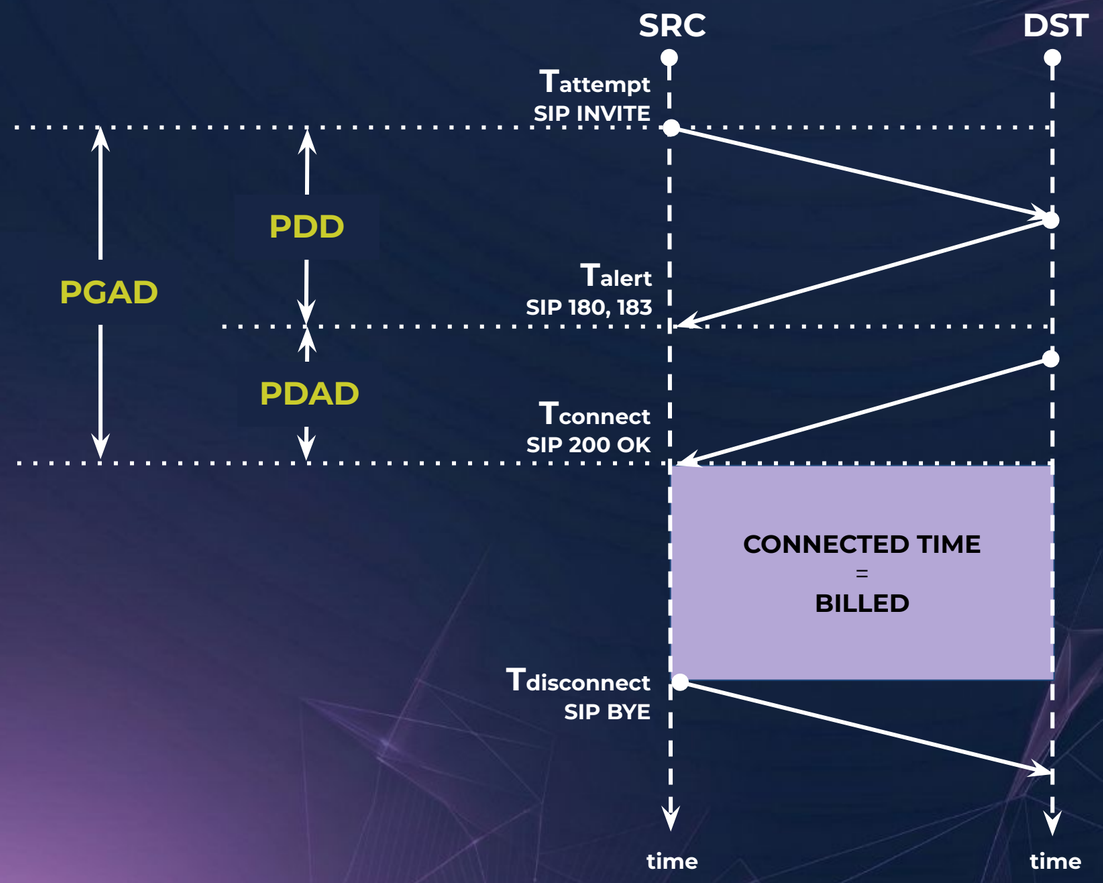
SRD (Session Request Delay) in RFC6076

PDAD (Post Dial Answer Delay)

Tconnect - Talert

PGAD (Post Gateway Answer Delay)

Tconnect - Tattempt



vayu

KPI AGGREGATI

Sono metriche di secondo livello valide per gruppi di chiamate (clienti, fornitori, direttrici, trunk)

ASR
(Answer Seizure Ratio)

$$ASR = \frac{\#\ \text{chiamate risposte}}{\#\ \text{totale tentativi}}\ \%$$

NER
(Network Effectiveness Ratio)

$$NER = \frac{\overbrace{\#\ \text{ch. risposte}}^{\text{SIP 200OK}} + \overbrace{\#\ \text{ch. utente non disponibile}}^{\text{SIP 486, 600, 480, 408, 603}} + \overbrace{\#\ \text{ch. numeri invalidi}}^{\text{SIP 404, 484}}}{\#\ \text{totale tentativi}}\ \%$$

ACD
(Average Call Duration)

$$ACD = \frac{\sum (T_{disconnect} - T_{connect})}{\#\ \text{totale chiamate connesse}}$$

vayu

Altri KPI utili

Call Randomness

misura il grado di dispersione statistica dei destinatari chiamati da una singola sorgente (o viceversa) in un determinato arco temporale.

Si calcola a partire da **UCN** (Unique Called Numbers), ovvero il numero di numeri unici chiamati nella finestra di osservazione

$$\textbf{Rand} = \frac{\text{UCN}}{\text{\# totale tentativi}} \%$$

Bassa Randomness: un utente chiama ripetutamente gli stessi 5-10 numeri (comportamento umano tipico, "Community of Interest")

Alta Randomness: una sorgente (o un cluster di sorgenti) chiama migliaia di numeri unici, spesso seguendo una distribuzione sequenziale o pseudocasuale (comportamento di un Robocalling)

Release Bias

misura la propensione di una direttrice di traffico (o di un singolo utente) a terminare le chiamate dal lato del destinatario (*Called Party*) rispetto al lato del chiamante (*Calling Party*).

$$\textbf{RelB} = \frac{\text{\# Rel Called Party}}{\text{\# Rel Calling Party}}$$

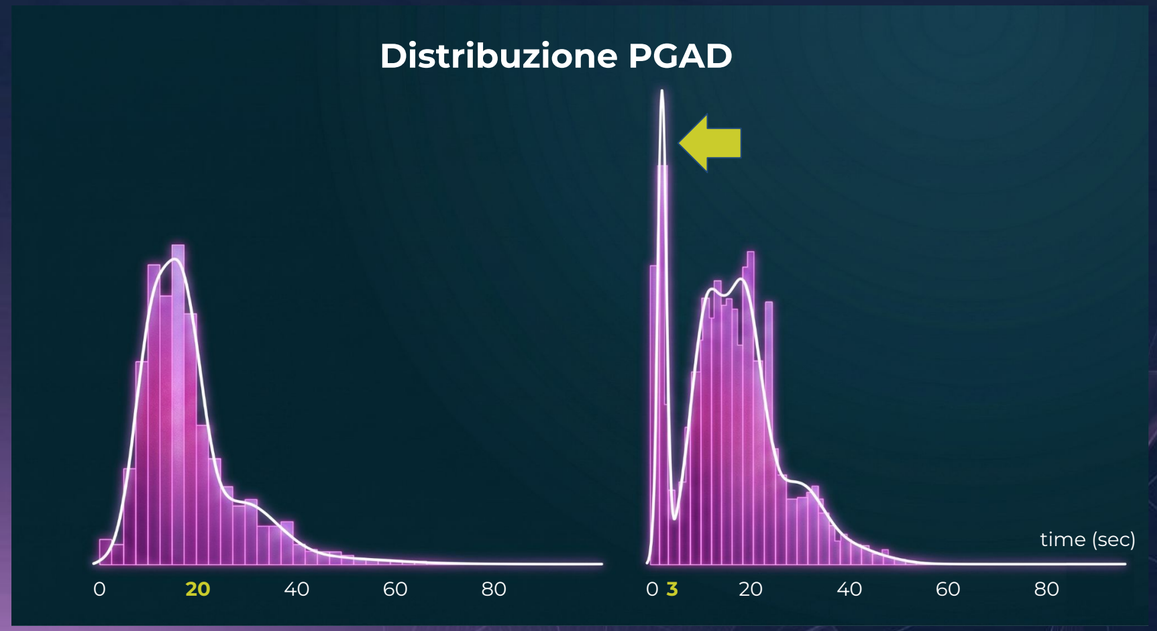
vayu

PBX Hacking

Un PBX hackerato spesso genera IRSF (International Revenue Share Fraud)

Chiamate contemporanee verso destinazioni altospendenti (tipicamente terminate verso un fornitore compiacente)
Metodo classico di protezione:
blacklist verso prefissi internazionali + TopStop (limite di spesa per determinati intervalli di tempo)

PGAD diminuisce
poiché le chiamate vengono terminate su un risponditore automatico, tipicamente questo risponde con lo stesso ritardo



vayu

PBX Hacking

Un PBX hackerato spesso genera IRSF (International Revenue Share Fraud)

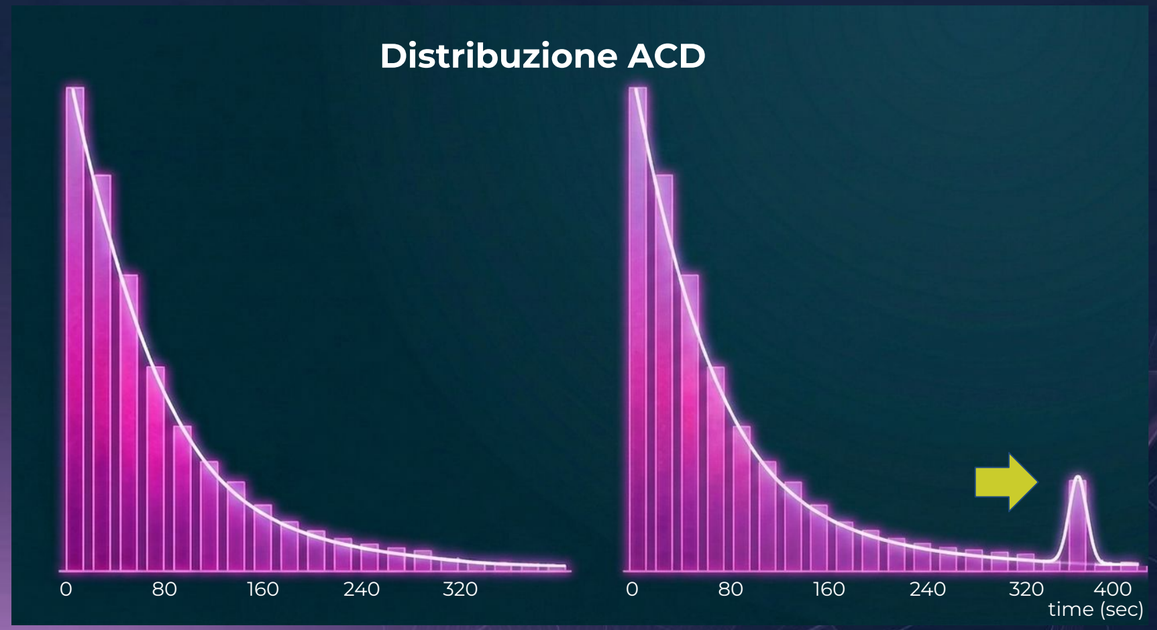
Chiamate contemporanee verso destinazioni altospendenti (tipicamente terminate verso un fornitore compiacente)
Metodo classico di protezione:
blacklist verso prefissi internazionali + TopStop (limite di spesa per determinati intervalli di tempo)

PGAD diminuisce
poiché le chiamate vengono terminate su un risponditore automatico, tipicamente questo risponde con lo stesso ritardo

ACD aumenta
si usano chiamate di lunga durata per ritardare l'effetto di antifrode non realtime (che bloccano solo le chiamate sopra soglia una volta rilevata l'anomalia)

Rand diminuisce

RelB aumenta



vayu

Robocalling

Un combinatore telefonico effettua chiamate in simultanea trasmettendo messaggi preregistrati a un numero elevato di destinatari

Sono molto utilizzati per Telemarketing Aggressivo quindi non necessariamente fraudolenti.

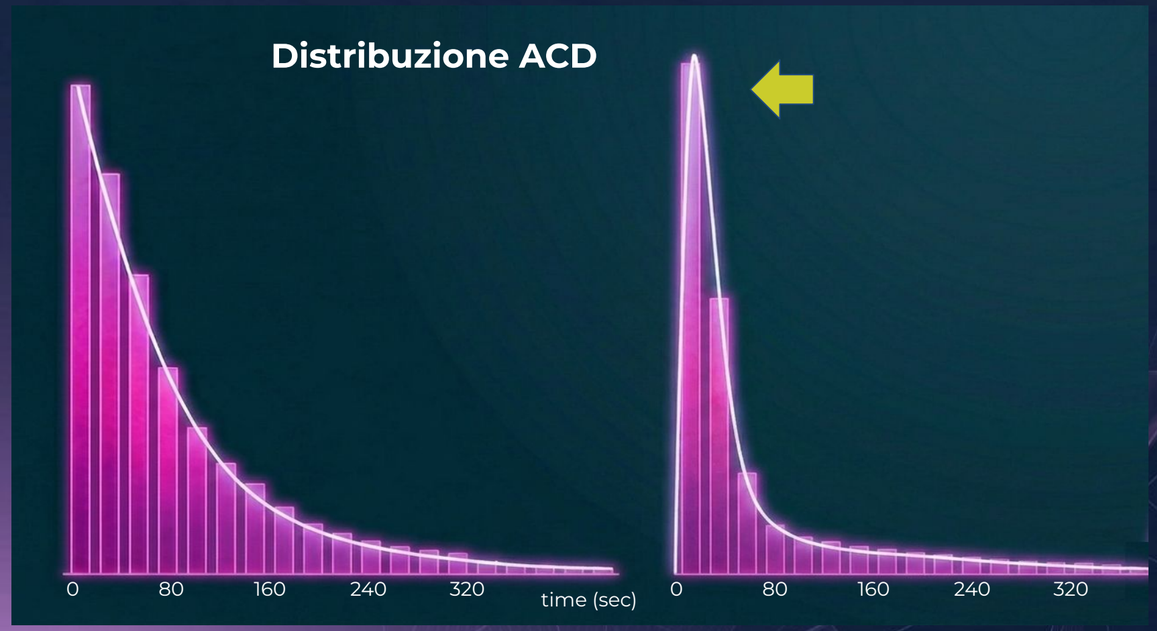
Come variano i KPI in presenza di Robocalling?

ASR crollo drastico
Molte chiamate non ricevono risposta o sono bloccate dai sistemi Antispam

NER costante o in calo
Crolla solo in presenza di saturazione delle risorse di terminazione

ACD riduzione estrema
La maggior parte delle chiamate dura < 10 secondi.

PDD picchi anomali
La rete può rallentare nel processare migliaia di tentativi di setup simultanei.



vayu

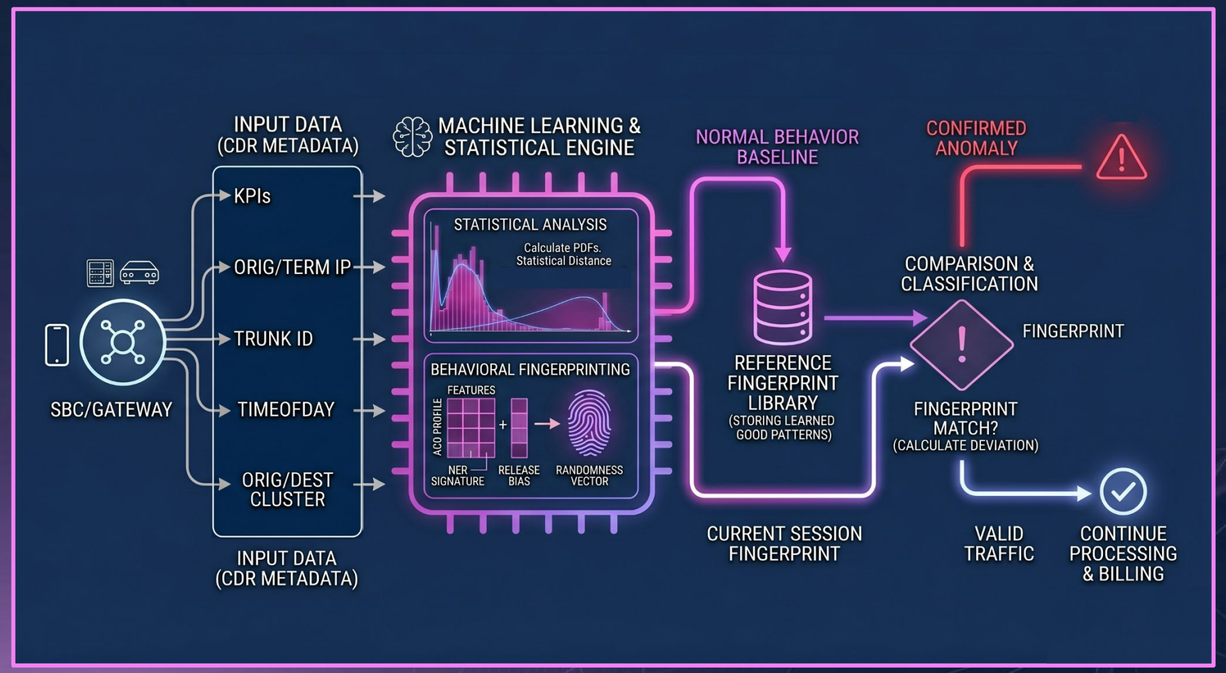
Modelli di Anomaly Detection intelligente

I Metodi Tradizionali

- Le soglie fisse (es. Alert se ASR < 30%) generano troppi falsi positivi o mancano attacchi sofisticati (come l'IRSF) che "si nascondono" sotto la media
- La rete è dinamica: il traffico di mezzogiorno è statisticamente diverso da quello delle 3 di notte

L'approccio basato su Machine Learning

- Non guarda il valore puntuale, ma la forma (PDF - Probability Density Function) della distribuzione dei KPI.
- Il modello apprende la "forma normale" del traffico per ogni direttrice, cliente, trunk, fascia oraria e costruisce una Baseline
- L'anomalia viene rilevata calcolando quanto la distribuzione corrente si discosta dalla baseline (Distanza Statistica)
- Si usa la tecnica del Fingerprinting ovvero si attribuisce ad ogni tipo di anomalia/frode conosciuta una devianza dalla PDF di uno o più KPI che permette una categorizzazione immediata dell'anomalia riscontrata



vayu

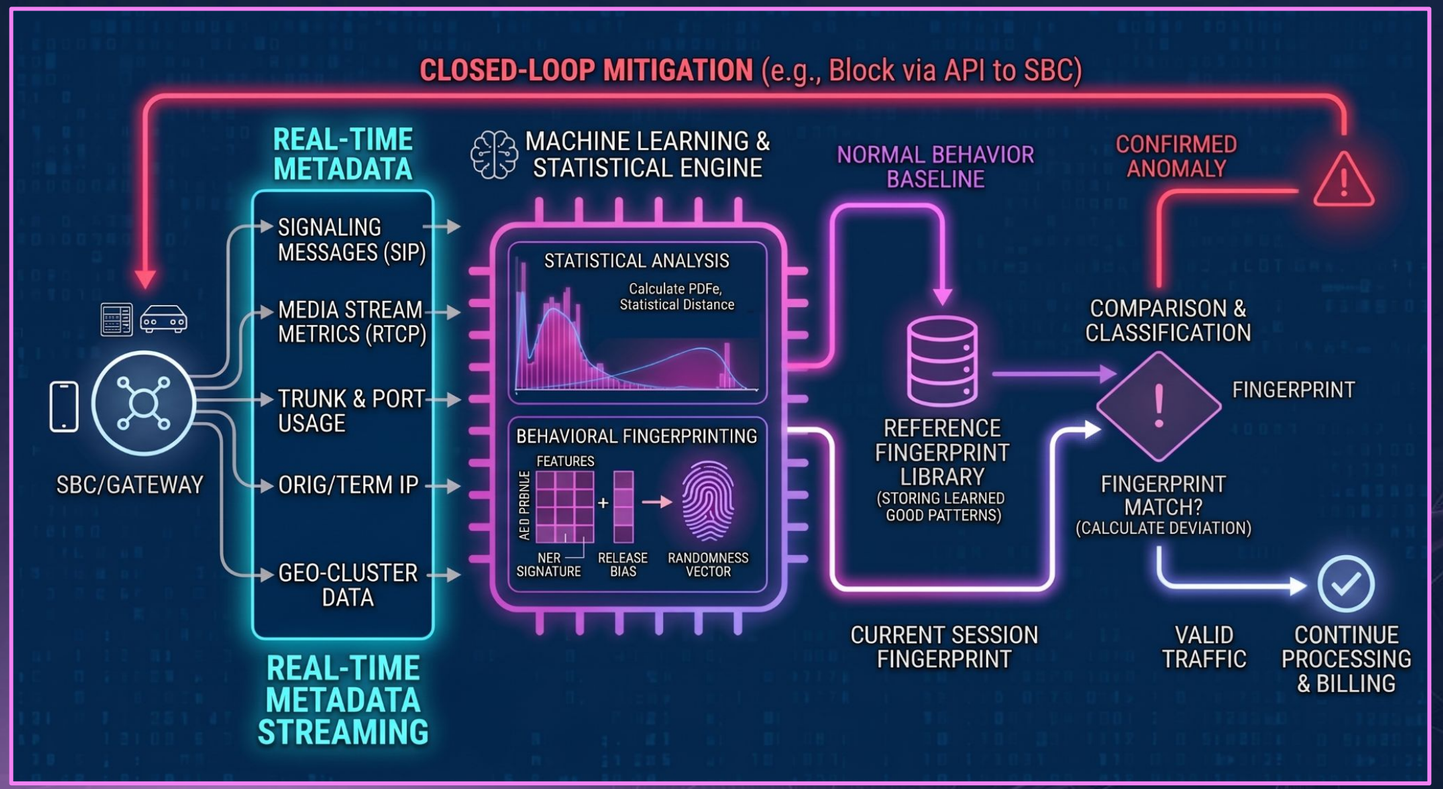
Architetture di Monitoraggio Real-Time

I processi finora descritti funzionano bene ma sono offline, ovvero lavorano sui CDR che vengono prodotti ed elaborati a chiamata già chiusa

Quindi sono tardivi nel mitigare frodi e non eliminano tutte le chiamate in perdita

Possono essere resi più efficienti se i Network Element (SBC) presenti in rete permettono:

- L'accesso in tempo reale ai metadati delle chiamate in corso
- La possibilità di drop di chiamate da sistemi esterni (Sistemi Closed-Loop)



vayu

Integrità del Dato e Revenue Assurance

**Se l’Anomaly Detection protegge dai costi "esterni" come le frodi,
la Revenue Assurance protegge dai costi "interni" generati da inefficienze o errori operativi, i cosiddetti Revenue Leakage.**

La Catena di Riconciliazione (SBC vs. Billing)

Il processo di riconciliazione non è solo un confronto numerico, ma una verifica di coerenza tra due mondi:

SBC/Gateway - Il dato grezzo
Se l'SBC dice che la chiamata è durata 120 secondi, quella è la realtà fisica della rete

Rating/Billing System - Il dato interpretato
Qui vengono applicate le tariffe, gli arrotondamenti e le regole di business.

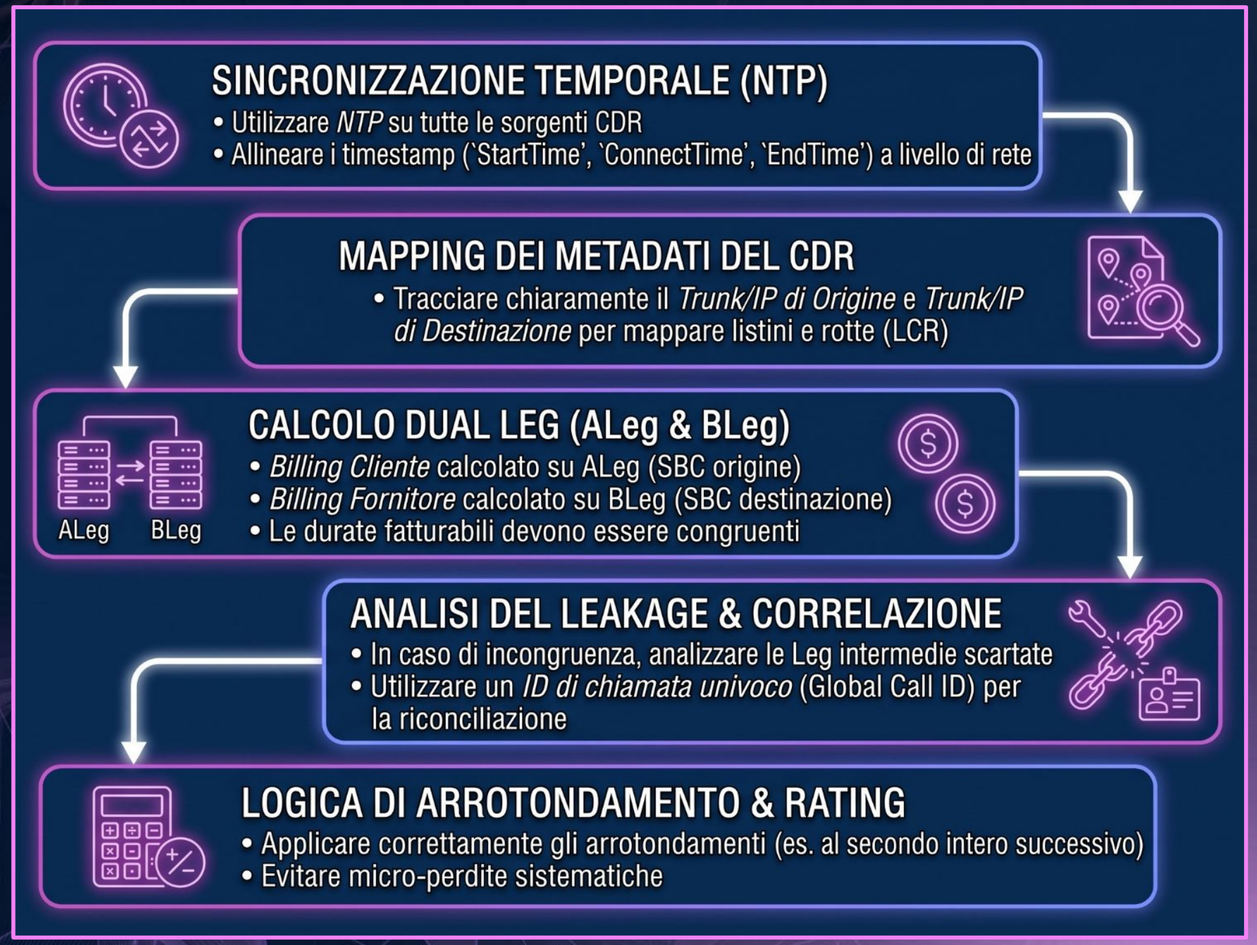
Il Leakage nasce quando $\sum \text{DURATA}_{\text{SBC}} > \sum \text{DURATA}_{\text{Billing}}$

Se l'SBC registra traffico che il sistema di rating non vede, stiamo erogando minuti gratuitamente (un "buco" nero finanziario)

vayu

Best Practices per la Revenue Assurance: la Mediation

In presenza di un unico SBC che genera i CDR, l'unica sorgente di possibili discrepanze è il processo di billing.
Ma che succede se l'architettura di rete fonia è complessa con SBC multipli e diverse sorgenti di CDR?



Serve un processo di **MEDIATION** ovvero
un processo che riconcilia tra loro CDR appartenenti
alla stessa chiamata ma a SBC diversi

I CDR così elaborati sono pronti per il processo di Billing

vayu

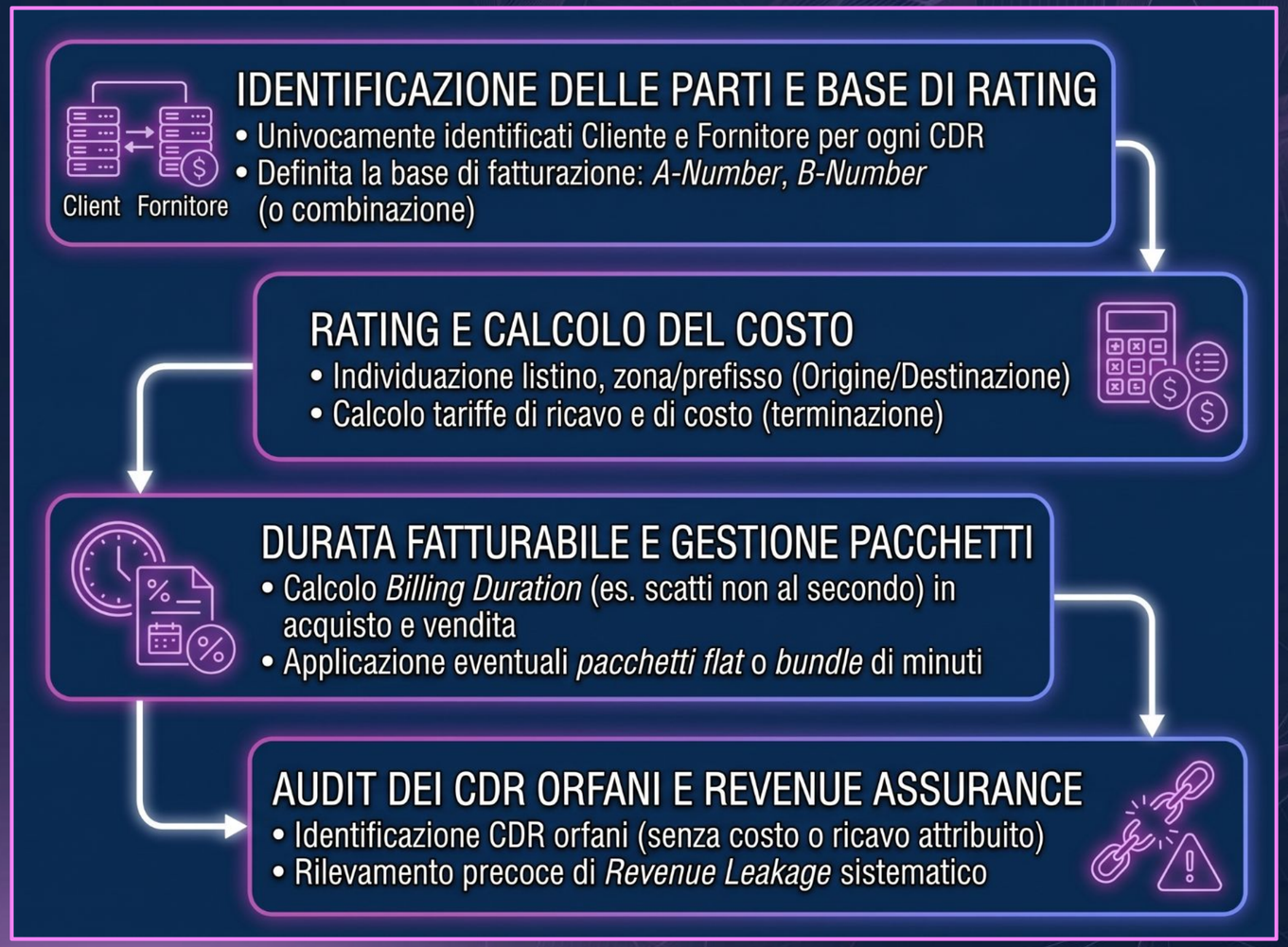
Best Practices per la Revenue Assurance: il Billing

Best practices di Billing

Il processo anche se non perfetto è considerato accettabile se:

- **la differenza in termini di minuti/importi è al di sotto dello 0.5% del totale per i CDR orfani**
- **la differenza in termini di importi prevede un margine superiore ad una soglia predefinita discrezionale**

Margin Assurance



vayu

Grazie per la vostra attenzione!

Emanuela Bevilacqua
emanuela@vayu.it