NetTrace AI

Application Documentation & Capabilities

This document provides an overview of the NetTrace AI application, its high-level architecture, and its comprehensive capabilities for mobile network analysis (Voice & Data).

2. Packet Processing Workflow

The system employs a multi-stage decoding strategy involving both Scapy (lightweight) and TShark (Deep Packet Inspection).

- **Step 1: Ingestion:** PCAP files are uploaded and validated.
- **Step 2: Field Extraction (TShark):** The decode/tshark.py module runs tshark -T json to extract specific telecom fields (e.g., sip.Call-ID, gtp.teid, ngap.procedureCode). This allows access to deeply nested vendor-specific fields that standard parsers miss.
- **Step 3: Transaction Building:** Raw packets are grouped into logical transactions (Request/Response pairs) by decode/transactions_builder.py. This handles retransmissions and helps calculate precise latency.

3. Analysis Logic (Voice & Data)

Data Analysis

- **Flow Aggregation:** Packets are hashed by 5-tuple (Src/Dst IP & Port, Protocol) to create 'Flow' objects.
- **Session Correlation:** The engine links independent flows into 'Subscriber Sessions' by matching GTP-TEIDs (Tunnel Endpoint IDs) or IP pairs. This allows correlation of Control Plane (Signaling) with User Plane (Data).

3. Voice & IMS Capabilities (Deep Dive)

The system includes a dedicated Media Plane Analyzer that processes RTP/RTCP streams to detect quality degradation.

- **Call Flow Reconstruction:** Builds complete SIP call flows (Invite -> Bye) and correlates them with media streams using SDP port parsing.
- **One-Way Audio Detection:** Analyzes bidirectional RTP flow pairs. If a call has Established state but RTP packets flow in only one direction (e.g., UE->Network only), it triggers a 'Critical' finding.
- **Silent Call / Low Activity:** Detects established calls where the packet rate is below 10pps (Packets Per Second) for duration > 5s, indicating silence or potential Comfort Noise Generation (CNG) issues.
- **SRVCC/Handover:** Detects Single Radio Voice Call Continuity by correlating release causes (SIP 200 OK after INFO) with S1-AP HandoverRequired messages.

4. Key Performance Indicators & Formulas

Network health is determined by specific telecom KPIs derived from RFC standards.

Voice Quality (RTP)

- **Jitter (RFC 3550):** Calculated as the mean deviation of inter-arrival time. Formula: J(i) = J(i-1) + (|D(i-1, i)| - J(i-1))/16. Threshold: >50ms is Warning.

- **Packet Loss:** Detected by sequence number gaps.
  Formula: Loss % = (Expected - Received) / Expected * 100. Threshold: >2% is Critical.
- **MOS-LQE (E-Model):** Estimated Mean Opinion Score based on ITU-T G.107.
  Derivation: R-Factor = 93.2 - Id(Delay) - Ie(Loss).
  Mapping: R < 60 -> MOS < 3.1 (Poor).

Signaling KPIs

- **Post-Dial Delay (PDD):** Time from SIP INVITE to 180 Ringing. Analyzed to detect Core Network latency.
- **Setup Success Rate (SSR):** Ratio of sessions reaching 'Active' state vs. total attempts.
- **SIP Retransmissions:** Duplicate requests (same Branch ID) within T1 timer (500ms). Indicates packet loss or server overload.

5. AI-Driven Root Cause Determination

Root Cause Analysis is a multi-step process integrating deterministic rules with Probabilistic AI:

- **Context Gathering:** The backend aggregates all Flows, Transaction Failures, Bandwidth Stats, and SIP/GTP Error Codes into a structured context JSON.
- **Pattern Matching (Deterministic):** The system first checks for known signatures (e.g., specific Release Causes like 'Radio Link Failure' or 'Network Congestion').
- **LLM Reasoning (Probabilistic):** The aggregated context is sent to the LLM. The model analyzes the relationship between signaling failures and data throughput (e.g., 'High retransmissions on GTP-U caused SIP timeout').
- **Confidence Scoring:** The AI assigns a confidence score (High/Medium/Low) based on the strength of the evidence (e.g., specific error codes vs. general timeouts).