AI in 5G Security

Feng Gao
China Unicom
What AI do for 5G security

Enhanced Mobile Broadband

Typical service security
- eMBB security
- mMTC security
- URLLC security

5G network security
- MEC security
- Network slice management security
- Service capability exposure security
- Security edge protection
- Network security situational awareness

Network element security
- Automatic network element security assurance
Typical service security
Typical service security - eMBB

- 8K videos
- 3D videos
- AR/VR
- Various new applications

**Embedded virus**
- Content detection by AI technology
- Filter embedded virus

**Malicious code**
- Filter embedded code

**Spam**
- Filter spam

**Illegal content**

**AI enables video filtering**

**AI enables new application security**
- Pattern learning, cluster, and migration
- Security check for the new application before on-line
Network Data Analytics Function (NWDAF) has been introduced in the 5G System Architecture in 3GPP.

NWDAF perform data analysis using a 3-layer Deep Neural Network to cluster the heterogeneous UEs into multiple UE group(s).

- **Input layer**: UE behavioral information per UE
- **Output layer**: Expected UE behavioral information per UE group

NWDAF provides the expected UE behavioral information to help supervision of mIoT terminals.
Typical service security - eMTC

UE behavioural information collected from 5GC NF(s)

<table>
<thead>
<tr>
<th>Information</th>
<th>Presence</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE ID</td>
<td>M</td>
<td>AMF/SMF</td>
<td>Could be e.g. SUPI, which is used by NWDAF to correlate the UE behavioural information from different 5GC NFs.</td>
</tr>
<tr>
<td>Location info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;Timestamp</td>
<td>O</td>
<td>AMF</td>
<td>The timing for the UE</td>
</tr>
<tr>
<td>&gt;Location</td>
<td>O</td>
<td>AMF</td>
<td>The location info for the UE e.g. Cell ID or TA ID</td>
</tr>
<tr>
<td>Communication Pattern Info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;Communication start time</td>
<td>O</td>
<td>SMF</td>
<td>Start time when the UE is available for communication</td>
</tr>
<tr>
<td>&gt;Communication end time</td>
<td>O</td>
<td>SMF</td>
<td>End time when the UE is unavailable for communication</td>
</tr>
<tr>
<td>Network Configuration Info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;UL or DL Packet Latency</td>
<td>O</td>
<td>SMF</td>
<td>Indicating the delay for uplink or downlink packets transfers for the UE</td>
</tr>
</tbody>
</table>

Expected UE behavioural information for a UE group provided by the NWDAF

<table>
<thead>
<tr>
<th>Information</th>
<th>Presence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stationary indication</td>
<td>O</td>
<td>Identifies whether the UE is stationary or mobile, e.g. only on demand. (TS 23.682 [5], clause 5.10.1).</td>
</tr>
<tr>
<td>UE Moving Trajectory</td>
<td>O</td>
<td>Identifies the UE’s expected geographical movement (TS 23.502 [3], clause 4.15.6). Example: A planned path of movement</td>
</tr>
<tr>
<td>Periodic communication</td>
<td>O</td>
<td>Identifies whether the UE communicates periodically or not, e.g. only on demand. (TS 23.682 [5], clause 5.10.1).</td>
</tr>
<tr>
<td>Indicator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication duration time</td>
<td>O</td>
<td>Duration interval time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1). Example: 5 minutes</td>
</tr>
<tr>
<td>Periodic time</td>
<td>O</td>
<td>Interval Time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1). Example: every hour</td>
</tr>
<tr>
<td>Scheduled communication</td>
<td>O</td>
<td>Time zone and Day of the week when the UE is available for communication (TS 23.682 [5], clause 5.10.1). Example: Time: 13:00-20:00, Day: Monday</td>
</tr>
<tr>
<td>Maximum Latency</td>
<td>O</td>
<td>Indicating maximum delay acceptable for downlink data transfers (TS 23.682 [5], clause 4.5.21).</td>
</tr>
<tr>
<td>Maximum Response Time</td>
<td>O</td>
<td>Indicating the time for which the UE stays reachable to allow the AF to reliably deliver the required downlink data (TS 23.682 [5], clause 4.5.21).</td>
</tr>
<tr>
<td>Suggested Number of</td>
<td>O</td>
<td>Indicating the number of packets that the UPF shall buffer in case the UE is not reachable (TS 23.682 [5], clause 4.5.21).</td>
</tr>
<tr>
<td>Downlink Packets</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AI analysis module in the V2X security operation center performs data analysis using a 3-layer Deep Neural Network to cluster the heterogeneous vehicles into multiple vehicles group(s).

- **Input layer**: Vehicle behavioral information per vehicle
- **Output layer**: Expected vehicle behavioral information per vehicle group

**Typical service security - URLLC**

AI enables V2X abnormal behavior analysis
Typical service security- URLLC

AI enables V2X secure path planning

Data collected from multiple sources, AI enables secure path planning

- Vehicle data
- Vehicle sensor data
- Road infrastructure data
- Network data
- Weather data
- Large events data
- Analytics data

![Diagram](image)

NWDAF provides the prediction of secure path planning

NEF to help planning the best and secure path
5G network security
5G network security - MEC security

Multiple access

Edge cloud computing

MEC APP

RAN CU

UPF

GW-U

vBRAS-U

vCPE

vCDN

AI enables APP security

- Pattern learning, cluster, and migration
- Security check for the new application before on-line

AI enables network security

- Automatic molding network environment
- Verify the network security policy
5G network security - network slicing

AI enables network slicing management security

- Pattern learning, cluster, and migration
  - Monitoring the network slicing access
  - Supervising the network slicing operation
- Perform data analysis using a 3-layer Deep Neural Network to cluster the heterogeneous UEs subscribed user into multiple subscribed user group(s).
  - Supervising the abnormal behavior by the subscribed user

1. UE access unauthorized network slicing
2. Unauthorized operation for the network slicing
3. Abnormal behavior by the subscribed user
Security Edge Protection Proxy (SEPP) in 3GPP:

- Message filtering and policing on inter-PLMN control plane interfaces
- Topology hiding

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signalling. (3GPP TS 33.501)

- Perform network rate analysis between operators using a 3-layer Deep Neural Network to cluster the heterogeneous network rate into multiple network rate models.
  - Intelligent and automatic makes the decision for rate-limiting functionalities
  - To defend the potential DDoS attack

AI technology
5G network security - Service Capability Exposure

AI enables the service capability exposure security

Service Capability Exposure Function (SCEF) in 3GPP:

- *provides access to network capabilities through homogenous network application programming interfaces (e.g. Network APIs) defined over T8 interface*

- *supports the Common API Framework (CAPIF) API*

API invoker outsides of the PLMN trust domain
- utilizes the CAPIF-1e, CAPIF-2e and the CAPIF-3 interfaces to onboard.

API invoker within the PLMN trust domain
- via the CAPIF-1, the CAPIF-2 and the CAPIF-3 interfaces prior to granting access to CAPIF services.

- Perform trust evaluation to classify the trusted API invoker and un-trusted API invoker instead of checking whether it is in the PLMN trust domain.
  - User feedback of the application
  - Malicious code detection of the application
  - Attack monitoring of the application
  - ….

CAPIF functional security model
AI enables the 5G network security situational awareness

Security management platform
- Key management
- Certificate management
- User management
- Key, certificate, identity management

Security analysis platform
- Based on the AI analysis, to detect the signaling storm, DDoS, OAM attacks.
- Data collection (log/signaling/traffic)

Security control platform
- Engine
- Action List
- Playbook
- Security policy arrangement
- Security policy issue

5G network security - Network security situational awareness
Network element security
Network element security

3GPP studies the network element security assurance almost 6 years, from the methodology to the specification for the 4G and 5G network elements.

Maybe in the future, the AI robot can do the test and evaluation for the network elements automatic and intelligence. We will see!
Thanks!