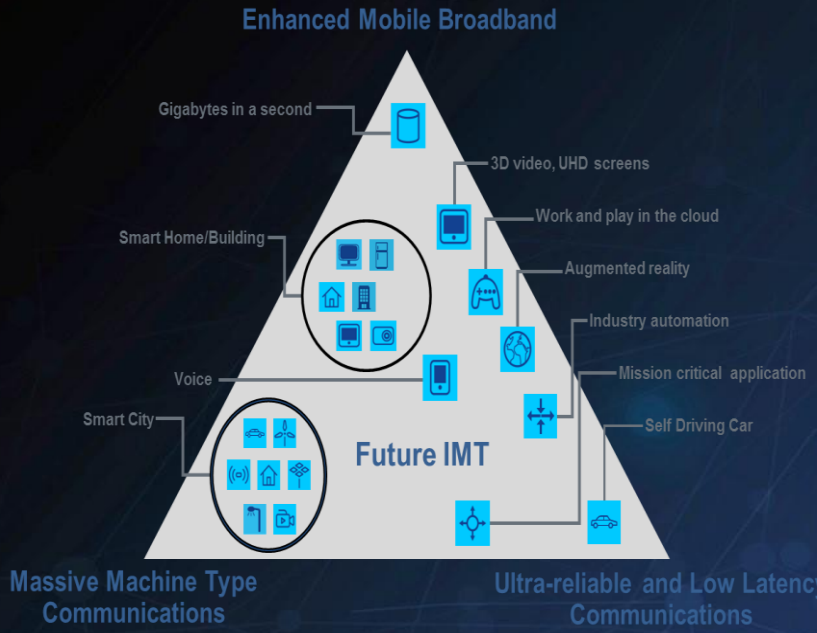
AI in 5G Security

Feng Gao

China Unicom

What AI do for 5G security



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

Malicious code

Spam

Illegal content

AI enables video filtering

- Content detection by AI technology
- Filter embedded virus
- Filter embedded code
- Filter spam

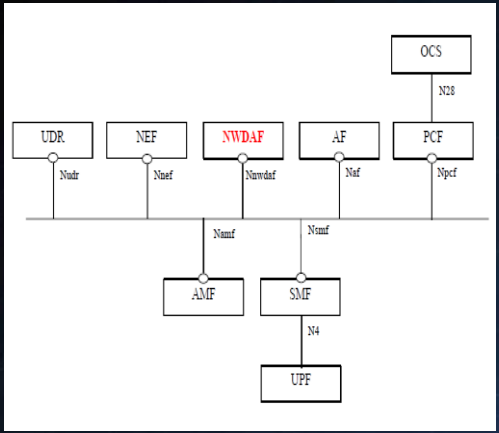
AI enables new application security

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

Typical service security- eMTC

AI enables mIoT Terminals supervision

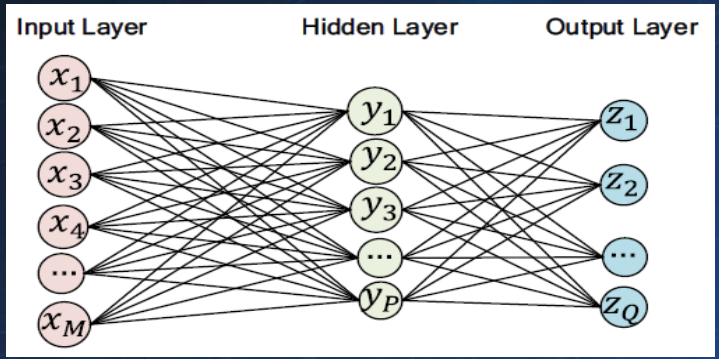
Network Data Analytics Function (NWDAF) has been introduced in the 5G System Architecture in 3GPP.



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

UDM

to help supervision of mIoT terminals

Typical service security- eMTC

UE behavioural information collected from 5GC NF(s)

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

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

Information	Presence	Description
Stationary indication	O	Identifies whether the UE is stationary or mobile, e.g. only on demand. (TS 23.682 [5], clause 5.10.1).
UE Moving Trajectory	O	Identifies the UE's expected geographical movement (TS 23.502 [3], clause 4.15.6). Example: A planned path of movement
Periodic communication indicator	O	Identifies whether the UE communicates periodically or not, e.g. only on demand. (TS 23.682 [5], clause 5.10.1).
Communication duration time	O	Duration interval time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1). Example: 5 minutes
Periodic time	O	Interval Time of periodic communication (may be used together with 1) (TS 23.682 [5], clause 5.10.1). Example: every hour
Scheduled communication time	O	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
Maximum Latency	O	Indicating maximum delay acceptable for downlink data transfers (TS 23.682 [5], clause 4.5.21).
Maximum Response Time	O	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).
Suggested Number of Downlink Packets	O	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).

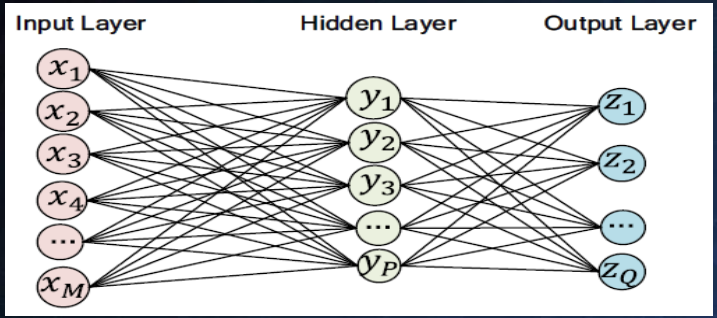
Typical service security- URLLC

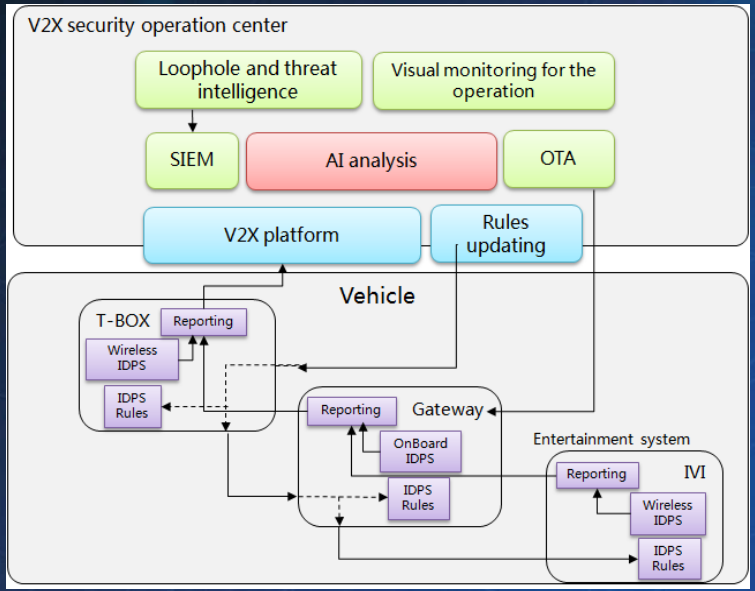
AI enables V2X abnormal behavior analysis

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



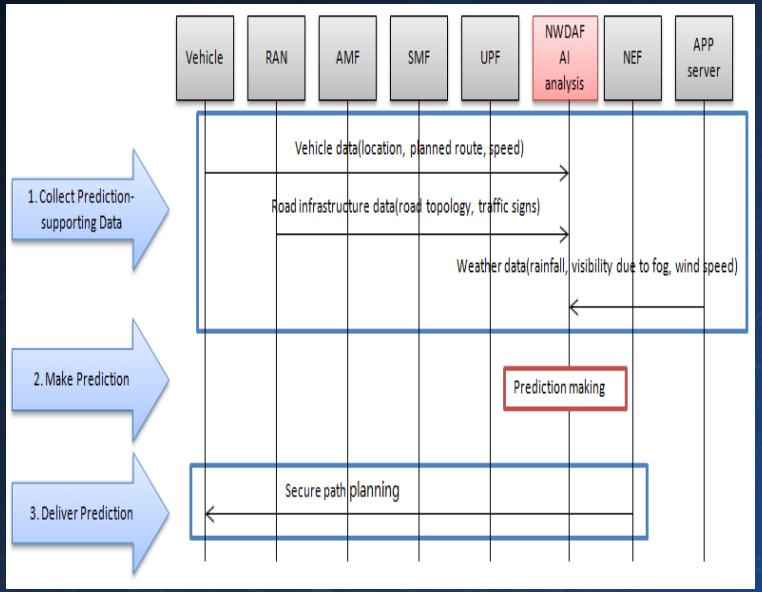


Typical service security- URLLC

AI enables V2X 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



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

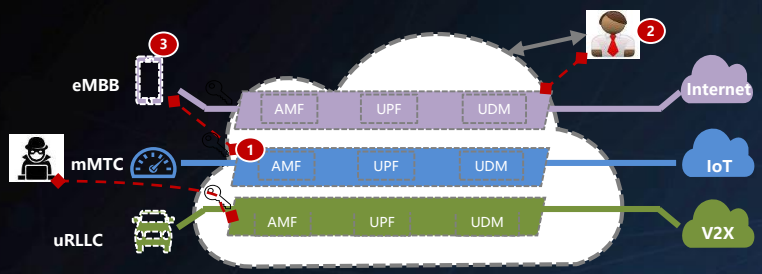
- Pattern learning, cluster, and migration
- Security check for the new application before on-line

AI enables network security

- Automatic molding network environment
- Verify the network security policy

5G network security- network slicing

AI enables network slicing management security



1. UE access unauthorized network slicing
2. Unauthorized operation for the network slicing
3. Abnormal behavior by the subscribed user

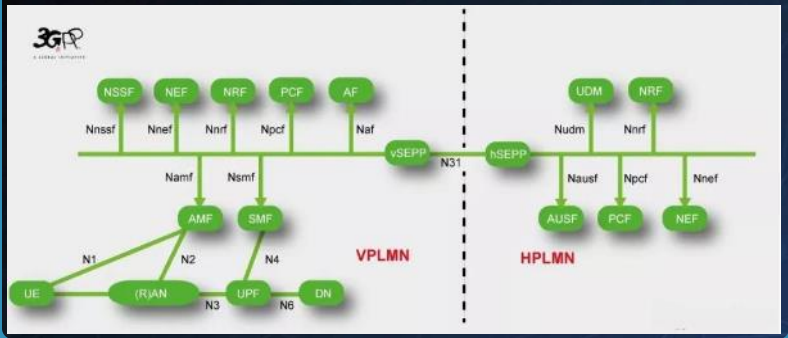
- Pattern learning, cluster, and migration
  - Monitoring the network slicing access 1
  - Supervising the network slicing operation 2
- Perform data analysis using a 3-layer Deep Neural Network to cluster the heterogeneous UEs subscribed user into multiple subscribed user group(s).
  - Supervising the abnormal behavior by the subscribed user 3

5G network security- Security Edge Protection

AI enables the E2E security between operators

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)

AI technology

- 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

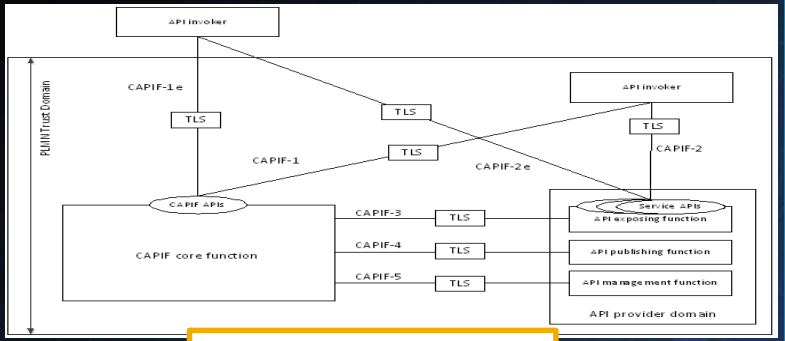
5G network security- Service Capability Exposure

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



CAPIF functional security model

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

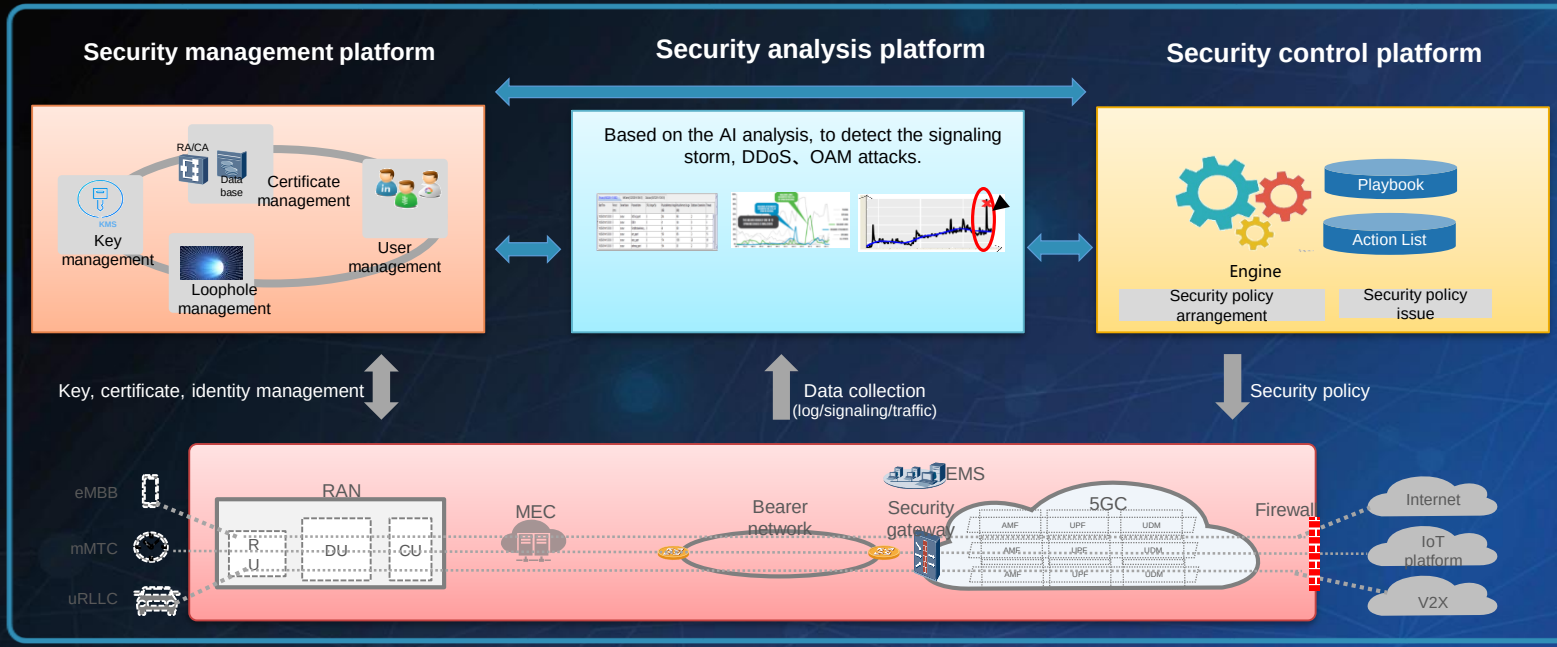
API invoker within the PLMN trust domain
- via the CAPIF-1, the CAPIF-2 and the CAPIF-3 interfaces prior to granting access to CAPIF services.

AI technology

- 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
  - ....

5G network security- Network security situational awareness

AI enables the 5G network security situational awareness



Network element security

Network element security

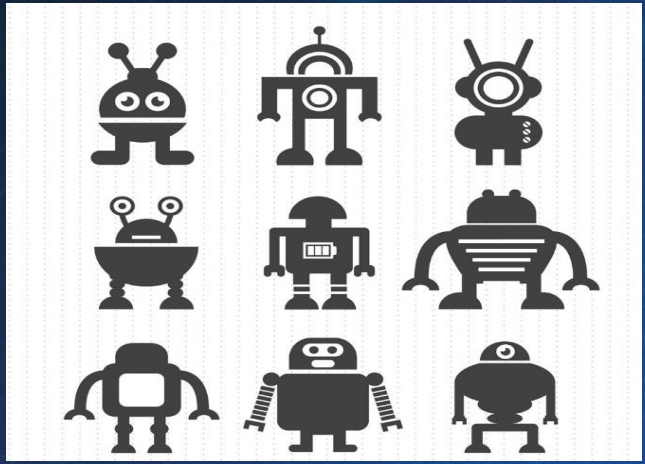
3GPP studies the network element security assurance almost 6 years, from the methodology to the specification for the 4G and 5G network elements.

MME

eNB

PGW

- NR Node B (gNB)
- Access and Mobility management Function (AMF)
- User Plane Function (UPF)
- Data Management (UDM)
- Session Management Function (SMF)
- Authentication Server Function (AUSF)
- Security Edge Protection Proxy (SEPP)
- Network Repository Function (NRF)
- Network Exposure Function (NEF)



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


Thanks!