S3-192109

Discussion Paper for Mitigation of DDoS Attack

Huawei, Hisilicon

5G Availability may be challenged by CIoT UEs

- CIoT UE will be Main Target of the Attacker in 5G:
  - Large Number & Single Function: Once a type of CIoT UEs exposes an vulnerability, massive similar CIoT UEs may be compromised (High Yield)
  - Multi Manufacturers: Manufacturers for the applications on the CIoT UE have different development capability, the app may exploit many vulnerabilities (Low Difficult)
  - Difficult Management: CIoT UEs may be non-human devices, which are hard to manage and update (Low Difficult)
- CIoT UE Sends User Data in Signaling:
  - Infrequent UE: user data is in NAS in RRC
  - Frequent UE: user data is with RRC
- 5G NE Needs Higher Processing Capability Cost:
  - Improved System Capacity: except for eMBB, 5GS shall support massive IoT, URLLC terminal, n times more than LTE
  - Higher User Data Rates: 10 times more than LTE
- Observation 1:
  - Since CIoT UEs are main target of the attacker, and they are sending user data in the RRC/NAS signalling, the attacker could control occasion of sending RRC/NAS signalling by triggering the UEs to send the user data without touching the low layer. Furthermore, improved capacity and higher data rate may lead much higher processing capability of network entities in 5G, e.g. n*10 times more than LTE. Once DDoS attack happens, those massive CIoT UEs may send the user data with signalling simultaneously and continously, the extreme case happens, which may cause the network entities signalling overload.

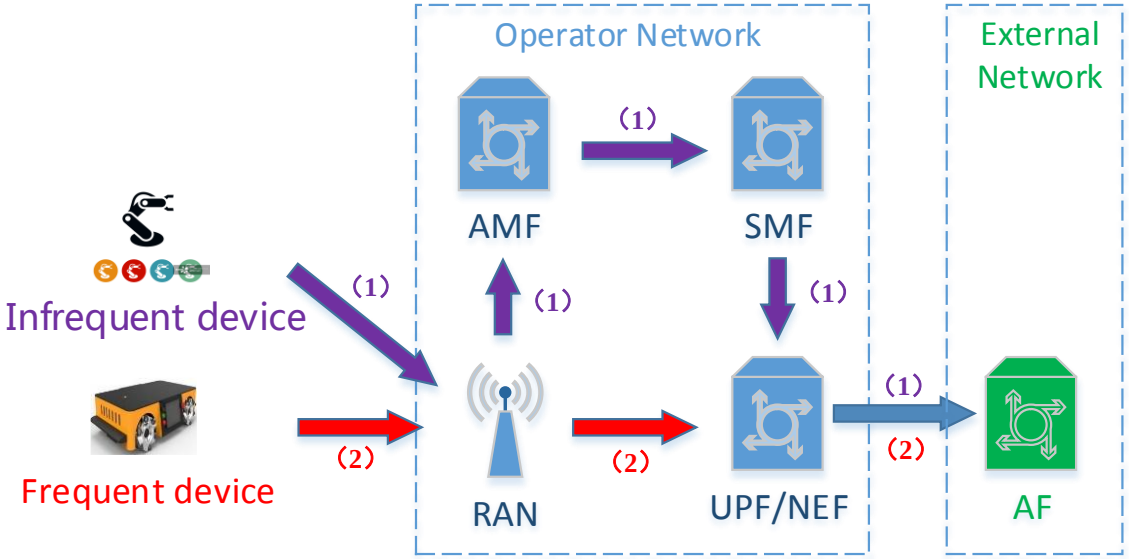
Impacted Network Entity

❑Infrequent IoT Devices：

- UE-RAN: user data in RRC and NAS
- RAN-AMF: user data in NAS
- AMF-SMF-UPF/NEF-AF: user data

❑Frequent IoT Devices：

- UE-RAN: user data with RRC
- RAN-UPF/NEF-AF: user data



❑Observation 2：

- Signaling with user data is terminated in RAN and AMF, since the signaling has higher priority, if the attacker could control enough CIoT UEs to trigger DDoS attack to an external AF, the massive signaling may cause RAN and AMF signaling overload.

Current Overload Control mechanism for RAN/AMF

Node	Method	Standardization	Control Method	Detection Method	Problem
RAN	RACH back off	5.1.4 in TS 38.321	Drop new preamble	RAN itself according to CPU usage and flow static which is not precise	May be a DoS attack to the normal UE
	RRC Reject	5.3.15 in TS 38.331	Reject new RRC request		
	RRC Release	5.3.8 in TS 38.331	Release UE in extreme case		
	Access Barring Control	5.3.14 in TS 38.331	Broadcast to lower UE’s access attempt		
AMF	N2 Overload Control	5.19.5.2 in TS 23.501	Inform RAN to trigger overload control mechanism such as RRC reject, RRC Connection Release and unified access barring	AMF itself according to CPU usage and flow static which is not precise	May be a DoS attack to the normal UE
	NAS congestion control	5.19.7 in TS 23.501	Reject new NAS signaling per DNN, S-NSSAI, internal group		

❑Observation 3：

- Current signalling overload control mechanisms on the RAN/AMF may be a DoS attack to the normal UE in case of signalling overload caused by DDoS attack.

Solution Overall of KI#4

Requirement	Solution	Overall	Benefit	Drawback
The 5GS shall be able to identify UEs that are operating normally and UEs that are misbehaving (Identify Misbehaving UEs)	16	NWDAF outputs misbehaving UEs (DDoS attack) to AMF/SMF/PCF	1. NWDAF has higher detection precision than RAN/AMF itself since NWDAF could get more data from AMF/SMF/AF 2. NWDAF is an NE in the operator network, which is easily communicating with other NEs using SBA.	NWDAF cannot guarantee 100% precision, current handling of misinformation may lead normal UE DoS
The 5GS shall support a secure mechanism to isolate the misbehaving UEs from the network (Active Mitigation Method)	6	AMF indicates the UE to drop IP packet, lower NAS signaling, lower QoS, etc.	Control position is the closest to the UE, attack can be controlled in the source	1. Control method is strict, may be DoS for the UE if misinformation happens 2. Big changes on the UE and AMF
	12	Part of solution 6, PCF indicates UE to drop IP packet	1. Control position is the closest to the UE, malicious flow is isolated. 2. Control granularity is finer, misinformation may not lead UE totally DoS	Misbehaving UE is not completely isolated.
The 5G network shall be able to protect itself against signalling overload from specific (e.g. malicious) UEs (Passive Mitigation mechanism)	17	Preconfigure misbehaving UE IDs in the RAN, handle the UEs only in overload case	1. Guarantee RAN usability: RAN can protect itself from big malicious 5G user data without changes on the UE. 2. Guarantee UE usability: Reduce impact on the UEs in case of misinformation	Only protect RAN itself, if the RAN could tolerate the attack, the mitigation will not be triggered, but the malicious data flow may be congest on the NEs behind RAN, i.e. AMF
	19	Preconfigure misbehaving UE IDs in the AMF, handle the UEs only in overload case	1. Align with solution 17 2. Guarantee AMF usability: AMF can protect itself from big malicious user data sent by infrequent UE without changes on the UE 3. Guarantee UE usability: Reduce impact on the UEs in case of misinformation	Only protect AMF itself, RAN is before the AMF, cannot be protected

Proposals

- Proposal 1:
  - SA3 should address signalling overload on RAN and AMF due to Malicious Applications on the UE in normative work.

- Proposal 2:
  - For identifying misbehaving UEs, solution 16 is recommended for normative work.

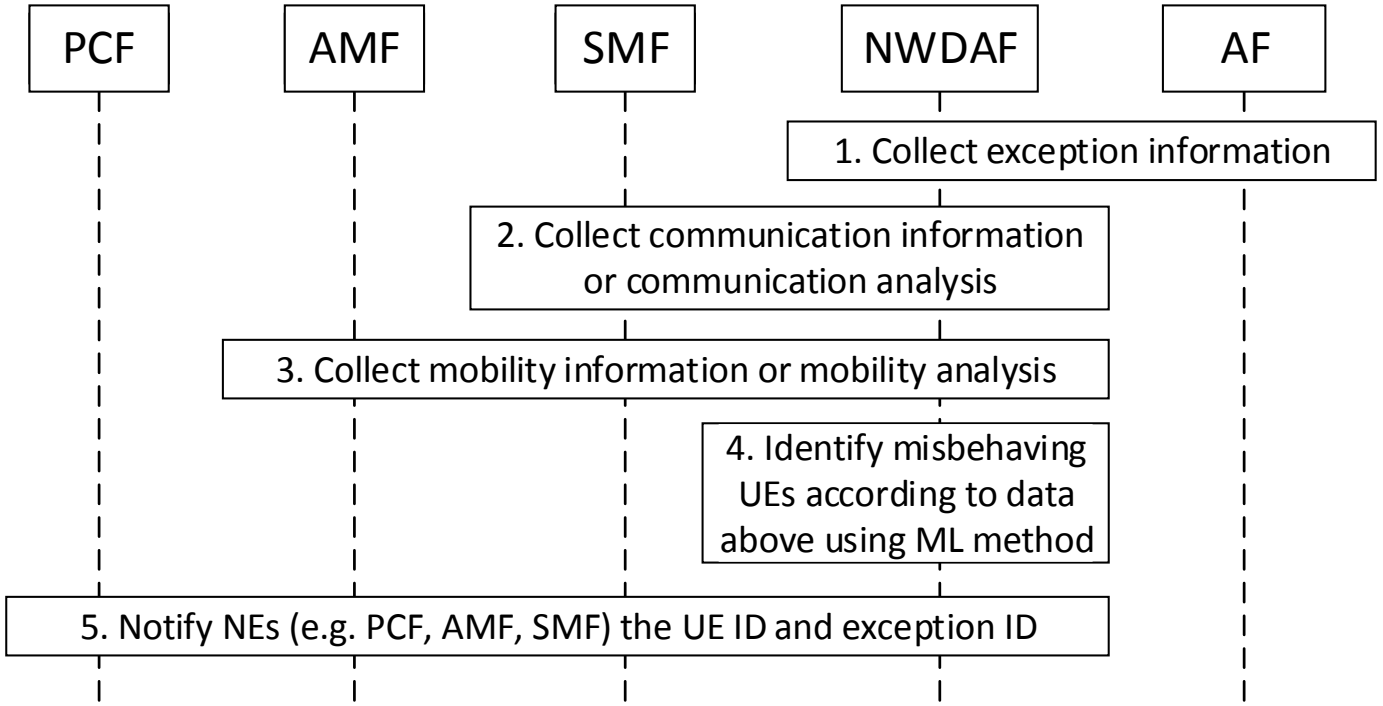
- Propoal 3:
  - For isolating the misbehaving UEs, solution 12 is recommended for normative work.

- Proposal 4:
  - For protecting itself against signaling overload, solution 17 and 19 are recommended for normative work to support RAN and AMF protection.

Annex Solution Details

Identify Misbehaving UEs

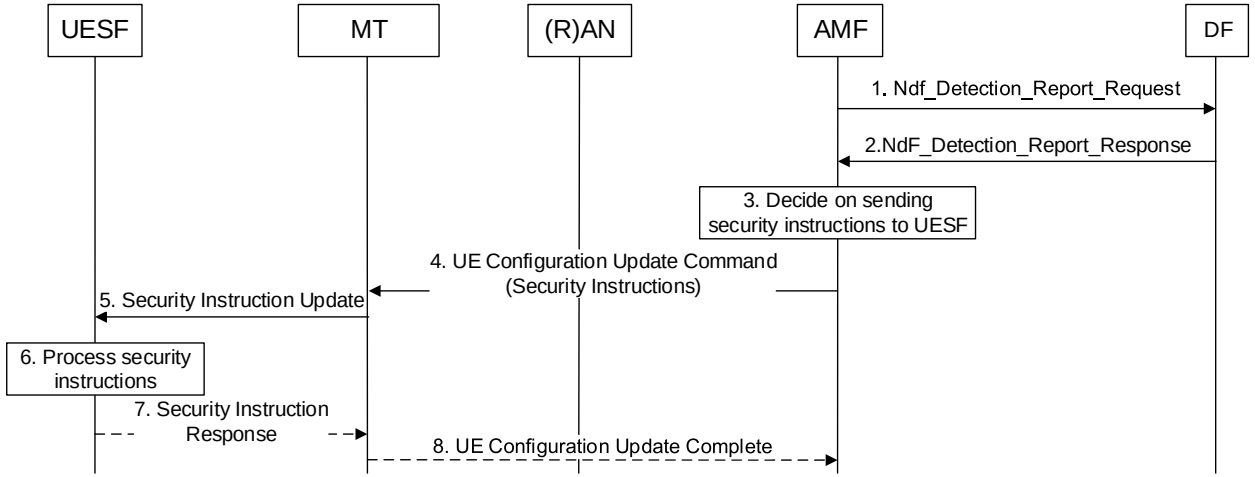
1. Solution#16: NWDF identify misbehaving UEs



- Overall:
  - The solution has been already standardized in TS 23.288, and is used to identify misbehaving UEs (including DDoS attack).
  - The NWDAF could collect mobility analytics from AMF, communication analytics from SMF, exception information from AF, and identify misbehaving (including DDoS attack) UEs, and outputs UE IDs and exception ID to the AMF, SMF, PCF.
  - For DDoS attack, SA2 recommended NWDAF to inform SMF to release PDU session of the UEs
- Benefits:
  - NWDAF is an NE in the operator network, which is easily communicating with other NEs using SBA.
  - NWDAF has higher detection precision than RAN/AMF itself since NWDAF could get more data from AMF/SMF/AF.
- Drawbacks:
  - NWDAF cannot guarantee 100% precision, current handling of misinformation may lead normal UE DoS.

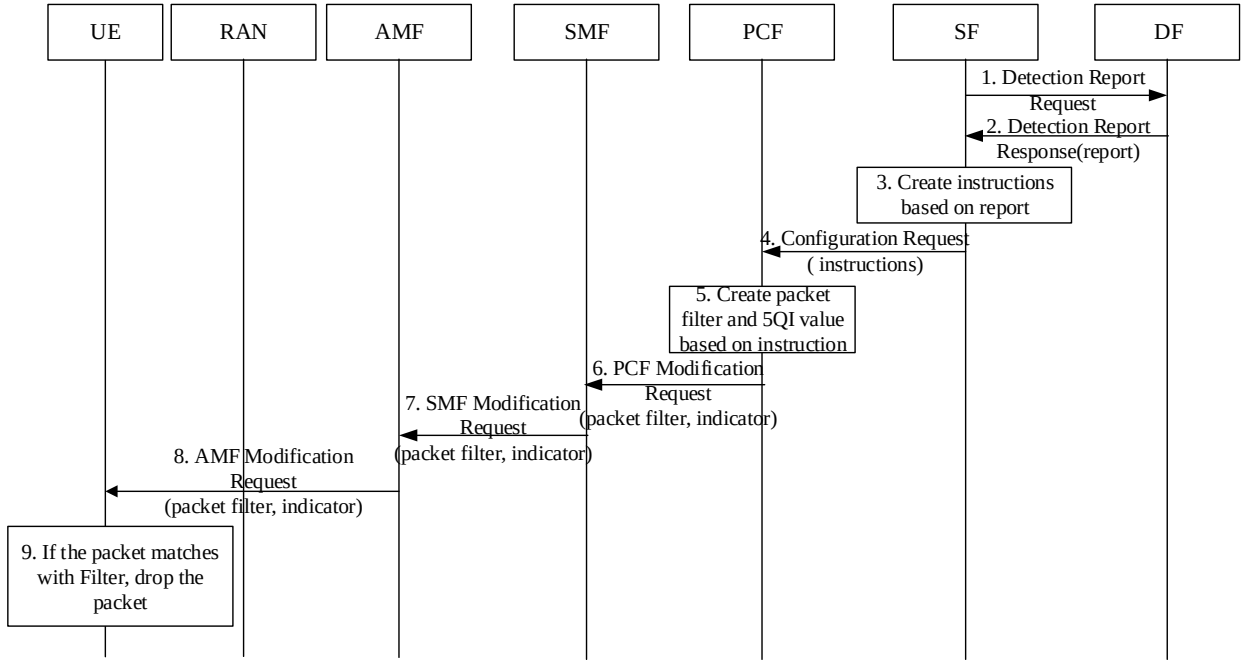
Active Mitigation Method

1. Solution#6: UE Control NAS Signaling Transferring



- Overall:
  - Security Instruction includes:
    - a) Cannot contact certain IP
    - b) Cannot contact the network for next x minutes
    - c) Adopt lower QoS for next z minutes
- Benefits:
  - Control position is the closest to the UE, UE is isolated
- Drawbacks:
  - Control method is strict, may be DoS for the UE
  - Big changes on the UE and AMF

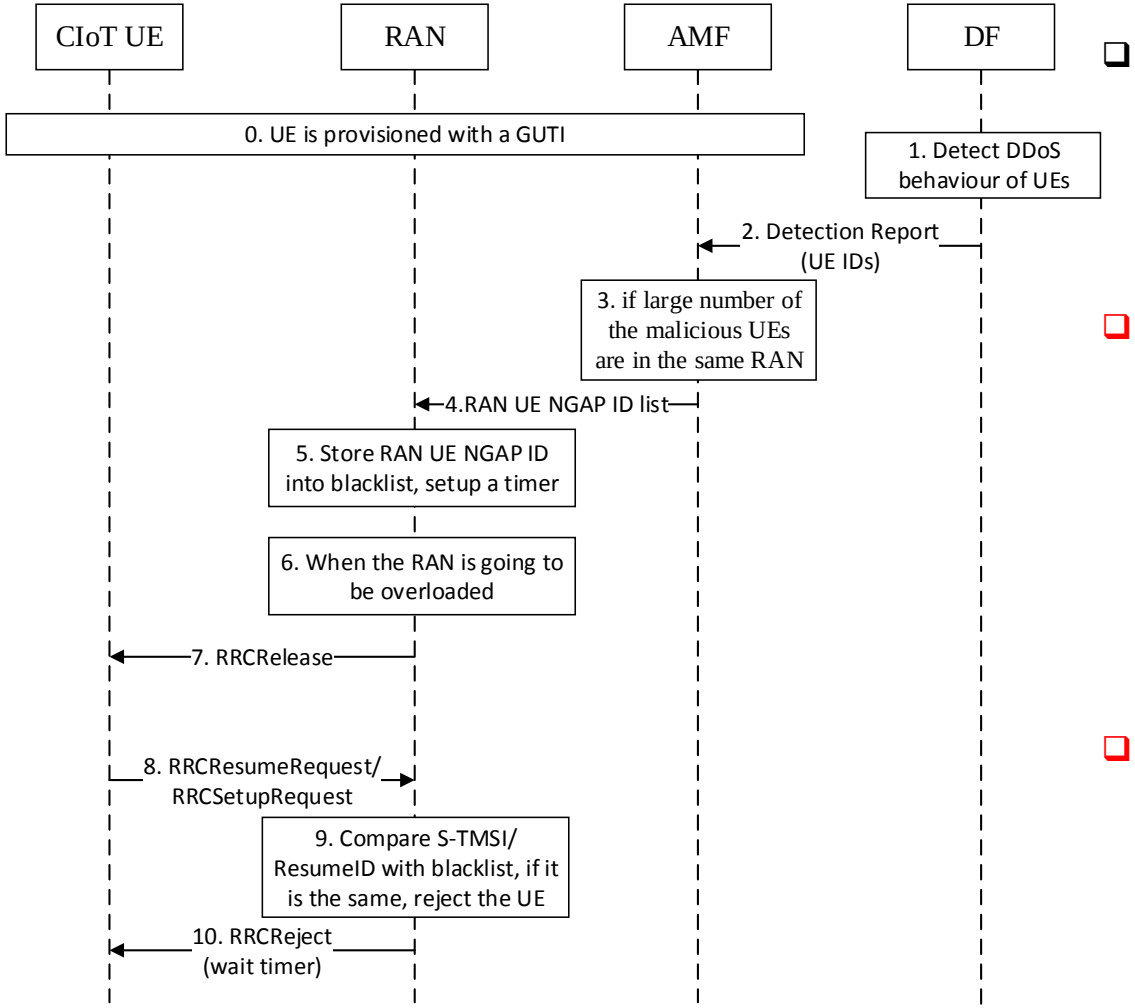
2. Solution#12: UE Drop Malicious Flow



- Overall:
  - Similar like a) security instruction of solution 6, reuse PDU session Modification procedure
- Benefits :
  - Control position is the closest to the UE, malicious flow is isolated.
  - Control granularity is finer, misinformation may not lead UE DoS
- Drawbacks:
  - Misbehaving UE is not completely isolated.

Passive Mitigation Method 1

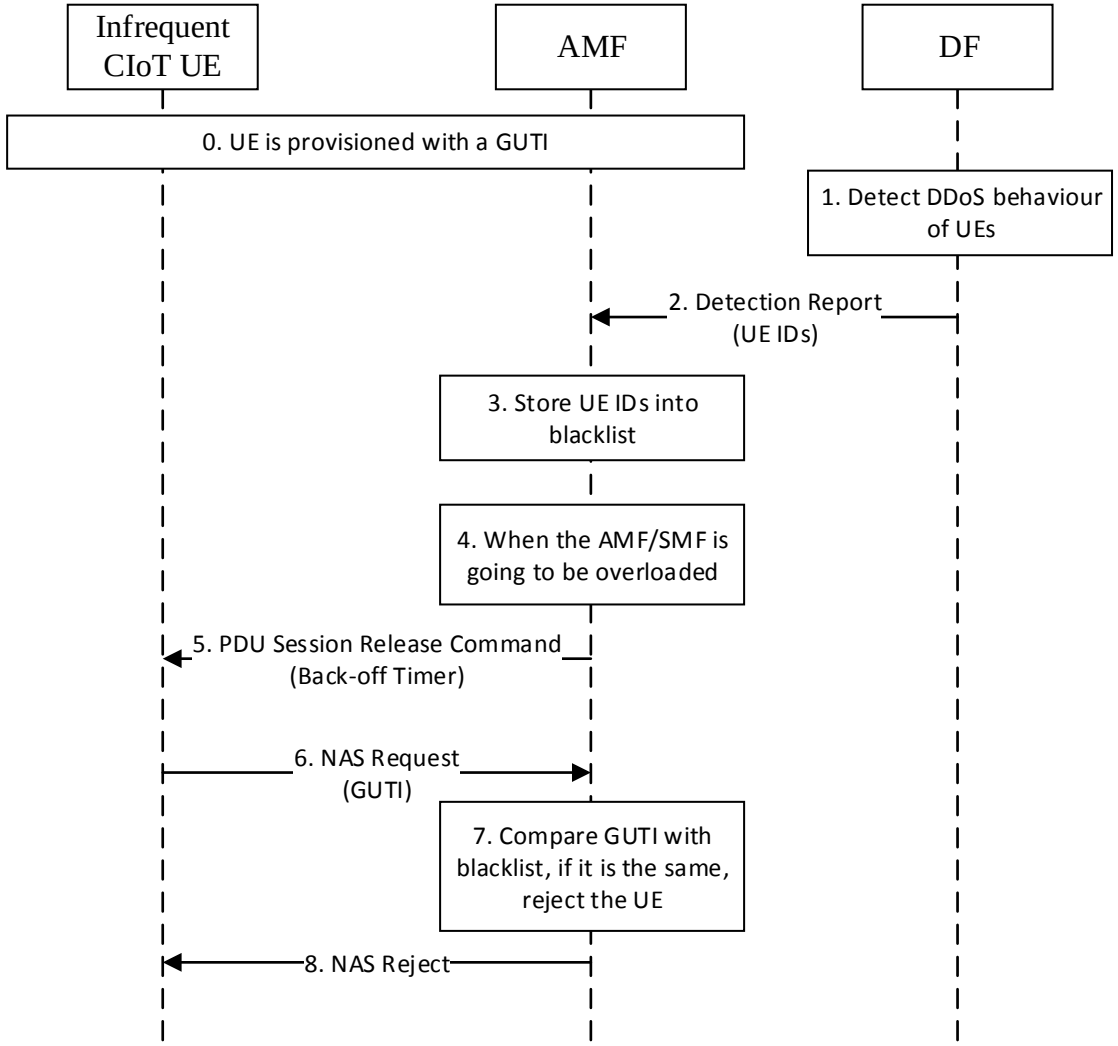
1. Solution#17: RAN protection method



- Overall:
  - Preconfigure misbehaving UE IDs in the RAN.
  - When the RAN is going to be overloaded, the RAN starts to control the malicious UEs.
  - When the RAN is recovered, the handling stops.
- Benefits:
  - Guarantee RAN usability: RAN can protect itself from big malicious 5G user data without changes on the UE.
  - Guarantee UE usability: DF cannot guarantee 100% precision, misinformation exists. In order to mitigate UE impact caused by the manslaughter, the RAN will not launch the blacklist to isolate the UEs under the acceptable bound, i.e. whether it is going to be overloaded. The solution will mitigate unnecessary complaint caused by manslaughter.
- Drawbacks
  - Drawback: Only protect RAN itself, if the RAN could tolerate the attack, the mitigation will not be triggered, but the malicious data flow may be congest on the NEs behind RAN, i.e. AMF.

Passive Mitigation Method 2

1. Solution#19: AMF protection method



- Overall:
  - Preconfigure misbehaving UE IDs in the AMF
  - When the AMF is going to be overloaded, the AMF starts to control the malicious UEs.
  - When the AMF/SMF is recovered, the handling stops.
- Benefits :
  - Align with solution 17.
  - Guarantee AMF usability: AMF can protect itself from big malicious user data sent by infrequent UE without changes on the UE.
  - Guarantee UE usability: DF cannot guarantee 100% precision, misinformation exists. In order to mitigate UE impact caused by the manslaughter, the RAN will not launch the blacklist to isolate the UEs under the acceptable bound, i.e. whether it is going to be overloaded. The solution will mitigate unnecessary complaint caused by manslaughter.
- Drawbacks:
  - Drawback: Only protect AMF itself, RAN is before the AMF, cannot be protected.