**3GPP TSG-SA3 Meeting #102bis-e *S3-211027r1***

**e-meeting, 1- 5 March 2021**

**Source: Apple**

**Title: Adding evaluation for solution#4**

**Document for: Approval**

**Agenda Item: 2.1**

1 Decision/action requested

***It is proposed to add the evaluation for solution#4 in 5GFBS TR 33.809.***

2 References

Null

3 Rationale

This pCR proposes to add the evaluation for solution#4.

There is one EN on the impact of UE power consumption. However, UE power consumption is not in SA3 scope, and SA3 already sent LS to Ran2 on the feasibility of this solution. Therefore, it is proposed to delete this EN.

4 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

6.4 Solution #4: Enriched measurement reports

6.4.1 Introduction

This solution addresses the first security requirement in the following key issue:

- Key issue #3: network detection of false base stations (first requirement).

The solution provides a mechanism for enhancing the detection of false base stations by enriching the measurement reports from the UE. The solution is applicable to UEs in RRC\_IDLE, RRC\_INACTIVE, and RRC\_CONNECTED states.

6.4.2 Solution details

6.4.2.1 Enrichment of measurement report

The UE measurement reports specified in 3GPP TR 38.331 [2] already contain several information relevant for the detection of false base stations, e.g., identifier and received-signal strength information of the cell. Additionally, 3GPP TS 38.331 provides support for reporting of Cell Group Info (CGI\_info) which contains information broadcasted in MIB and SIB1.

In addition to the existing information, the system should support the following new information about camped and neighbouring cells to be included in the measurement report:

- mib\_info = hash of the MIB, which helps in detection of DoS attempts, e.g., cellBarred=barred;

- sib\_info = list of {SIB number, hash of the SIB}, which helps in detection of DoS, fraud, and subscription identification attempts, e.g., ims-EmergencySupport=false, tampered SI-SchedulingInfo, and useFullResumeID=true;

NOTE 1: The sib\_info could contain at least SIB1 which the UE currently obtains to generate CGI\_info.

NOTE 2: The mib\_info and sib\_info could contain their corresponding recorded time.

NOTE 3: The network can set the requesting frequency for CGI info, similar to the ANR frequency configuration. That is implementation specific.

It is suggested to reuse the algorithm of SHA256 to calculate the hashes of MIB/SIBs.

In addition to the information above which can be transmitted by UEs in CONNECTED mode, it is also possible to extend the logged measurements, currently discussed in TS 38.331 for Rel-16, to include the following information that can help in detecting false base stations:

- reject\_info = information about REJECTs that the UE had received earlier, which helps in detection of DoS attempts, e.g., presence of rogue REJECTs;

- signal\_info = information about signal as below, which helps in detection of DoS attempts, e.g., presence of erratic radio signals:

- just power: signal is not associated with any normal pilots or reference signals.

- power with just pilots: signal is associated with normal pilots or reference signals, but those signals do not provide any readable system information.

- power with pilots and system info: signal is associated with normal pilots or reference signals and those signals provide system information, but the system information is wrong (e.g., inconsistent information, not possible to access the network according to the information).

The UE should send the above information to the network only after a successful AS security mode command procedure.

The network should verify and compare the above information with what is expected, e.g., comparing hashes of MIB/SIBs for reported cells with those of genuine cells using the same hash algorithm used in the UE.

To verify the hashes of MIB/SIBs reported by the UE in the MR, the gNB should store the hashes of all broadcasted MIB/SIBs of all cells that belong to the gNB and records the changed time when the MIB/SIBs are modified.

6.4.2.2 Verification of the MIB/SIBs Hashes

When the serving cell receives a MR/logged MR with hashes of neighbouring cell MIB/SIBs, the serving cell can report the MR/logged MR to OAM, then the OAM communicates with the corresponding neighbouring cells to do the MIB/SIBs hashes verification; the serving cells also can communicate with the OAM to get the corresponding neighbouring cell's MIB/SIBs hashes, and verify the reported MIB/SIBs hashes in local. The communication between OAM and cells are implementation specific.

If verification fails, e.g., the hashes do not match, the network may consider it as a factor to detect the presence of the false base station.

During handovers, the serving cell may use the above information, i.e., the MIB/SIBs hashes verification result, to decide whether or not to attempt handover of the UE to the reported neighbouring cell.

6.4.3 Evaluation

Editor's Note: Impacts on UE power consumption is FFS.

Enriched measurement reports certainly help in enhancing the detection of false base stations.

This solution fulfils the first requirement in key issue#3, which is “5G system should be able to detect false base stations.”

This solution has impact on UE and serving RAN nodes. Editor’s Note: Further evaluation is FFS.

NOTE: The definition of new information to be included in measurement reports is out of scope of the present document

**\*\*\*\*END OF CHANGES \*\*\***