**3GPP TSG-SA3 Meeting #107e AdHoc *S3-221371-r2***

**e-meeting, 27 June - 1 July 2022** Revision of S3-20xxxx

**Source: Huawei, HiSilicon, Ericsson, Apple, Philips**

**Title: Evaluation of solution #4**

**Document for: Approval**

**Agenda Item: 5.1 FS\_5GFBS**

# 1 Decision/action requested

***Approve this pCR to add evaluation to solution #4***

# 2 References

[1] S3-211427 (RAN2) Reply LS to SA3 on FBS detection

[2] S3‑193940 (RAN3) Reply LS to SA3 on FBS detection

# 3 Rationale

Evaluations from RAN2 [1] and RAN3 [2] are included in the evaluation clause.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES \*\*\*

### 6.4.3 Evaluation

This solution addresses FBS network detection of Key issue #3. It enhances FBS detection by enriching the measurement reports from UEs.~~The following evaluation is based inputs from RAN2 (S3-211427) and RAN3 (S3‑193940)~~

A) Potential impact to RAN radio interface and resource ~~RAN2 evaluation~~:

1. Regarding hash value reporting:

* Reporting hashes of system information is currently not supported. The logged MDT, mobility history information and CGI reporting procedures could be modified but that requires additional work.
* Regarding MIB/SIBs reading, the existing ~~RAN2~~ procedures already require UEs to read MIB and SIBs:
	+ UEs in RRC\_IDLE/INACTIVE state UEs read MIB/SIB1/other interested SIBs of camped cell. Calculating the hash of these MIB/SIBs is not expected to have a negative impact on power consumption. However, calculating the hash of additional SIBs (i.e. SIBs currently not acquired by the UE) will cause extra power consumption and is not preferred ~~from RAN2 viewpoint~~.
	+ UE in RRC\_CONNECTED state UEs, when configured with CGI reporting, read MIB and SIB1 of neighbour cells. The existing CGI reporting creates interruptions whenever the UE needs to tune in to another cell. Too frequent request of CGI reporting in CONNECTED will not only cause extra power consumption but will also create frequent interruptions. Those impacts become much worse if something else than MIB/SIB1 needs to be acquired. Thus, ~~from RAN2 viewpoint,~~ the scope of CGI reporting (i.e. acquired MIB/SIB1) is preferred not to be expanded and the procedure should not be triggered often.

2. Regarding reporting reject\_info and signal\_info

* The reporting RSRP/RSRQ/RSSI/beam level information of SSB or CSI-RS is supported since Rel-15. And reporting connection establishment failure and radio link failure is supported in Rel-16. If other information is required to be reported, additional ~~RAN2~~ work will be required.

B) Potential impact to RAN network interfaces ~~RAN3 evaluation~~:

- Performing an enriched measurement report does not have any direct impact to ~~RAN3~~ RAN network interfaces.

- There might be ~~RAN3~~ impacts to RAN network interface depending on the triggering mechanism, e.g. if triggered by CN or RAN nodes, NGAP and XnAP might be impacted. However, such impacts are expected to be straightforward and the overhead introduced can be implementation dependent (out of scope of 3GPP). No ~~RAN3~~ impact is foreseen in case the enriched measurements are triggered by the OAM.

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

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

Considering that typical false base stations are mobile and portable, the network based false base detection may be limited to post-mortem diagnostics. In particular, the false base station attacks may be discontinued in the concerned area at the time of detection because precise detection may require the network to collect information from many different UEs.

Reporting hash of SIBs can detect SIB modification or fake SIB injection attacks that would typically result in DoS. Since DoS can be launched against UEs by other means (e.g., jamming), the benefit of enhancing measurement report for this specific attack detection would be very marginal if any. Furthermore, mismatch of hash values is not sufficient for identifying the root cause of the issue, e.g., whether it is due to an attack or bit error in reading SIBs.

For SIB modification or fake SIB injection being successful against the UEs in the connected mode, the attacker needs to broadcast those SIBs with higher power than those transmitted from the legitimate base stations. Such attacks can be detected with the existing power measurement.

It is also possible that a malicious UE may report faked measurements, which may lead to network falsely classifying a legitimate base station as false. Such a classification by the network may lead to degraded service to the UE as the network may decide not to handover the UE to a legitimate base station.

The benefit of the enriched measurement report is very marginal considering the complexity and UE power consumption caused by the extra measurement and reporting.

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