**3GPP TSG-SA3 Meeting #103-e *S3-211598r1***

**e-meeting, 17 - 28 May 2021**

**Source: Huawei, HiSilicon**

**Title: Update to solution #25**

**Document for: Approval**

**Agenda Item: 5.1 FS\_5GFBS**

# 1 Decision/action requested

***Approve this pCR to updates solution #25.***

# 2 References

[1] 3GPP TS 38.211: "NR; Physical channels and modulation”

# 3 Rationale

This document updates Solution #25 and remove NOTE1 and NOTE2.

Removing NOTE1: Since gNB keeps only one RRC connection with a UE with a legitimate identity. A MitM FBS can not have multiple UEs parts with multiple connections/SFN values.

Removing NOTE2: Step3 and step 7 are updated, where an existing RRC message “Assistance information” is used to trigger the detection and deliver SFN value, with an optional IE for each purposeSo it is hard for attackes to know when the detection start.

# 4 Detailed proposal

pCR

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

## 6.25 Solution #25: Detection of Man-in-the-Middle false base stations

### 6.25.1 Introduction

This solution addresses the first requirement of key issue #3 “Network detection of false base stations”.

A false base station (FBS) capable of performing man-in-the-middle (MitM) attacks consists of two parts, i.e. a fake gNB unit and a fake UE unit. The logic between the fake gNB and the fake UE allows an attacker to process incoming message and just forward them, but also drop, manipulate or inject specific messages. These operations require receiving, processsing, and retransmissing the messages and cannot be performed without introducing some processing delay.

This solution is based on the link allocated resource parameters between a UE and the gNB, i.e. UE’s *SFN*(system frame number). The gNB can compare the SFN it has allocated to the UE (it would be the SFN of the “fake UE” if one sits in between) and the “real” SFN that the UE has reported to determine the existence of a FBS.

This solution does not address the scenario where a malicious node RF repeater relays messages of a victim UE to the real gNB. Note that even if such malicious RF repeaters relays are present, those devices cannot perform a MitM attack as such since they cannot drop/inject/manipulate specific messages as such.

### 6.25.2 Solution Details

4. Time resource allocation (SFN2)

UE

gNB

FBS

FakeUE

8. RRC (SFN1)

3. RRC (null)

9. Compare SFN1 and SFN2

5. RRC（SFN Check）

7. RRC (SFN1)

6. Keep UE’s SFN2

1. RRC security established

2. Time resource allocation (SFN1)

(2a)

SR

(2b) DCI (K2)

(4a) SR

(4b) DCI (k2’)

3. RRC（SFN Check）

Figure 6.25.2-1 – Flow diagram showing detection of man-in-the-middle attack

The steps can be summarized as follows.

1. Assuming a UE has established a connection with a real gNB through a MitM gNB. The RRC security is established, i.e. all RRC messages are protected from the FBS.
2. In order for a UE to send a RRC message (to trigger the FBS detection), the UE requests resource from the FBS according to the current RAN procedure. Assuming the set of SFN parameters allocated by the FBS is indicated by SFN1 (in this solution SFN refers to system frame number, subframe number, timeslot, start symbol as well as parameters in the resource allocation message, in particular, the “k2” value).
3. The UE sends a RRC message to trigger FBS detection. To avoid defining a new RRC message, the existing RRC message “UEAssistanceInformation” can be used with a new optional element “SFN Check” to trigger FBS detection.
4. As usual, the FBS intends to forward the RRC message to gNB. First, the FBS (or the fake UE) needs to request resource from the gNB. Assuming the gNB will allocate a set of SFN parameters, i.e. SFN2 to the Fake UE.
5. The FBS (Fake UE) forwards the RRC message to the gNB according to the scheduled SFN2.
6. Once received the “SFN Check” indicator, the gNB stores SFN2 it allocated.
7. The UE sends the SFN1 value (allocated at step 2) in a RRC message (security protected from FBS). To avoid defining a new RRC message, the existing RRC message “UEAssistanceInformtion” can be used with a new optional element “SFN result” (its value set to SFN1).
8. The FBS (Fake UE) unknowingly forwards to the gNB.
9. The gNB compares the SFN1 value received with the SFN2 value stored and determine whether there is a FBS

This solution can be adapted to support “on demand” FBS detection by having the base station send a protected RRC message to the UE indicating that the FBS detection procedure needs to be started. This message is included between message 1 and message 2 in the Figure. Since this message is security protected, the attacker is not able to know the content or tell from a normal RRC messeage.

NOTE1: SFNs are not protected by crypto. So, this solution should study whether a resourceful attacker can acquire all SFNs from legitimate gNB and use the one that fits the case.

NOTE2: This solution may not work against a resourceful attacker that can surreptitiously drop messages.

### 6.25.3 Evaluation

TBA.

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