**3GPP TSG-SA3 Meeting #106-e *S3-220111***

**e-meeting,** **14 – 25 February 2022** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: Update to solution #25**

**Document for: Approval**

**Agenda Item: 5.1 FS\_5GFBS**

# 1 Decision/action requested

***Approve this pCR updates to the Solution #25.***

# 2 References

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

# 3 Rationale

This document provides the text under Evaluation. In addition, revisions to NOTE1 and NOTE2 are proposed due to the following consideration:

For NOTE1: under a causal procedure, an attacker sends a Scheduling Request (SR) message to a real gNB (step 4a) AFTER receiving messages at steps 3 and 2a, where the attacker has to determine the SFN1 before SFN2 is allocated (the attacker needs an oracle to make SFN1 equal to SFN2). Although it is legitimate to send multiple SR messages before it receives from the victim UE (step 4a), it is unlikely to match the victim UE’s timing to the allocated SFN2 by the real gNB, since

* “SFN” here is defined as “system frame number, subframe number, timeslot, start symbol, and the “k2” value. In order to make “SFN1” equal to “SFN2”, the attacker requires k2 (time difference between step 2b and step 3) = k2’ (time difference between step 4b and step 5). This means the step will arrive at FBS later than the required (by gNB) timing of the step 5, since the step 4a happens earlier than the step 2a in this scenario

For NOTE2: It is too strong to assume that an attacker can pin point the RRC message 3 as it has been encrypted. In addition, dropping RRC messages will cause failure events that would make known to the network. It is proposed to remove this NOTE.

# 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 message.

NOTE1: SFNs are not protected by crypto. So, this solution assumesan attacker cannot acquire all SFNs from legitimate gNB beforehand and use the one that fits the case.

NOTE2: To prevent an attacker identify the RRC message 3, the RRC message can be formulated with a different length and sent in a different timing from time to time.

### 6.25.3 Evaluation

.

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

It detects the presence of MitM FBS based on the UE’s report on SFN information.

The solution requires to add a new IE to the existing RRC message “UEAssistanceInformation” for a UE to report as configured.

~~The solution can be adapted to support “on demand” detection if needed.~~

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