**3GPP TSG-SA3 Meeting #101e *S3-202892***

**e-meeting, 09 - 20 November 2020** Revision of S3-20xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title: pCR to 33.809 – New solution for KI #7 and KI #5, based on modified CSI reports**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Adding to TR 33.809 a solution proposal addressing key issue #7 (m-i-t-m fBS detection) and key issue #5 (authentication relay attack) by using modified CSI reports***

# 2 References

# 3 Rationale

This pCR adds a new solution allowing to detect a Man-in-the-Middle false base station, thus addressing Key Issue #7 as well as Key Issue #5.

# 4 Detailed proposal

*\*\*\*\*\* Start of Text (All text new) \*\*\*\*\**

## 6.X Solution #X: Encrypting the CSI reporting to detect MitM

### 6.X.1 Introduction

This solution addresses the following key issues, #7: Protection against Man-in-the-Middle false BS attacks and #5: Mitigation against the authentication relay attack.

In this solution, after AS security setup, UE and the legitimate BS (LBS) agree via encrypted RRC communication on a temporary modification of the CSI reporting. CSI reports will be altered during an agreed time period by the UE in a way that the report still looks valid to the false BS. However, the false BS will interpret the CSI report incorrectly, leading to a notable deterioration of the reception of the radio signal by the UE. The LBS and the UE can detect that the communication is broken or severely deteriorated. Hence both ends can detect that the radio traffic is relayed via a Man-in-the-Middle false base station. If no falseBS is present, no such deterioriation will happen.

The procedure may be triggered on a routinely basis, such as once per hour, or on demand, i.e. when the presence of a m-i-t-m fBS is suspected due to other indications. The LBS may decide to carry out the procedure with multiple UEs to increase the reliability of the detection.

### 6.X.2 Solution details

As mentioned above, the solution depends on the encrypted CSI information exchanged between the LBS and the UE, which the MiTM is not able to decode. The encrypted information comprises:

* An activation instant
* An activation duration
* The CSI report (as described in the dedicated section below)

This information is exchanged in encrypted RRC messages. Encryption must not be deactivated for RRC. The MitM FBS only sees the encrypted message but cannot derive the cleartext content.

Moreover, the information should be passed in a way that analysis of the encrypted traffic does not allow to detect transmission of such information (which would be the case e.g. if this information is sent in a dedicated message type with a unique message size).

#### 6.X.2.1 Detection based on modified CSI reports

Based on the secret agreement between the BS and the UE, the UE sends modified (encrypted) CSI reports. These reports look like normal reports, but the PMI field has been modified (encrypted). These modified CSI reports are correctly interpretable only by the BS. When the FBS exploits these reports, it will pre-code in wrong directions, and the UE will not receive signals, or only at weak power.



Figure 1: Conventional CSI report operation.

In the absence of FBS (above), the UE receives signal from the gNB at nominal power, and reports CSI conventionally.

#### 6.X.2.1.1 CSI reporting Via an FBS



Figure2: CSI reporting via FBS with no detection

In presence of a FBS (above), the UE camps on a cell of the FBS and reports channel measurements to the FBS. The FBS pre-codes the DL signal based on the CSI reports received from the victim UE. In parallel, the FBS/UE sends CSI reports to the gNB which, on its side, pre-codes towards the FBS/UE

 

Figure 3: Detection mechanism activated

Figure 3 above illustrates the operation with the detection mechanism activated between the Victim UE and LBS.

The detection is done as follows:

* In the absence of a FBS (left side), the gNB interprets and decode correctly the CSI reports emitted by the UE and will pre-code towards the UE using the decoded CSI. The UE will receive signal at nominal power.
* In presence of a FBS (right side), the FBS/BS will wrongly interpret the CSI reports from the UE, and will pre-code in a wrong manner. In consequence, the UE will receive only noise, or a much weaker signal power
* The gNB receives the un-coded CSI reports from the FBS/UE, but will treat them as if they were encoded. In consequence, the gNB will pre-code wrongly, and the DL communications between the gNB and the FBS/UE will be severely disturbed or broken.

The operation can be repeated with different CSI reports encodings. In presence of a FBS, the UE will measure significant receive power variations when the encryption method is modified. These power variations happening at predefined times will reveal the presence of a FBS. These power variations can be distinguished from the natural pathloss and fading since they happen abruptly at known instants.

The detection of fluctuating received powers at predefined instant is the indication that the UE is connected to a FBS

In presence of a FBS, the two radio channels (victim UE->FBS/BS and FBS/UE->LBS) are severely disturbed, in consequence the user and control plane data does not go through. The breaking of the end to end connection at the two ends (victim UE and LBS) at the precise moment when the detection mode is activated is a very reliable indication of the presence of an FBS.

Both ends (LBS and UE) gets aware of the presence of a FBS and take appropriate measures to eliminate the threat

6.X.2.1.2 Message Exchange for MitM detection

The Message exchange between the UE and LBS is given below,



Figure 4: Message Exchange between the UE and LBS

## 6.X.2.1.3 CSI reports encryption

The 5G CSI reports contain the following fields:

* CQI (Channel Quality Information)
* PMI (Precoding Matrix Indicator)
* CRI (CSI-RS Resource Indicator)
* SSBRI (SS/PBCH Resource Block Indicator)
* LI (Layer Indicator)
* RI (Rank Indicator) an/or L1-RSRP

The proposed detection mechanism will keep all CSI fields unchanged, except the PMI field. The precoding matrix determines how the individual data streams (called layers in LTE) are mapped to the antennas. The 5G framework is very rich and contains a lot of options described in 3GPP TS 38.214.

6.X.2.1.4 Eaxmple PMI Encryption

 As an illustration, we describe the PMI encryption principle of the invention in the simplest configuration mode ‘Type I Single Beam (L=1) Codebooks: Rank 1’. The principle can readily be extended to all the other modes. In this mode, the UE reports the coordinates of the beam it receives at the highest power. As shown on Figure 4



Figure 5: Beam grid, and selected beam in Type 1, rank 1. Horizontal and vertical axis. ‘O’ refers to the spatial oversampling factor

These coordinated are 2 integer numbers i11 and i12 for the horizontal and vertical directions respectively. The principle of the encryption is to apply perturbations to each of these values. Without knowing these values, the MitM will not receive the beams correctly at the designated instances, this will result in loss of RF link or very poor reception at the UE designated instances.

### 6.X.3 Evaluation

The solution allows to detect the presence of a Man-in-the-Middle false base station after setup of AS security.

The solution requires to transmit additional information between UE and the gNB in encrypted RRC messages.

This solution cannot prevent that the UE camps on a cell of a false base station that has not yet been detected, but it allows that the gNB detects the false base station when it operates as a Man-in-the-Middle. Subsequently, the faked cell may be blacklisted.

*\*\*\*\*\* End of Text \*\*\*\*\*\*\*\**