

A Study on 5G NR Based False Base Station Detection Technology

Kisoon Sung^{*}, Hyungdeug Bae, Yousun Hwang, Jisoo Shin,
Sungmin Oh, Jong-Geun Park

Electronics and Telecommunications Research Institute
{Kssung, hdbae, ys3838, smoh, jshin, queue}@etri.re.kr

Abstract

5G NR-based mobile communication technology is a network infrastructure that can provide advanced services to industries, defense, and public sectors as well as communications for individuals through eMBB (enhanced Mobile Broad), URLLC (Ultra-Reliable Low Latency Communication), and mMTC (massive Machine Type Communications). In other words, instead of the large nationwide network provided by a small number of operators, demand organizations or operators can build custom wireless networks within a limited range of buildings, facilities, and land. This is a critical infrastructure that can provide state-of-the-art services, while also being a major target for cybersecurity attacks. One of the various attack methods, the false base station, simulates the cell information of the normal base station. This induces the UE to access itself, leading to service disconnection and delay. This can be a fatal attack on defense or industrial sectors that are sensitive to delays. In this paper, we propose several solutions that can detect false base stations and present test results that can verify one of the solutions.

Keyword: 5G NR, False base station, SSB time offset, RRC measurement report

1 Introduction

3GPP 5G provides a variety of technologies aimed at advancing technologies such as eMBB (enhanced Mobile Broad), URLLC (Ultra-Reliable Low Latency Communication), and mMTC (massive Machine Type Communications). Beamforming and massive MIMO technologies were introduced to efficiently use high frequency and ultra-wideband frequencies, and network slice technology that supports flexible network structures was applied to ensure the quality of high-latency or high-trust services.

This technological growth has resulted in the expansion of the domain to which existing mobile communication is applied. This enables the establishment of a wireless network to apply 5G services within a limited range such as smart factories, smart cities, hospitals, construction sites, power plants, and concert halls/stadiums, rather than a network for personal communication services provided nationwide by several operators. Major countries around the world are already accelerating the use of

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19- 21, 2023, Okinawa, JAPAN, Article No. 37

^{*}Corresponding author: Electronics and Telecommunications Research Institute, Daejeon, 34129, Republic of Korea,
Tel: +82-042-860-6114

5G specialized networks by supplying frequencies dedicated to them and creating service environments in various fields.

As the nature of data transmitted and received through mobile networks changes, it can be a good target for hackers. Attacks on 5G mobile networks can appear in various forms, but we define attack using false base station in this paper and propose defense solutions of them. We also present experimental results on feasibility one of the proposed solutions.

2 Definition of False Base Station

False base stations induce UEs within the coverage of normal base stations to access themselves. This type of attack causes service disconnection or delay, which significantly lowers service quality. To describe in more detail, false base stations simulate cell information such as SSB (include Synchronized signal, physical cell id and MIB) and SIB1 of normal base stations, and broadcast that information with stronger power near normal base stations. As a result, UEs synchronize with the false base station and attempt to access that. False base stations can attract UEs sufficiently up to procedures that can be performed using system information, that is, initial random access and RRC connection establishment procedures. However, for *RRCSetupComplete* messages sent by UE after RRC connection is established, false base stations can no longer simulate normal base stations and carry out the remaining procedure because it includes an initial NAS message delivered to the core network, and the response is the authentication message of the UE. False base stations do not know UE subscription information that is in the USIM and HSS in the 5GC for authentication, the procedure will fail. UE will retry the procedure that has failed as possible as it is configured and finally try to find another cell. Attacks that cause time delays like this are very fatal to smart factories, defense-related systems and medical systems that perform delay-sensitive processes.

In order to discuss how to detect attacks by false base stations, it is decided how false base stations attack mobile networks. In this paper, it is assumed that a false base station attacks by simulating a normal base station in the same way. In other way, a false base station copies all information of a normal base stations, physical cell ID, parameters in system information. This is because if a false base station attacks using its own physical cell ID or system information, it can be easily detected through various methods, such as reporting measurement information that has neighbor cell ID, RSRP, Global cell ID, and so on. Because base stations know neighbor cell's physical cell ID in general, if they are reported by UE unknown physical cell ID, then request more information about information about cell has unknown ID, that is Global Cell ID. This consists of the MNC + MCC + gNBID + cellID that is the unique ID in worldwide and broadcasted in SIB1. If false base stations use its own physical cell ID or system information that is not same information of normal base stations, it's only a matter of time before it's revealed.

As a result, network can know the existing of a false base station and its physical cell ID. Although network manager cannot remove false base stations physically, it can broadcast black cell list to prohibit access to the cell and change physical cell ID of the normal base station.

3 Case study of False Base Station Detection

In this chapter, we discuss some solutions to detect false base station attacks.

3.1 Solution using UE information procedure

RRC (Radio Resource Control) is one of the 3GPP wireless communication protocols that perform functions such as radio resource management, connection management between UE and gNB, measurement reporting, and handover. The UE information procedure is defined in the RRC layer to report various situations such as RRC connection failure, handover success, and RLF that the UE experiences within the specific cell to the base station.

Figure 1 describes the UE Information procedure and some of parameters included in the *UEInformationResponse* message.

UE Information procedure is triggered by the base station transmitting the *UEInformationRequest* message to the UE, and then the UE reports the information collected for a certain period to the base station using the *RRCInformationResponse* message.

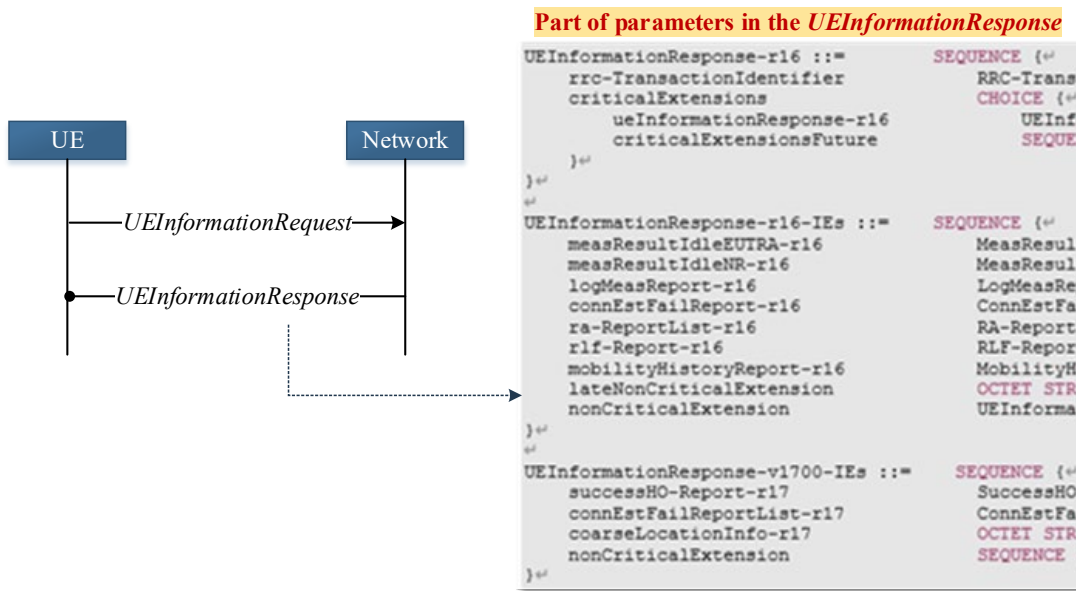


Figure 1: UE information Procedure and Parameters of *UEInformationResponse* message [1]

Figure 2 describes the flow in an example of detecting false base stations using UE information procedure. BS#1 is a serving cell that receives reports from the UE, normal base station #2 is nearby, and false base station #2 that simulates it exists.

It is assumed that the false base station successfully attracts the UE to the initial random-access procedure and then sends an *RRCreject* message in the process of establishing an RRC connection, or interferes with the RRC configuration of the UE in other abnormal ways to cause service delay.

The UEs may report to the serving cell what happened in the other cell using a message indicating a failure by attempting to access a specific cell. The UE does not know whether the BS #2 it accessed is a normal base station or a false base station, but information on RRC setup failure can be accurately reported and BS#1 sends relevant information to the False Cell Detector. BS#2 also sends information to the False Cell Detector on the number of times an RRC failure occurs when the UEs attempt to access itself. If a false base station exists, the number of failed transmissions from BS#1 will be much higher than those transmitted from BS #2. The False Cell Detector can detect the existence of false base stations based on this information.

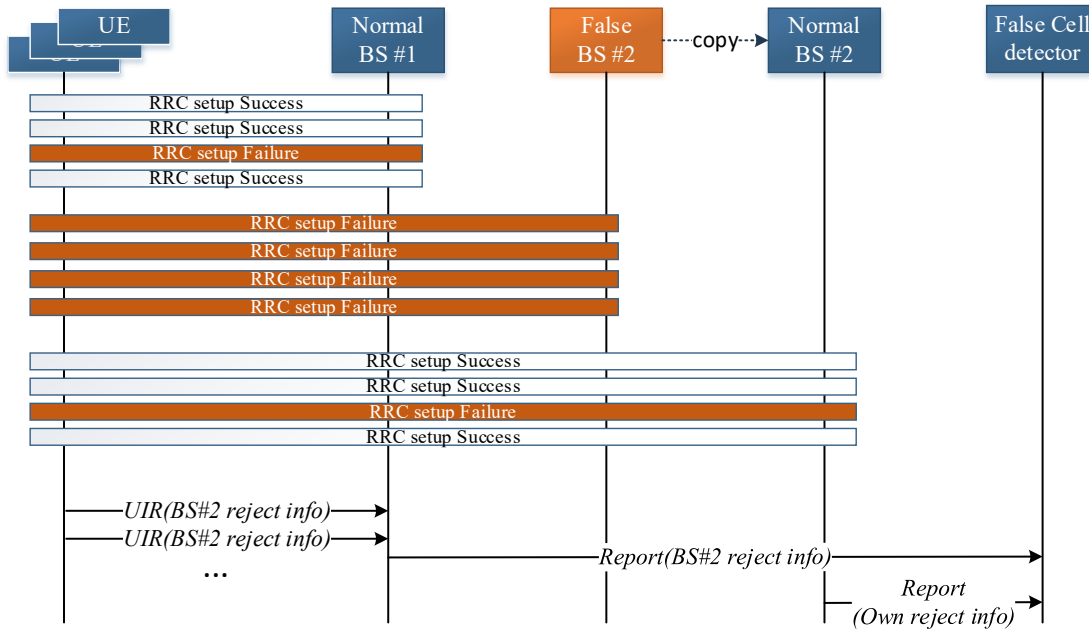


Figure 2: Example of False Base Station detection using UE Information procedure

However, this solution alone cannot be completely sure that a false base station exists because the quality of the radio wave environment is determined by various variables other than false base stations. In addition, this solution can determine that false base stations exist after multiple UEs have already undergone connection failure and RLF, so a preemptive response to block the connection itself is impossible. However, it can be used as a good basis for determining that false base stations may exist in parallel with other detection technologies.

In other words, it can be used as a good basis for detecting that false base station may exist in parallel with other detection technologies.

3.2 Solution using Handover Failure

This solution is to detect the presence of false base stations through handover induced by false base stations. Figure 3 describes the procedure in which a false base station (Cell#1) attracts a UE with the same physical cell id as normal base station (Cell#1). In this case, the false base station will broadcast the SSB with a strong signal to attract the UE, but even if the UE is attracted to the false base station, the handover command (*RRCReconfiguration*) will be transmitted by the normal base station (Cell#1). In this case, if the normal cell power is sufficient, the handover will succeed, but if there is not enough signal, the handover will fail. [2]

This paper does not discuss false base stations that simulate physical cells differently from normal neighbor base stations because the neighbor cell information held by the serving cell immediately reveals that it is a false base station.

If a UE is lured to a false base station and a handover starts, the possibility of handover failure is very high, so if handover failures occur exceptionally frequently in a specific area, the existence of a false base station may be suspected.

In this case, as in the solution described in the previous chapter, false base stations can be detected only after many UEs have been reported to have suffered multiple handover failures, and if there are

many fixed UEs with not much mobility, there are few handover occurrences and detection is impossible.

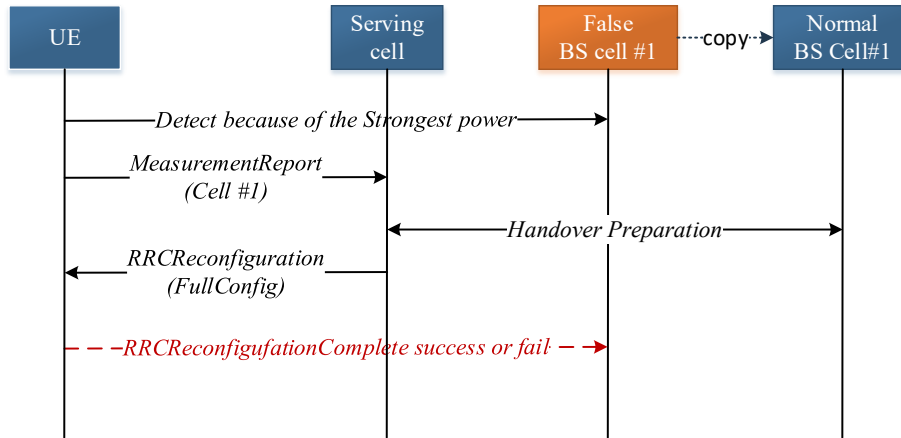


Figure 3: Handover procedure induced by false base station [3][4]

3.3 Solution using measurement of SSB/SIB1

A synchronization signal block (SSB) is an information block consisting of cell synchronization signals and master information block (MIB) information. The base station broadcasts the SSB per cell at predetermined intervals at predetermined times.

The UE that receives the best quality SSB synchronizes with the cell, then acquires the remaining system information using the physical cell id and MIB that include in SSB, and acquires time synchronization with the base station. In other words, the SSB contains key information of the base station, and if this information can be analyzed closely, it can be noticed that a false base station exists in the area.

So, if the UE uses the Measurement Report procedure to report the SSB information of the neighbor cell to the serving cell, the central monitoring system analyzes this information and can find that a false base station exists in a specific area.

In this paper, based on SSB measurements, we want to define specific scenarios to avoid attacks from false base stations and apply them to a test bed to present experimental results that can actually detect false base stations.

4 Study of false base station detection technology using SSB & SIB1 measurement report

4.1 False Base Station Detection Scenario

Figure 4 describes the network configuration for testing false base station detection technology using SSB measurement reports. [5]

As mentioned above, it is assumed that the false base station conducts an attack that induces the UE to itself and degrades service quality by simulating the physical cell ID and system information of the normal base station in the same way.

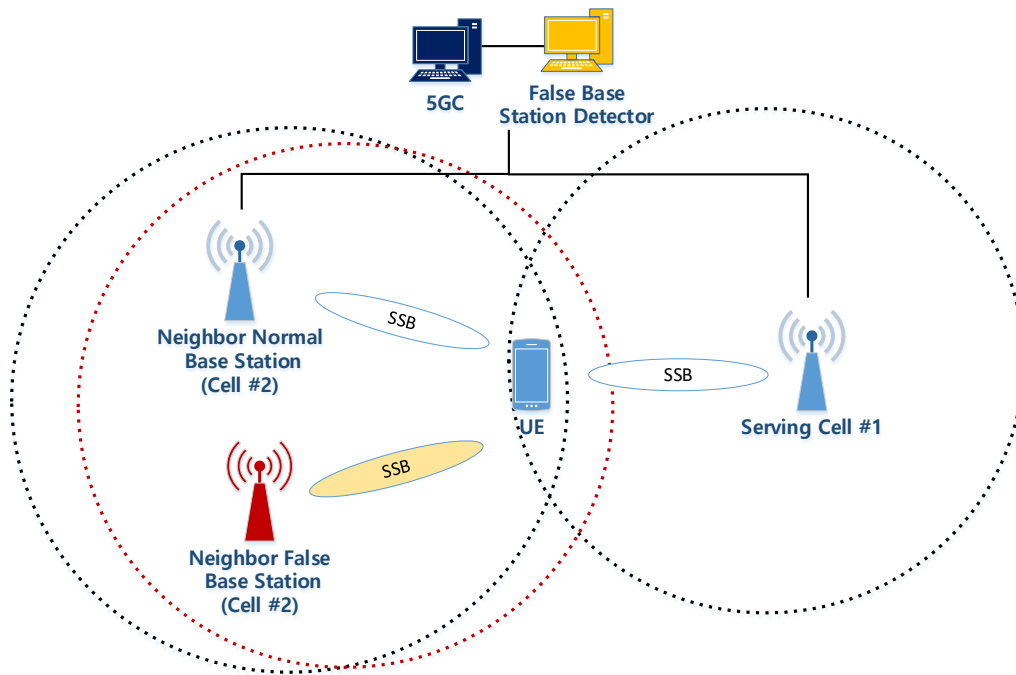


Figure 4: Network Architecture for test of False Base station detection

The UE is connected to the serving cell, and reports measured information about the neighbor cell. Measurement targets reported by the UE are as follows:

- Physical Cell Id
- SFN/Slot number
- RSRP
- SSB time-offset
- SIB1 information

Here, the SSB time-offset refers to difference of SSB transmission timing between serving cell and neighbor cell. Figure 5 schematically shows the definition of time-offset.

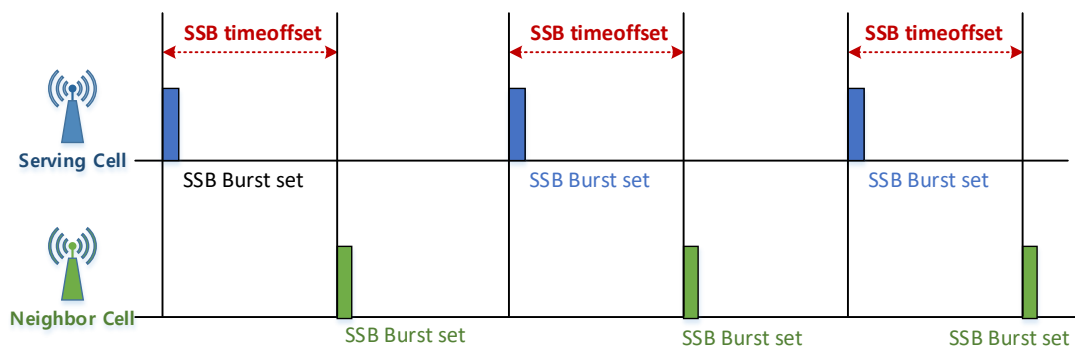


Figure 5: Definition of SSB time-offset

The UE modem needs time to synchronize with each cell to acquire global cell ID information contained in SIB1 in addition to the physical cell ID and RSRP that can be measured through SSB, read SSB, determine SSB1 transmission timing using the information, and decode SSB 1. In this test, measurement information is reported at the upper layer over time as shown in Figure 6.

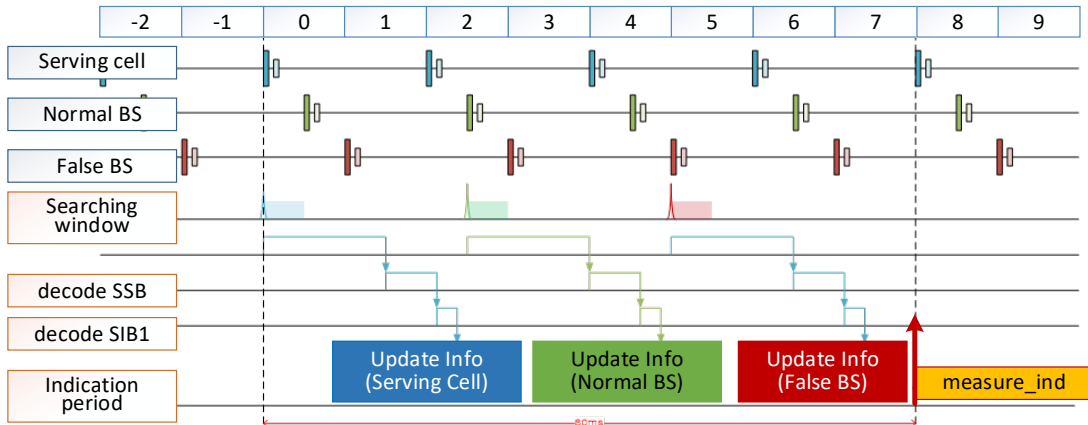


Figure 6: Operation of model for measurement on UE side

The upper layer that receives measurement information from the modem reports the information to the base station according to the measurement configuration, and the base station delivers the reported information to the False Cell detector.

False Cell detector knows cell composition information in a specific area in advance, such as cell placement, physical cell ID of the placed cell, Global Cell Id, SSB transmission timing, and RSRP range valid at a specific location. Based on this information, when receiving neighbor cell information measured by the UE from the base station, if information different from the cell configuration information is found, it is detected that a false base station is hidden in a specific area.

If the false base station accurately simulates the timing of transmitting SSB and system information with the normal base station, it is expected that the RSRP of a specific cell will grow or decrease outside the normal range. This is because the signals may overlap and be amplified or offset. Using this information, it is possible to predict that a false base station may exist. Otherwise, if the false base station broadcasts the same information as the normal base station, but transmits it with a time offset, the same information is measured at a time lag, so it can also be seen that there is a false base station in the central monitoring system.

4.2 Test environment and result

Figure 7 is the picture of lab for testing False cell detection solution. Testbed have 5GC, 3 base stations, on UE and the False Cell Detector. The 5G mobile network consists of one serving base station and one normal neighbor base station, which is connected to 5GC. The serving base station is connected to its DM that displays various operation information including measurement data reported from the UE. A false base station that simulates a normal neighbor base station operates separately from 5GC.

There is one UE that will connect to a serving base station and report measurement data of a neighbor base station.

The False base station detector determines the existence of a false base station by comparing the measurement information of the UE received from the serving base station with the cell configuration information.



Figure 7: Test Environment for False Cell Detection

If the SSB transmission time-off of the normal and false base stations is different, the test results are shown in the Table 1. Since there are two base stations that transmit the same system information with the same cell ID, the false base station detection result is 100% reliable.

Table 1: Test flow and result of False Base station detection using SSB transmission time offset

No.	Description	False Cell Detector
1	<p>[Step 1]</p> <ul style="list-style-type: none"> - Serving Cell power on - UE power on - UE access Serving Cell - gNB config UE measurement report parameter - UE report Serving Cell info <p>[Result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -61 	
2	<p>[Step 2]</p> <ul style="list-style-type: none"> - Normal Neighbor Cell power on - UE report Serving Cell, Neighbor Cell info <p>[Test result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -61 <p>Normal Neighbor Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 200 - Global Cell ID: 520093696 - RSRP (dBm): -61 - SSB SFN difference: 390 	

<p>3</p>	<p>[Step 3]</p> <ul style="list-style-type: none"> - False Neighbor Cell power on - UE report Serving Cell, Neighbor Cell <p>[Test result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -61 <p>Normal Neighbor Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 200 - Global Cell ID: 520093696 - RSRP (dBm): -52 - SSB SFN difference: 260 <p>False Neighbor Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 200 - Global Cell ID: 520093696 - RSRP (dBm): -52 - SSB SFN difference: 552 	<p>- Duplicated Physical cell ID/Global Cell ID</p> <p>- Difference SSB offset</p> <p>→ Detect False Base station</p>
----------	--	--

If the SSB transmission time-off of the normal base station and the false base station are the same, the test results are described in the Table 2. It can be seen that the RSRP becomes abnormally large due to the overlapping of signals. In an actual environment in which the UE moves, when the UE reports location information together, it may have a considerable meaning. If an RSRP outside the range is reported in a situation where the cell knows the effective range of the RSRP within a specific cell service area, it can be determined that there is a false base station.

Table 2: Test result of False Base station detection using RSRP

No.	Description	False Cell Detector
<p>1</p>	<p>[Step 1]</p> <ul style="list-style-type: none"> - Serving Cell power on - UE power on - UE access Serving Cell - gNB config UE measurement report parameter - UE report Serving Cell info <p>[Test result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -59 	

<p>2</p>	<p>[Step 2]</p> <ul style="list-style-type: none"> - Normal Neighbor Cell power on - UE report Serving Cell, Neighbor Cell info <p>[Test result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -61 <p>Neighbor Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 200 - Global Cell ID: 520093696 - RSRP (dBm): -62 - SSB SFN difference: 774 	
<p>3</p>	<p>[Step 3]</p> <ul style="list-style-type: none"> - False Neighbor Cell power on - UE report Serving Cell, Neighbor Cell info <p>[Test result]</p> <p>Serving Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 100 - RSRP (dBm): -61 <p>Neighbor Cell info</p> <ul style="list-style-type: none"> - Physical cell ID: 200 - Global Cell ID: 520093696 - RSRP (dBm): -52 - SSB SFN difference: 22 <p>→ Suspect False Base station</p>	

As a result of this test, it can be seen that false base stations can be sufficiently detected through measurements such as SSB transmission timing, SIB1 information, and RSRP.

5 Conclusion

False base stations that attract UEs by simulating normal base stations without connection with the core network fail to connect UEs to connect, but can cause service delays/disruption, resulting in lower service quality. This can be a fatal attack in networks that provide delay-sensitive services. Although the false base station detection technology mentioned in this paper cannot identify the physical location of the false base station due to the nature of the false base station, if it detects that a false base station simulating a specific cell is hidden in a specific area, the cell can be blacklisted and immediately changed the cell ID of the normal base station to prevent inducement to the false base station as much as possible.

When this technology is applied to UE exclusively for detecting false base stations, its utility may increase. It is a technology that is highly utilized in smart factories, smart medical care, and defense, which must provide delay-sensitive services.

Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability)

References

- [1] Radio Resource Control (RRC) protocol specification. Technical Report 38.331, 3rd Generation Partnership Project, 2022.
- [2] Study on 5g security enhancement against false base stations. Technical Report 33.809, 3rd Generation Partnership Project, 2022.
- [3] Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description. Technical Report 36.300, 3rd Generation Partnership Project, 2023.
- [4] NG-RAN; NG Application Protocol (NGAP). Technical Report 38.413, 3rd Generation Partnership Project, 2018.
- [5] System architecture for 5G System (5GS). Technical Report 23.501, 3rd Generation Partnership Project, 2017.