January 2021

Rogue Base Station Detection Techniques

Madhu Venkata

ROGUE BASE STATION DETECTION TECHNIQUES

Abstract

User equipment (UE) and cellular networks implement one or more techniques to detect and mitigate rogue base stations/cells. In one approach, a UE implements base station authentication techniques for detecting and mitigating rogue base stations. In this approach, the UE detects a failed authentication procedure and determines the associated base station is a rogue base station. The UE stores identifying information associated with the rogue base station and location information associated with the UE. Upon attachment with a legitimate base station/cell, the UE sends the identifying information and location information to the network. In another example, the network implements reverse mobility detection techniques for detecting and mitigating rogue base stations. In this approach, static mobile UEs are located throughout the network and monitor signal strength variations associated with cells for detecting rogue base stations. In yet another approach, a UE is configured to detect when a base station is attempting to downgrade the UE to a lower order radio access technology (RAT) and identifies the base station as a rogue base station. In a further approach, a UE is configured to determine when a received signal strength indicator (RSSI) is abnormally high, indicating that a rogue base station is using a signal-jamming mechanism.

Background

Rogue base stations are standalone devices that mimic legitimate base stations in a cellular network. A rogue base station intends to have user equipment (UE) connect to the rogue base station rather than a legitimate base station. Rogue base stations are not connected to the core network and typically operate by mimicking the cell identifier (ID), frequency of operation, mobile country code (MCC), mobile network code, etc., of a legitimate base station. Rogue base stations often transmit at a much higher power than a legitimate base station. Therefore, a UE may unintentionally connect

to a rogue base station since UEs are typically configured to connect to the base station with the strongest signal.

Once a UE is connected to a rogue base station, the rogue base station can perform various malicious acts. For example, private information of the UE, such as the international mobile subscriber identity (IMSI), can be exposed to the rogue base station since the UE typically sends this information to the network before authentication and security procedures are in place. Therefore, the rogue base station can intercept, decode, and alter communications from the UE before they are encrypted. In another example, the rogue base station can capture signaling messages sent by the UE over the air before encryption. Since the signaling messages are captured before being encrypted, the rogue base station can use, for example, standard Abstract Syntax Notation (ASN) to decode the messages. After the messages are decoded, the rogue base station can extract UE specific information such as the IMSI of the UE. The rogue base station may also attempt to downgrade the UE to a lower order Radio Access Technology (RAT) with lesser security mechanisms. As such, rogue base stations result in critical security concerns for a cellular network, financial loss for network operators, negative user experience, and so on.

Description

As described below, rogue base stations (cells) can be detected and mitigated (e.g., barred) using UE-based and network-based approaches, individually or in combination. These approaches, which can be implemented in various scenarios, include base station authentication techniques, rogue base station detection using reverse mobility techniques, detection and prevention of network/RAT downgrade attacks, and detection of signal jamming mechanisms.

For example, a first scenario is directed to a cell selection situation where a UE powers on in a rogue base station coverage area. In this example, a UE identifies cells, which may be legitimate

cells or rogue cells, during an initial scan. The UE selects the cell having the strongest signal. Rogue base stations are typically configured to transmit at higher power than neighboring legitimate base stations to increase the likelihood that a UE will connect to the rogue base station rather than a legitimate base station. The UE checks the public land mobile network (PLMN) code sent by the base station to a subscriber identity module (SIM) PLMN code. If the PLMN codes match, the UE checks the S-criteria for cell selection. Assuming the rogue base station is transmitting at a higher power than the legitimate base station, the cell selection passes on the rogue cell, and the UE proceeds to camp thereon. The UE initiates an attach procedure during which the UE may send its identity before an authentication procedure is performed, thereby enabling the rogue base station to capture unencrypted UE information, such as IMSI, international mobile equipment identity (IMEI), and so on. As such, a user's private data can be stolen by the rogue base station and used to perform illegal activities.

A second scenario is directed to a cell reselection situation. In this situation, a UE device, which is already in idle mode and camped on a legitimate cell, comes near and identifies a rogue cell. The UE determines that the rogue cell has a better cell strength than the legitimate cell and may reselect to the rogue cell. Cell reselection is an autonomous process performed by the UE without any network intervention. In a Fourth Generation (4G) Long-Term Evolution (LTE) network, the UE may initiate a tracking area update procedure. As part of this procedure, the UE may expose information specific to the UE that is captured by the rogue base station of the cell. Hackers can then use the captured information to extract personal information. As such, a user's private data can be stolen by the rogue base station and used to perform illegal activities.

A third scenario is directed to a handover situation. In this situation, a UE is in a connected state, identifies an intra-frequency rogue cell, and sends a measurement report to the network. The

network configures intra-frequency measurements for handover/mobility. If the rogue base station is transmitting in the same E-UTRA Absolute Radio Frequency Channel Number (EARFCN) as a legitimate base station, the UE may report the cell ID of the rogue base station along with the RSRP. If the cell ID is known to the legitimate base station, a handover may occur to the rogue base station. In at least some instances, the authentication may already be enabled during handover, so the rogue base station may not decode the UE information. However, the UE will lose its connection to the network when the UE connects to the rogue base station. Therefore, the user will experience a service interruption.

One approach for detecting and mitigating rogue base stations is shown below in Figure 1. In this approach, base station authentication techniques are implemented for detecting and mitigating rogue base stations. For example, an LTE or other standard-based network provides a robust authentication mechanism that will authenticate both the UE and network. The authentication procedure takes place each time the UE powers on and attempts to attach to the network. Once the authentication procedure is successfully completed, both the UE and the network can assume each other are legitimate entities. However, the input to the authentication procedure is the ID of the UE, such as the IMSI or IMEI. This information is typically sent by the UE before the authentication and security procedures are performed. For example, an identity procedure is performed before authentication. As part of the identity procedure, the network sends an identity request to the UE, and the UE responds with an identity response, which includes the UE ID.

A rogue base station mimics this process by sending the Identity request to the UE and captures the UE's response. The rogue base station may or may not respond with an authentication procedure. In either case, the authentication procedure fails when the base station is a rogue base station. Therefore, once the UE sends an identity response to a base station and the authentication procedure

subsequently fails, the UE determines the base station is a rogue base station (cell) and does not camp on the cell until the next power cycle. The UE can store its Global Positioning System (GPS) coordinates and information, such as the cell ID, EARFCN, and PLMN ID, associated with the failed rogue base station, in a rogue base station/cell list. Therefore, the next time the UE detects a cell, the UE can compare one or more of the GPS coordinates, cell ID, EARFCN, PLMN ID of the cell to corresponding information in the rogue base station/cell list. If matching information is found in the rogue base station list, the UE determines the cell is a rogue base station and does not camp on the cell.

Upon detection of a failed cell, the UE continues to select any other cell. If the UE can complete a successful authentication procedure on a new (legitimate) cell and attach to it, the UE notifies the network of the detected rogue base station(s). For example, the UE can send information associated with the rogue base station (e.g., GPS coordinates, the cell ID, EARFCN, PLMN ID, etc.) to the network. The UE can send the rogue base station information to the network through a signaling message or another mechanism. Alternatively, the UE can update a cloud server of the carrier with the rogue base station information. The carrier and law enforcement can then take appropriate action on the rogue base station information based on, for example, the GPS coordinates provided by the UE. In some instances, law enforcement may deploy base stations to capture criminals. These devices can be whitelisted so that the UE does not flag them as rogue base stations.

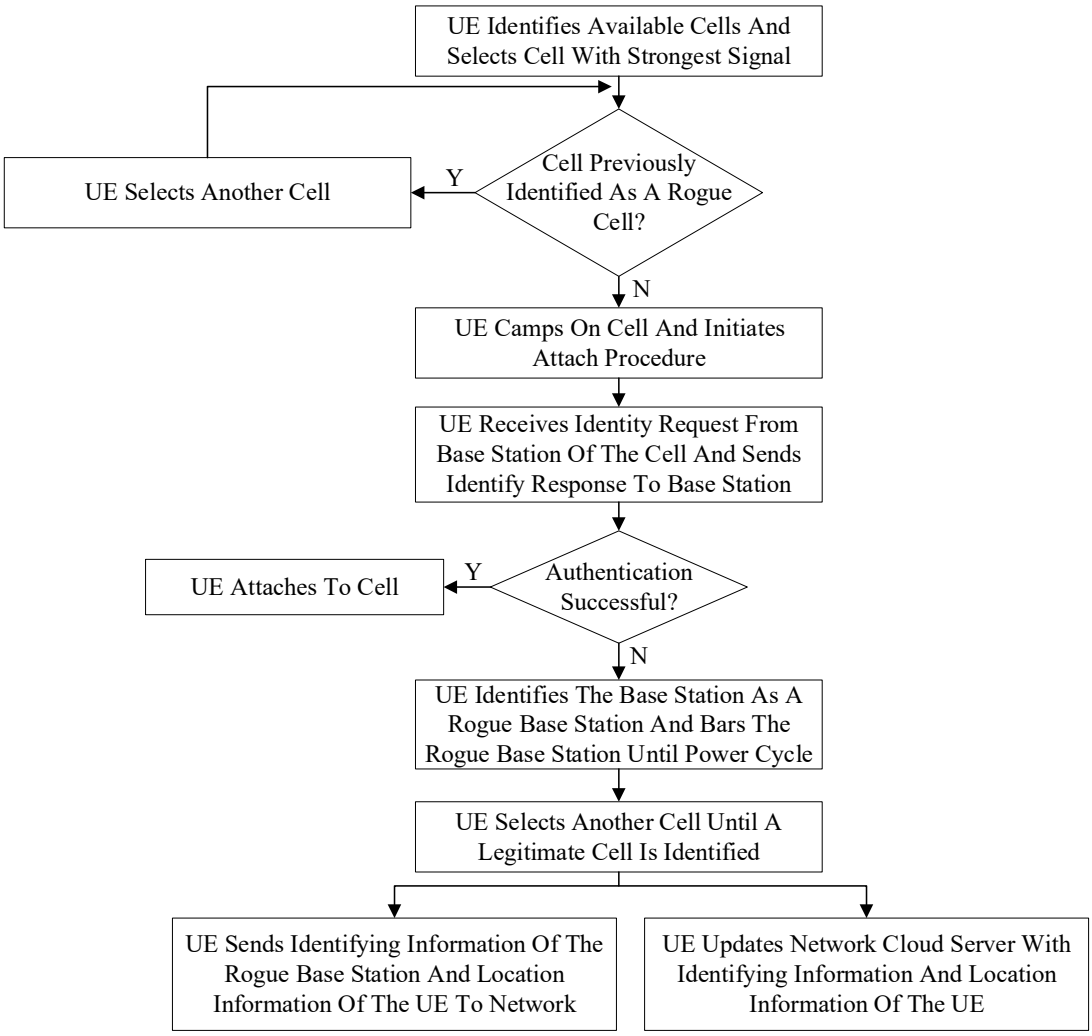

Figure 1

A second approach for detecting and mitigating rogue base stations is shown below in Figure 2. In this approach, reverse mobility techniques are implemented to detect and mitigate rogue base stations. Legitimate base stations are typically static, while UEs are generally mobile. Rogue base stations can also be mobile to capture the information of as many UEs as possible. For example, rogue base stations can be installed on the top of a vehicle. The vehicle can be driven across the network to capture the details of many UEs. Mobile rogue base stations can be detected and mitigated by installing static UEs in several locations throughout the network, such as in operator stores. An application can be installed on the static UEs that monitors signal strength variations of

detected cells. Wide variations in signal RSRP or Received Signal Strength Indicator (RSSI) is not expected from a well-planned legitimate base station. However, since a mobile rogue base station moves across the network, wide variations in signal RSRP or RSSI can be expected. As such, the application performs statistical analysis (e.g., mean, standard deviation, etc.) of signal characteristics, such as signal strength, using machine learning. If sudden or unexpected variations are detected, the static UE determines a mobile rogue base station is nearby. The static UE determines identifying information of the rogue base station, such as the cell ID, PLMN ID, MCC, MNC, etc. The static UE can send the identifying information along with the static UE's GPS coordinates to the network and law enforcement authorities so that the rogue base station can be located and shut down. The static UE can also share the time plot of signal variations since the peak of the plot indicates the time when the rogue base station was close to the static UE.

In another example, a network-based algorithm or technique can be implanted that configures all base stations to periodically update/send their GPS location to a network server. If one or more network components detect a large change in a base station’s location, this base station is identified as a rogue base station. In some instances, small changes in a base station's location are filtered out to compensate for small cells.

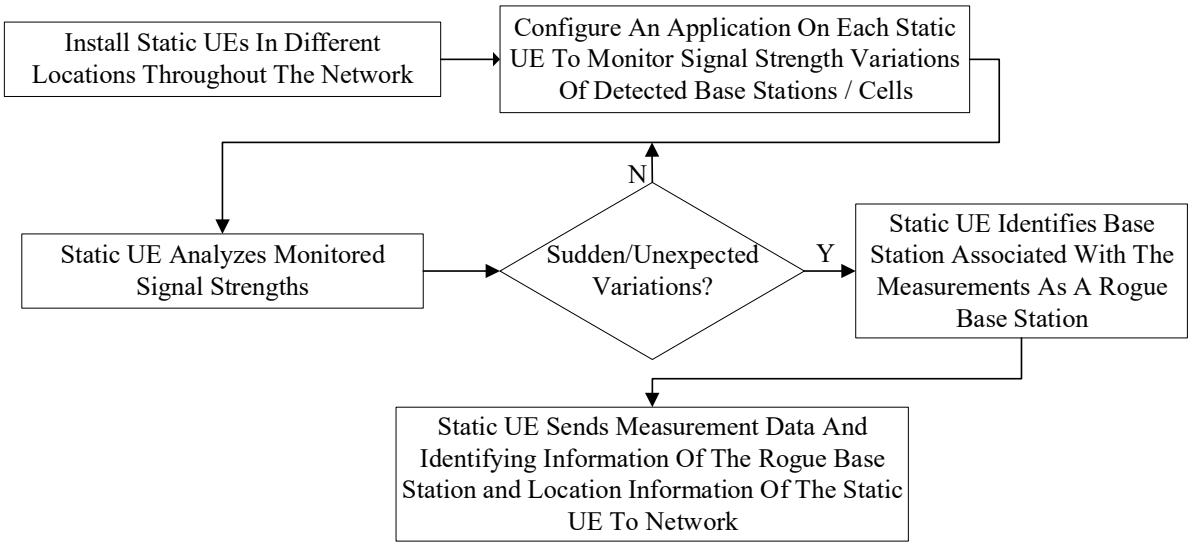

Figure 2

A third approach for detecting and mitigating rogue base stations is shown below in Figure 3. In this approach, network/RAT downgrade attacks are detected and prevented. Networks such as 2G (Second Generation), GSM (Global System for Mobile Communications), and 1x networks are less secure than 4G/5G (Fifth Generation) networks. As such, rogue base stations attempt to push UEs to a lower order RAT. Rogue base stations can typically capture more UE information on a lower order RAT due to its lesser security. For example, a rogue base station can implement multiple RATs such as LTE and 2G RATs. When a UE camps on the rogue base station using the LTE RAT, the rogue base station manipulates the cell reselection parameters (e.g., CellReselectionPriority and reselection thresholds) so that the UE reselects to the 2G RAT of the rogue base station. However, legitimate base stations typically assign higher priority to LTE/5G over 2G. As such, a UE can be configured to detect when the base station reverses priority and instructs the UE to reselect to a lower order RAT.

When the UE detects that the base station is instructing the UE to reselect to a lower order RAT, the UE identifies the base station as a rogue base station, and the UE does not camp on the cell until the

next power cycle. The UE can store its Global Positioning System (GPS) coordinates and information associated with the failed rogue base station, such as the cell ID, EARFCN, and PLMN ID, in a rogue base station list. Therefore, the next time the UE detects a cell, the UE can compare one or more of the GPS coordinates, cell ID, EARFCN, PLMN ID of the cell to corresponding information in the rogue base station list. If matching information is found in the rogue base station list, the UE determines the cell is a rogue base station and does not camp on the cell. The UE can then implement the techniques described above with respect to the first approach.

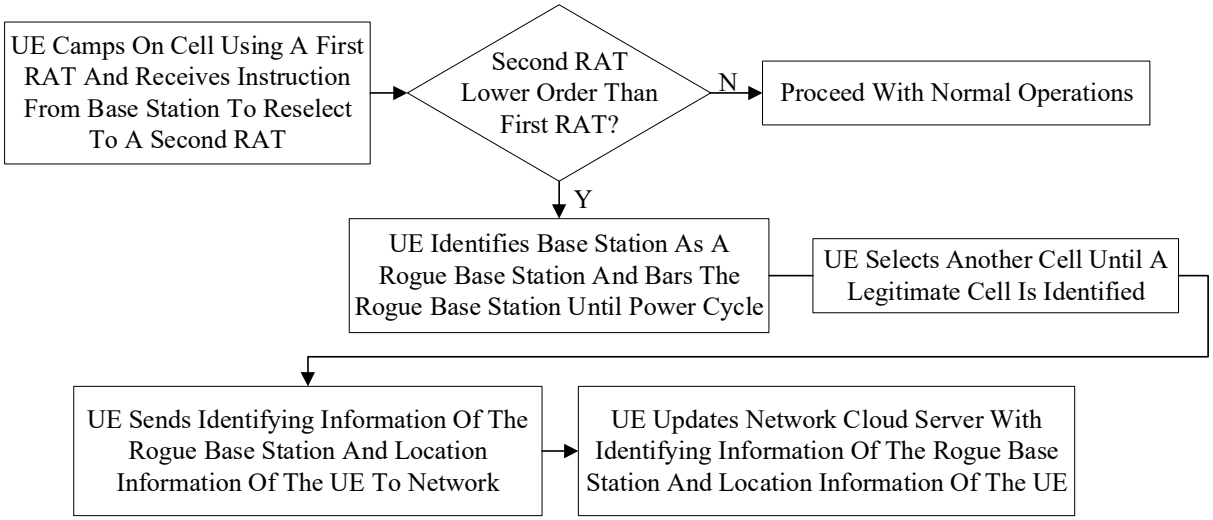

Figure 3

A fourth approach for detecting and mitigating rogue base stations is directed to signal jamming. Some rogue base stations may utilize a jamming mechanism that sends a signal with very high power so that UEs cannot locate legitimate cells. The jamming mechanism intends to obstruct the communications between UEs and the network. Rogue base stations that utilize jamming mechanisms are typically not real base stations but are just signal generators that transmit high power signals in the same frequency spectrum as legitimate base stations. As such, a UE can be configured to detect abnormally high RSSI, which indicates a jamming mechanism is being used on

the band. When the UE detects an abnormally high RSSI, the UE can attempt to find a legitimate cell on the frequency. If the UE cannot find a legitimate cell on the frequency, the UE can move to a different band or different RAT.

Use of the approaches outlined above, individually or in combination, enable network operators to detect rogue base stations and mitigate the security issues caused by the rogue base stations. Eavesdropping by a rogue base station can be reduced, thereby increasing user security and privacy. Modern solutions, such as machine learning and cloud-based services, can provide more robust and foolproof detection mechanisms that are easy to implement on the UE and network.

References:

1. U.S. Patent Application Publication No. 2016/0381545, entitled “System And Method For Faked Base Station Detection”, and filed on June 21, 2016, the entirety of which is incorporated by reference.

2. Chinese Patent Publication No. 105307119, entitled “Pseudo Base Station Positioning Method Based On RSSI Base Station Signal Estimation”, and filed on September 23, 2015, the entirety of which is incorporated by reference.

3. D. Mills, "System Behaviour On Receipt Of An Invalid Message Authentication Code (MAC)," 3GPP TSG SA WG3 Security – S3#11 22-24 February*, 2000 Mainz Germany*, the entirety of which is incorporated by reference.

4. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on 5G Security Enhancement against False Base Stations (Release 16), 3GPP TR 33.809 V0.3.0 (2019-03), the entirety of which is incorporated by reference.