March 2022

DETECTION, PREVENTION AND MITIGATION OF ROGUE BASE STATIONS IN 5G NETWORKS

NIRANJAN M M

DETECTION, PREVENTION AND MITIGATION OF ROGUE BASE STATIONS IN 5G NETWORKS

AUTHOR:
NIRANJAN M M

ABSTRACT

Rogue Base Station (RBS) threat is one of the major threats faced by different access networks. Here, the attackers use RBS to masquerade (mimic) as a legitimate base station to facilitate a Man-in-The-Middle (MiTM) attack between the mobile User Equipment (UE) and the mobile network, to steal user information, tampering the transmitted information, tracking the users, compromising user privacy, introducing DoS on 5G services etc., The techniques herein propose method to enhance the RBS detection techniques and subsequently prevent and mitigate (containment of) the rogues by detaching the UE from the RBSs and subsequently avoid UEs from attaching to earlier identified RBSs. Also, share the RBS information with the other legitimate base stations which are connected to 5G core, so that they avoid UEs connecting to RBS. Further, update the UEs about the list of RBS in the vicinity, so that UEs refrain from attaching or roaming to such RBSs.

DETAILED DESCRIPTION

Rogue Base Station (RBS) threat is one of the major threats faced by different access networks (5G, 4G, 3G, 2G, i.e., RBS threats exist since GSM networks). Here, the attackers use RBS to masquerade (mimic) as a legitimate base station to facilitate a Man-in-The-Middle (MiTM) attack between the mobile User Equipment (UE) and the mobile network, to steal user information, tampering the transmitted information, tracking the users, compromising user privacy, introducing DoS on 5G services etc.,

Typically, RBS may not be connected to the core network, and they mimic the Cell Identifier (CID), frequency of operations, Mobile Country Code (MCC), Mobile Network Code (MNC) etc., of legitimate base stations. For example, most of the published attacks at the 4G RAN layer include RBSs or IMSI catchers to attack IMSIs during the UE's initial attach procedure to the network, or paging attacks using the IMSI paging features.

With 5G security enhancements, attack by IMSI catchers is prevented by using Subscription Concealed Identifier (SUCI) until the device and/or network is authenticated. Only after that Subscribers Permanent Identifier (SUPI) (which includes IMSI and NAI) is disclosed. Despite 5G security enhancements, 5G networks still faces RBS-based threats such as

- Downgrade attacks (as 5G interwork with other access networks viz., 4G/LTE, 3G, 2G with lesser security mechanisms).
- Compromised 5G small cell can act as RBS.
- Exploit lack of gNB authentication in an idle mode to force UE to attach to RBS (in-turn cause DoS attack).

- RBS often transmit much higher power (RSSI) than the legitimate base stations, so that UE may connect to the RBS (because typically UEs are configured to connect to the base station with the strongest signal).

There are techniques which describe methods to detect the RBS in different cellular networks, such as, using UE-assisted and network-assisted RBS detection mechanisms along with radio-reporting analytics, but there are no methods which uses distributed method to detect, prevent and mitigate the RBSs in 5G deployments.

The techniques herein propose method to enhance the RBS detection techniques and subsequently prevent and mitigate (containment of) the rogues by

- Detaching the UE from the RBSs and subsequently avoid UEs from attaching to earlier identified RBSs.
- Share the RBS information with the other legitimate base stations which are connected to 5G core, so that they avoid UEs connecting to RBS.
- Update the UEs about the list of RBS in the vicinity, so that UEs refrain from attaching or roaming to such RBSs.,

In short, this method detects RBSs both at the UE and Base Station level along with preventing UEs from attaching or roaming to already identified RBSs. Also incorporates steps to mitigate RBS using legitimate base stations in 5G network deployments.

I. Detection and Prevention Techniques:

- UE Level RBS Detection and Prevention Techniques:
    - Base Station authentication at UE:
        - 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 code matches, the UE checks the S-criteria for cell selection.
        - If the S-criteria matches, as part of authentication procedure, both UE and the base station will be authenticated.
        - If failed in any of the steps above, UE consider this base station as RBS.
        - UE collects information of the RBS such as Cell ID, EARFCN, PLMN ID and its own location (using GPS coordinates) information.
        - UE stores base station along with location information of the RBS, so that later it does not attach to the already identified RBSs.
        - Upon attachment to the legitimate base station, UE sends information related to RBS to the network (5G core).
        - Later legitimate base stations scrutinise the RBS with base station level rogue detection techniques and once RBS is re-confirmed as rogue, will add the transaction with RBS information to the Hyperledger.
        - UE can also be configured to do base station authentication upon roaming or re-attach procedure especially in an idle mode scenario (as attackers can exploit lack of gNB authentication in an idle mode to force UE to attach to RBS).

- UE refrains from sudden downgrade of Radio Access Technology (RAT):
  - RBS try to do downgrade attack on UE as lower order RATs (4G, 3G, 2G) are having lesser security mechanisms and relatively easy to do attacks such as IMSI attack, paging attack etc.,
  - UE is configured to detect when a base station is attempting to downgrade the UE to a lower order Radio Access Technology (RAT), especially if such base station earlier detected with better RAT. For example: RBS implement multiple RATs (e.g., 5G and 2G). When UE attaches to the RBS using 5G, RBS manipulate the cell re-selection parameters (i.e., CellReselectionPriority, CellReselectionThresholds), so that UE reselects 2G RAT of the RBS.
  - Typically, legitimate base stations assign higher priority to LTE/5G over 2G. Identify such base stations which are trying to reverse the priority and instructing the UE to reselect to a lower order RAT, as RBS.
  - UE collects information of the RBS such as cell ID, EARFCN, PLMN ID and its own location (using GPS coordinates) information.
  - UE stores base station along with location information of RBS, so that later it does not attach to the already identified RBSs.
  - Upon attachment to the legitimate base station, UE sends information related to RBS to the network (5G core).
  - Later legitimate base stations scrutinise the RBS with base station level rogue detection techniques and once RBS is re-confirmed as rogue, will add the transaction with RBS information to the Hyperledger.
- High RSSI detection at UE:
  - UE is configured to determine when a Received Signal Strength Indicator (RSSI) is abnormally high.
  - Consider such base station as RBS, which is trying signal-jamming mechanism to downgrade the service. For example, RBS may send a signal with very high power so that UEs cannot locate legitimate cells (i.e., intended to obstruct the communications between UEs and the network).
  - These RBSs may not be real base stations, but they just signal generators that transmit high power signals in the same frequency spectrum as legitimate base stations.
  - If UE detects an abnormally high RSSI, collects information about RBS and its own location.
  - UE can attempt to find a legitimate cell on the frequency. If UE is not able to find legitimate cell on the frequency, it can move to different band or different RAT as well.
  - Upon attachment to the legitimate base station, UE sends information related to RBS to the network (5G core).

        - Later legitimate base stations scrutinise the RBS with base station level rogue detection techniques and once RBS is re-confirmed as rogue, will add the transaction with RBS information to the Hyperledger.
- Base Station Level RBS Detection and Prevention Techniques:
    - Detecting mobile RBS using legitimate base stations:
        - Legitimate base stations are static in nature and RSSI variations are less. But to capture information about as many UEs as possible, RBS may not be static (i.e., mobile) e.g., installed on the top of the vehicles etc., Hence, wide variations in signal RSRP or RSSI.
        - Base stations can run UE protocol stack (UE simulator) and attaches to nearby cells and monitor the signal strength variations of those cells. Application running on the UE simulator performs statistical analysis (e.g., mean, standard deviation etc.,) of signal characteristics (signal strength) using standard machine learning techniques.
        - If sudden or unexpected variations are detected, the UE simulator can consider it as mobile Rogue Base Station.
        - Along with simulated UEs on the base stations, operators can install static UEs in several locations throughout the network (e.g., operator stores) to detect the RBSs.
        - These UEs determine information about RBS such as cell ID, PLMN ID, MCC, MNC along with its own location (using GPS coordinates) information and send it to the network (5G core).
        - After detection of such rogues, legitimate base stations would add RBS information to the Hyperledger, so that other base stations are aware of such RBSs in the network.
    - Detecting compromised 5G cell:
        - Configure all base stations to periodically update/send their GPS locations as well peak RSSI value to a network server.
        - If there is large change in a base station's location and/or RSSI range is outside the configured threshold value, then we can consider that base station as compromised and hence Rogue Base Station (RBS).

Overall, legitimate base stations would add all the learned RBSs to the Hyperledger (private/permission blockchain), so that all other base stations of 5G network (of a particular area/deployment) will have the list of all RBSs in the network. Subsequently legitimate base stations use different techniques (as mentioned below) to mitigate (containment of) those rogues from affecting the services to the UE.

II. Mitigation Techniques:

- As part of UE attach procedure, legitimate base station can send list of RBSs (aka Blacklist) in the vicinity (based on GPS coordinates) to the UE, so that UE refrain from attaching or roaming to those RBSs even though their RSSI is better. Along with this, UE does base station validation/authentication before attaching to it (as mentioned above in "UE Level RBS Detection techniques") and hence UE can also detect RBS on its own. In short, UE runs multiple methods to detect along with the

ones instructed by base station and hence subsequently avoid attaching to those RBSs.

- As part of UE attach procedure, legitimate base station can also send list of legitimate base stations (aka Whitelist) contains base stations which are actively monitoring/detecting or even mitigating the RBS, so that UE should not flag them as rogue base stations.
- The mitigating techniques include:
    - Base station runs simulated UEs which would try to attach to the detected RBSs, so that it generates flood on the RBS and in-turn avoid UEs to get attached to those RBSs.
    - As part of RBS detection techniques, legitimate base stations roughly know the location of the RBS using GPS coordination and the time plot of signal variation sent by the UE (i.e., peak of the plot indicates the time when the RBS was close to that UE). Using this information about the RBS, legitimate base station increases the RSSI value more than that of RBS, so that UEs would try to disconnect from RBS and attach to the legitimate base stations having better RSSI.
    - If UE is already serviced by one of the legitimate base stations, it refrains from acting on such activities (configured to do so), otherwise it might create flood on the legitimate base station with higher RSSI, where multiple UEs might try to attach.

Figure-1 describe detection, prevention, and mitigation of Rogue Base Stations.

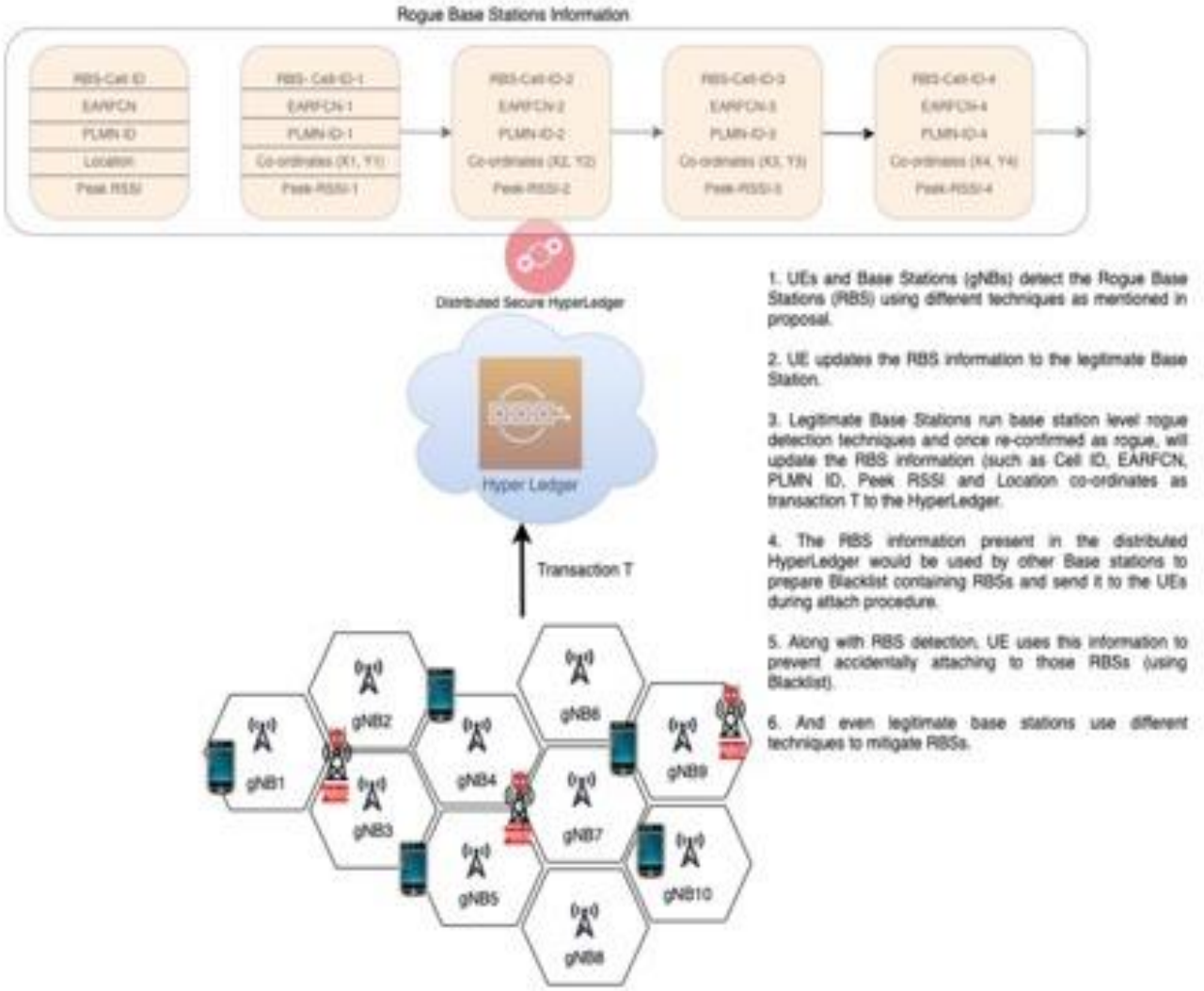

Figure-1

The techniques presented herein define methods to detect rogue base stations in 5G and other access networks along with secure distribution of RBS information across the network via Hyperledger. Moreover, this method helps to prevent UE from attaching to RBSs. Additionally, this method incorporates mitigation techniques to reduce the effect of RBSs on customer (UE) experience.