Detecting false base stations in mobile networks

3GPP standardization takes yet another step to combat false base stations. The security group in 3GPP (called SA3) identified that radio condition information received from devices – which is an integral part of all generations of mobile networks (2G/3G/4G/5G) – could contain fingerprints of false base stations. SA3 has described a solid framework based on this information, enabling mobile networks to reliably detect such false base stations. The framework complements other mechanisms introduced in 5G to protect users against false base stations, for example encrypted long-term identifiers and fresh short-term identifiers. This blog post outlines the framework and describes some practical experiments we have performed in our lab.



JUN 15, 2018 |  6 min.

[](https://www.ericsson.com/en/blog/contributors/m-p/prajwol-kumar-nakarmi)

[Prajwol Kumar Nakarmi](https://www.ericsson.com/en/blog/contributors/m-p/prajwol-kumar-nakarmi)

Senior Specialist RAN Security

[](https://www.ericsson.com/en/blog/contributors/i-l/karl-norrman)

[Karl Norrman](https://www.ericsson.com/en/blog/contributors/i-l/karl-norrman)

CATEGORY

[Research](https://www.ericsson.com/en/tags/category/research) [Security](https://www.ericsson.com/en/tags/category/Security) [5G](https://www.ericsson.com/en/tags/category/5g)

HASHTAGS

[#Falsebasestations](https://www.ericsson.com/en/search?q=Falsebasestations)[#privacy](https://www.ericsson.com/en/search?q=privacy)[#roguebasestations](https://www.ericsson.com/en/search?q=roguebasestations)[#EricssonResearch](https://www.ericsson.com/en/search?q=EricssonResearch)

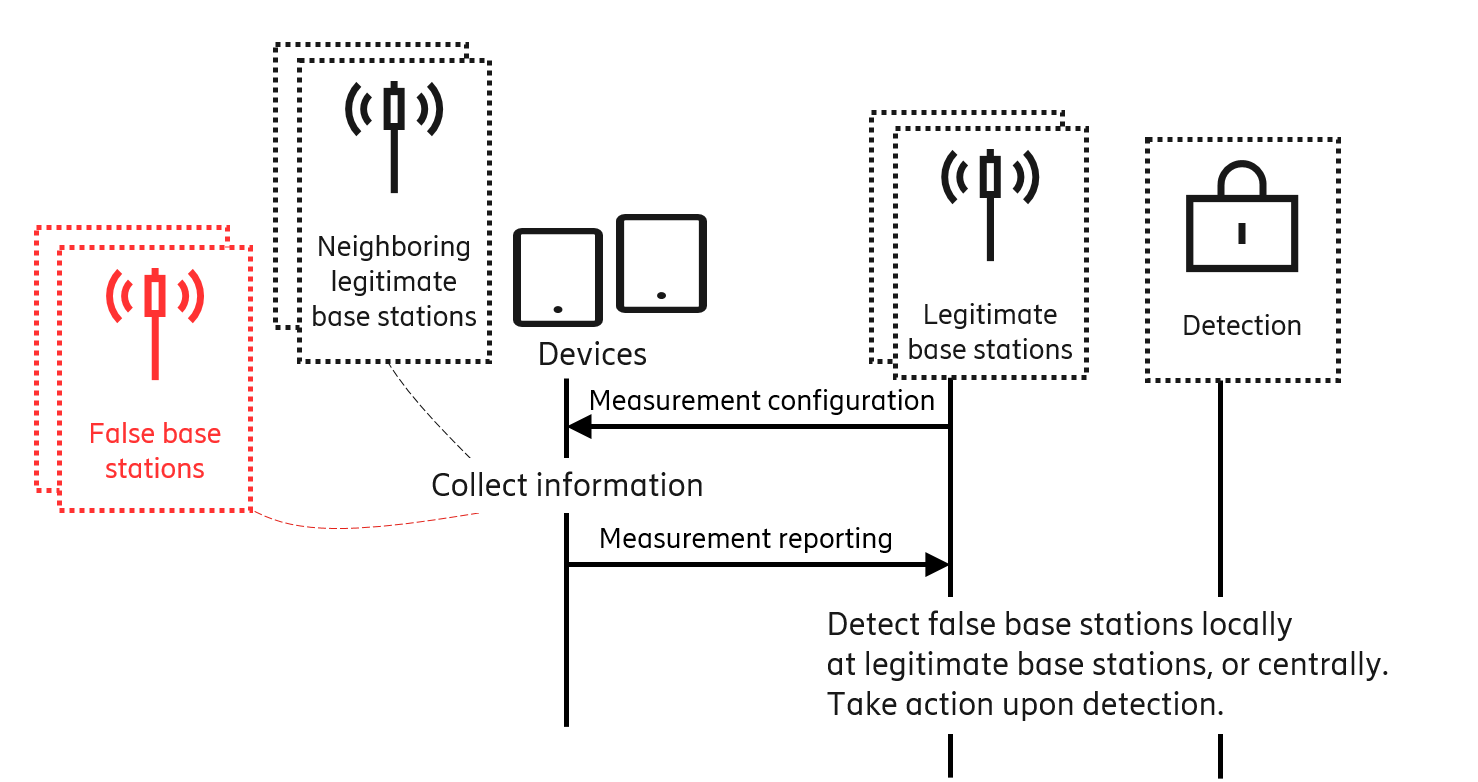
Last year, we wrote the blog post [Protecting 5G against IMSI catchers](https://www.ericsson.com/research-blog/protecting-5g-imsi-catchers/), containing a brief introduction to false base stations or rogue base stations – popularly known as IMSI catchers – and how subscribers' privacy could be enhanced in 5G networks by encrypting the long-term identifier (IMSI). 5G networks are also designed from the start to enforce frequent changes of subscribers’ short-term identifiers (5G-GUTI). These two mechanisms already significantly improve resistance to false base stations in 5G networks compared to earlier generations.

While the two mentioned mechanisms provide preventive measures, this blog post describes a framework for detecting false base stations in mobile networks. We proposed this framework to SA3 during the study phase of 5G security and it is now described in the 5G security specification [3GPP TS 33.501](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169). The framework fits seamlessly into all generations of mobile networks as will be described in the following.

The framework re-uses measurements of the radio environment that the devices report to the network for management of radio links or network topology. Because the data is already present in the network, a mechanism that detects anomalies in the data, indicating the presence of a false base station, can be added on top – without requiring a new measurement machinery being established. A new measurement machinery would require addition of new sensor hardware as the existing hardware is occupied with performing its regular tasks. Thus, the framework fills a current gap in terms of solutions and avoids building a completely separate system. A document from the US Department of Homeland Security, see end of this [AP News article](https://apnews.com/d716aac4ad744b4cae3c6b13dce12d7e), explains their concerns over hardware/software/labor in this matter.

Device-assisted network-based detection

Figure 1 shows a simplified illustration of the detection framework. It is device-assisted because part of information necessary for the detection is collected via devices. It is network-based because the actual detection is done in the network. On a high-level, the framework consists of devices collecting information about their radio environment, which they report to the mobile network for anomaly detection. In more detail, the network configures the device with how to perform measurements – for example which radio frequencies to scan and the periodicity of scans – and which information to collect – say neighboring base station cell identifiers and received-signal strengths. The device collects the requested information and reports it back to the network. The network analyzes the reported information from the configured devices in combination with other relevant information, for instance network cell topology. If anomalies in the reported information indicate that false base stations are, or may be, present in a certain area, further actions can be taken, for example triangulating the indicated false base stations.



Device-assisted part

The device-assisted part of the detection framework uses measurement configuration and measurement reporting procedures. The measurement reports from devices are very effective in detecting false base stations, as will be described later. Because the measurement reports already exist in all generations of mobile networks to manage device mobility, the detection framework fits seamlessly in all mobile network generations.

The framework also exploits the fact that devices can report measurements related to many radio access types. That is, a device could be configured, for example, to report measurements of 2G networks to a 5G network of the same operator. The operator can then implement the framework in the newer generation network and enable it for devices also supporting 2G. Doing so allows detection of 2G false base stations without upgrading the 2G network.

Network-based part

The network-based part performs the data analysis and can be done locally in base stations or centrally. A false base station may evolve and use stealthier techniques over time in order to circumvent detection techniques. Therefore, to be able to quickly adapt to evolving attack methods, 3GPP leaves exact detection techniques to implementations. The framework itself does not pose restrictions to the implementations. In the following, we discuss simple examples of what those implementations could look like in a rule-based system to give a rough idea of how the analysis part of the framework could work. Clearly, more complex analysis methods would increase reliability and detection rate.

The network could detect unexpected radio access types. For example, a network, which has phased out 2G deployments and offers only 3G, 4G and 5G, does not expect to see 2G base stations in measurement reports. Therefore, any 2G base station devices report in its network is a false base station.

The network could also make use of the fact that foreign networks are not allowed to operate in its country. Therefore, any base station broadcasting a foreign mobile country code is also a false base station.

Similarly, deployment information of its legitimate base stations could be utilized by the network to detect inconsistencies in the measurement reports from devices. One example is to detect invalid identifiers broadcasted by false base stations. Another example is to detect false base stations operating in other frequencies than expected. Yet another is to detect invalid neighboring base station information broadcasted by false base stations.

Other behavioral traits of false base stations could also leave their fingerprints. For instance, it is common for false base stations to lure devices by transmitting high power radio signals. Therefore, the network could correlate the received-signal strengths from multiple neighboring base stations reported by devices and potentially identify false base stations.

It is worth repeating that this device-assisted network-based detection framework does not require any special purpose devices or application in devices. The framework is also more reliable than device-only based detection, used by solutions like SnoopSnitch or CryptoPhone. The reliability comes from the fact that while the network knows its own topology, devices or applications in devices do not. Therefore, the risk of false positives is close to nil in some cases – like when identifying invalid radio access types or cell identifiers– and very small in others – like identifying erratic signal strengths.

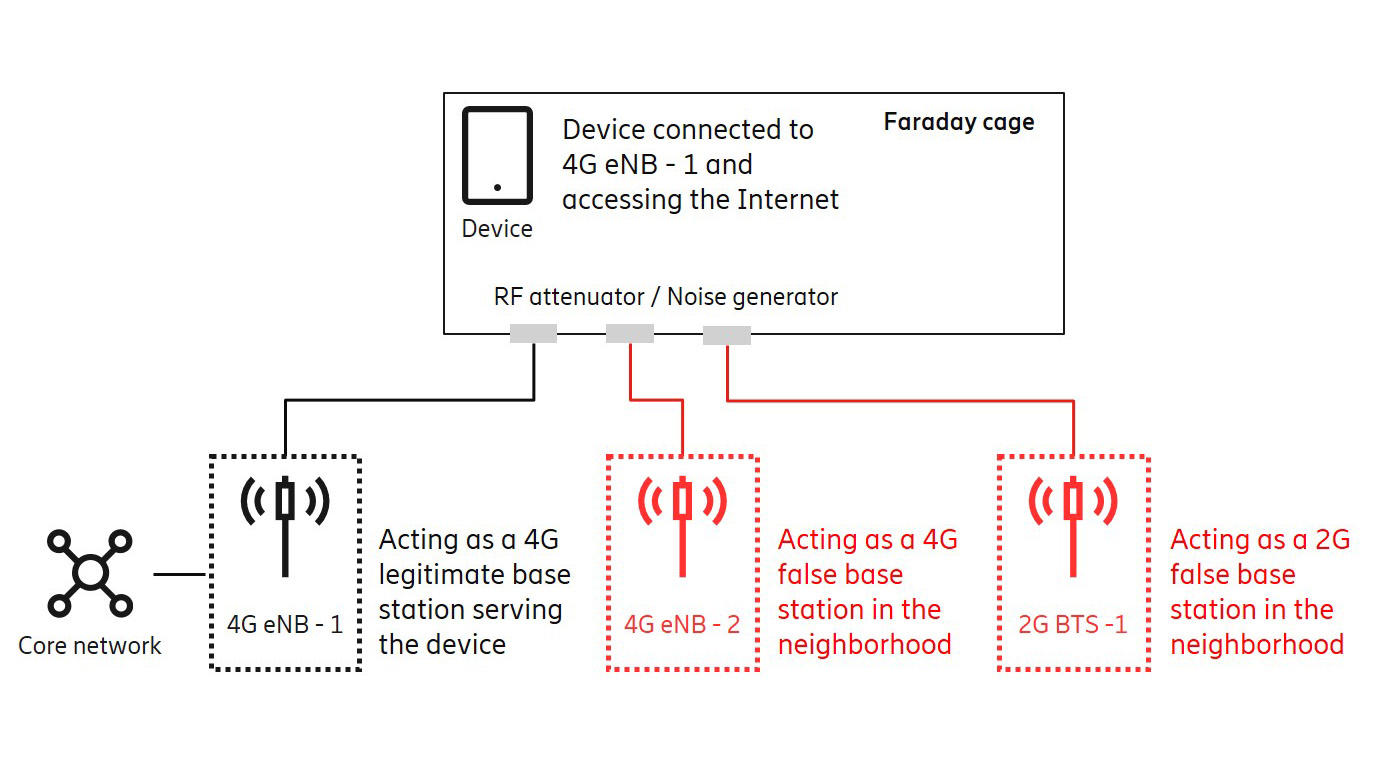
Further, this detection framework offers immense flexibility for the network in choosing how to collect and analyze information. It goes without saying that privacy must be seriously considered right from the start and therefore proper data protection needs to be done at every stage of data collection and data analysis. The starting point for such an analysis is especially good in this case, because subscribers’ long-term identifiers are not present in the base stations for normal operations. Therefore, accidentally linking any collected data to particular subscribers is a priori difficult. Nonetheless, great care must be taken so that privacy problems are not inadvertently introduced. Implementations of this framework must be in compliance with regulations, like GDPR in Europe. Examples of the above-mentioned flexibility are shown in Figure 2. The network could choose to use information for detection only at susceptible locations - like a parliament building (examples reported by [The Washington Times](https://www.washingtontimes.com/news/2018/jun/1/stingray-devices-used-spy-cellphone-activity-disco/), [Aftenposten](https://www.aftenposten.no/norge/i/q36m/Secret-surveillance-of-Norways-leaders-detected), and [CBC News](http://www.cbc.ca/news/politics/imsi-cellphones-spying-ottawa-1.4050049)), certain dates or times, or when detection priority is high for example during high-profile international events.

Figure 2: The network's flexibility in using the framework

Experiments in our lab

We ran some experiments with a 4G setup in one of our test labs, the Smartphone lab, which we will now describe from a rather technical perspective.

The setup, shown in Figure 3, uses base stations of two network generations, 2G base stations called BTS, and 4G base stations called eNB. The purpose is to verify that a 4G network can be used to detect both 4G and 2G false base stations.

Figure 3: Simple experiments setup

In our experiments we used measurement configuration and measurement reporting procedures in 4G radio resource control (RRC) protocol. Figure 4 shows – in a human-readable form –selected parts of measurement reports for the 4G radio access type (EUTRA) and the 2G radio access type (GERAN). Mind that the same device sent measurement reports for both the 4G and 2G radio access types. Interested readers may consult [3GPP TS 36.331](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440) for further technical details, see for example clause 5.5 on Measurements and clause 6.3.5 on Measurement information elements.

Figure 4: Examples of neighboring cells reported by the device in our experiments

Measurement reports received by the network (4G eNB-1 in Figure 3) were collected in log files. These log files were first sanitized by removing all device specific references and then used for analysis. The measurement reports were compared against the network’s cell topology database. We varied the content of the database to simulate various network deployments. For example, when we simulated phased-out 2G deployment in the network by removing all 2G cells from the database, the 2G cell in the measurement reports (see GERAN physCellId in Figure 4) was flagged as a false base station. We also simulated a case when a false base station uses a foreign PLMN ID by first configuring the mobile country code (MCC) of the network to 001. Then, the reported MCC 111 (see GERAN plmn-Identity in Figure 4) was flagged as a false base station. Similarly, we simulated a case when a false base station uses an invalid cell identifier by first removing the cell identifier 204 from the cell topology database. The reported cell with identifier 204 (see EUTRA physCellId in Figure 4) was flagged as a false base station.

The flagged false bases stations were then reported to a demo User Interface (UI) with some counters, list, and a map, see the demo UI in the below photo. In this demo UI, the map showed the false base stations location at the range of the eNB from where the measurement reports were collected.

Road ahead

It is important to continue research on the topic of false base stations or rogue base stations, not only on detection but also on prevention. It is also worth studying how a network's coverage and ability to analyze various other protocol messages can be leveraged, because other protocol messages could also contain fingerprints of false base stations. Examples of this would be implausible jumps of a same device between two distantly separate locations, sudden decrease in radio resource control messages in one legitimate base station without the corresponding increase in neighboring base stations, or suspicious initial registration from already connected devices, to name but a few. Obviously, this is an area where machine learning techniques can prove useful.

Further reading on security in 5G:

* [5G security – enabling a trustworthy 5G system](https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system)
* [5G standardization – Ericsson key contribution areas](https://www.ericsson.com/en/tech-innovation/standardization/5g-standardization)
* [5G open for business](https://www.ericsson.com/en/5g)

Acknowledgement: We thank our colleagues at the Smartphone lab, especially Per Bardun, who were immensely helpful and made our experiments possible. We also thank our colleagues in the *Ericsson Security Manager* development team, especially Antti Jaakkola, who provided us with a demo UI. The top image shows Per in action and Antti with his UI.