COMTECH
LOCATION TECHNOLOGIES

Mobile Location Detection Rules are Changing:

Solution Brief on RF Signature Based Detection and Positioning

May 2020

Knowing the answer to **“where”**

Table of Contents

1. Location & Positioning Introduction

Reliable location information has become a cornerstone of many applications, including emergency services, navigation, commercial services, recreation, tracking and networking. Global Navigation Satellite Systems (GNSS) have emerged as the leading technology to provide location information to these Location-Based Services (LBS), largely because a GNSS receiver provides accurate location--quickly and efficiently--anywhere in the world and in any weather conditions. Improvements in GNSS receiver technology have resulted in very reliable and affordable technology leveraged for a wide range of applications, including mobile devices, resulting in the widespread adoption of consumer applications that rely on LBS.

Although GNSS is known as the cornerstone technology to provide user equipment (UE) location and can be found in every smartphone, it is also known that is does not work well indoors and in dense urban environments. This fact has encouraged the development and use of alternative positioning technologies to ensure accuracy and completeness of coverage.

In addition to GNSS, other positioning methods include Observed Time Difference of Arrival (OTDOA), Cell ID (CID), Enhanced Cell ID (E-CID) and Assisted Global Navigation Satellite System (A-GNSS).

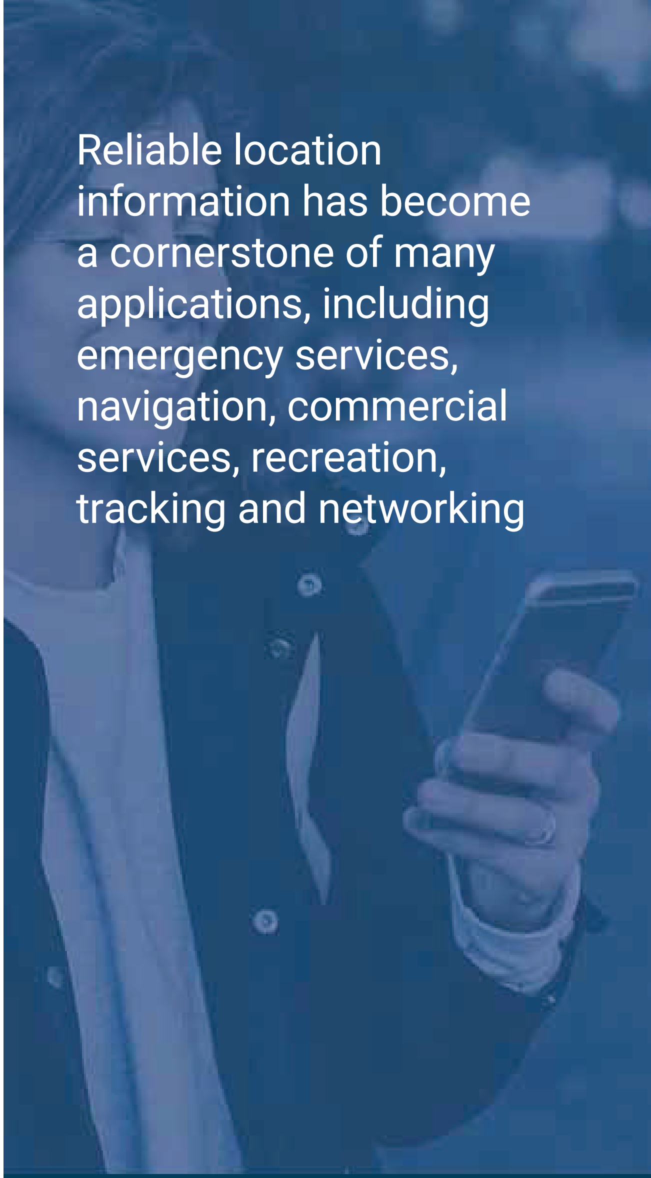
These methods leverage measurements from the UE device, such as Wi-Fi scans, serving cell, neighboring cells and/or other GNSS measurements, to assist in the positioning determination. The actual implementation of the positioning methods relies on two aspects within the radio access network (RAN).

The first aspect is where and how the measurements are obtained for the positioning server to process and calculate the accurate location. This is also known as the Positioning Mode. There are three potential Positioning Modes:

a) UE-Based – The UE performs position measurements as well as position calculation.

b) UE-Assisted – The UE performs position measurements and transfers it to the network, and then the network performs position calculation.

c) Network-based – The network performs position measurements, as well as position calculation.



Reliable location information has become a cornerstone of many applications, including emergency services, navigation, commercial services, recreation, tracking and networking

GNSS receiver provides accurate location--quickly and efficiently-anywhere in the world and in any weather conditions

The second aspect is how and where the measurements are used to determine the positioning of the UE. This is also known as the Positioning Plane. There are three potential Positioning Planes:

a) Control Plane – The network operator is responsible for locating a device using control plane network nodes and protocols.

b) User Plane – The network operator is responsible for locating a device using user plane network nodes and protocols.

c) Data Plane – Also commonly referred to as Over-the-Top (OTT) and still on the User Plane, this method differs in the fact that the network operator is not involved. In this case, a different location service provider is used to identify the positioning of a device using proprietary protocols over a data (TCP/IP) connection.

The decision to use one positioning method over another is determined by the UE technology and the mobile operators' preferences and capabilities.

2. Location Services Requirements

The demand for mobile network operators (MNOs) to accurately locate mobile devices is well documented as a core requirement for two primary purposes:

1. Address government mandates related to law enforcement, emergency response services and security monitoring.

2. Enable delivery of feature-rich solutions for commercial applications such as turn-by-turn navigation, localized advertisements and a variety of IoT solutions in multiple industries, including banking, technology, real estate, healthcare and transportation.

In both cases, the items being located are GNSS-enabled smartphones, tablets and other mobile devices. The sheer volume and variety of these devices drives the need for MNOs to deploy precise location technologies for devices connected to a mobile operator's Radio Access Networks.

> Location services enable delivery of solutions for law enforcement and commercial applications such as turn-by-turn navigation, localized advertisements and a variety of IoT solutions in industries such as banking, technology, real estate, healthcare and transportation.

2.2 Current Location Market Landscape

To support lawful intercept mandates and commercial use cases, the market has demanded a location technology that can accurately determine the position of a mobile device, but completely independent of mobile device capabilities. It is this technology and the associated services that are changing rapidly and will impact the ability of MNOs to offer precise LBS.

Add into the mix the fact that UE manufacturers have taken steps to disable the UE-assisted positioning modes currently available to MNOs, while enabling alternative positioning solutions for non-emergency location applications. Some manufacturers are blocking the data related to local Wi-Fi scans, serving cell, neighboring cells and/or GNSS measurements from MNOs, ensuring only OTT positioning systems are now available for Location-Based Applications (LBA) on the User Equipment.

It is this evolving landscape of technology that has prompted the introduction of Radio Frequency (RF) Signature Processing (RFSP). RSFP caters to the demand for accurate location determination with its ability to precisely locate handsets using network measurements and without a handset's active participation. In this document, we describe the evolving technology of RFSP and the value and application of RFSP within the mobile location systems.

> RSFP caters to the demand for accurate location determination with its ability to precisely locate handsets using network measurements and without a handset's active participation

2.3 Current Location Solutions

Currently there are two standard methods for obtaining location by an application.

The first method relies on an OTT process leveraging the TCP/IP connection to transmit local positioning measurements from the client application to a private server. UE applications with handset-based location, such as client applications for handset-based A-GNSS, are widely used for location-based services.

A-GNSS is highly accurate at identifying location in direct, line-of-sight conditions with the satellites but performs less well in challenging dense urban and indoor environments. A-GNSS is used by wireless network operators for navigation and other location-based services utilizing recognized standards, such as the Secure User Plane Location (SUPL) standard from the Open Mobile Alliance (OMA).

The other method uses 3rd Generation Partnership Project (3GPP) and 3GPP2 standards-based protocols on the wireless service provider's network to offer secure and accurate location services. This is critical for emergency service applications, such as E911, where security and privacy are prime considerations.

With iOS devices, mobile operators cannot initiate a location request to the UE because the iOS operating system does not allow the information to be shared from the device, which typically is requested by the wireless carrier. The only exception to this is when a UE initiates an emergency safety call, e.g., 911, which results in location information being sent to the network to meet mandatory legal requirements.

Android devices are different. Network-initiated requests for local data are allowed and the mobile carrier is able to make a precise location determination. As shown in Figure 1, the UE shares RF environmental measurements with the carrier network to facilitate location calculation.

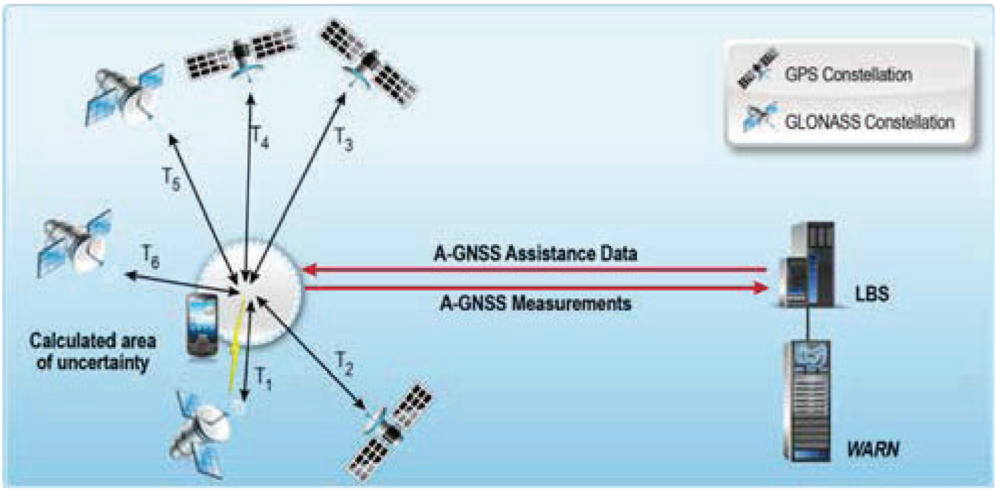


Figure 1. User Equipment providing environmental measurements to enable highly accurate location detection by mobile infrastructure

Recently however, Google changed Android to restrict the sharing of local RF environmental measurements. While older versions of Android may remain unaffected for now, eventually all Android devices will be affected, along with the MNO's ability to position them. This change will potentially impact many wireless services offered by the operator.

2.4 RF Signature Processing (RFSP)

There is, however, a unique solution that can leverage both the security and accuracy of the Control Plane and still be network based.

Radio Frequency Pattern Matching (RFPM) is a general class of positioning techniques by which a set of RF measurements--typically signal strength measurements and timing measurements--are made either by the UE or the RAN. These measurements are compared against a reference set of values in order to estimate the UE location. The reference set of values may be based on predicted and/or collected measurements.

An important aspect of the RFPM technology is that it can be deployed in any RAN network, 2G, 3G, 4G or 5G, while addressing the limitations of other location technologies in deep indoor and dense urban environments.

An important aspect of the RFPM technology is that it addresses the limitations of other location technologies in deep indoor and dense urban environments.

RFPM is available within the standard framework of both the 3GPP control plane as well as OMA SUPL location services architecture.

The Comtech implementation of RFPM industry standard is referred to as RF Signature Processing (RFSP), which offers a high accuracy scalable location solution. RFSP also requires no changes to the UE or the RAN base stations.

RFSP computes a handset's location by using its reported RF signature (that is, ranges to serving-cells and neighbor-cells power-level measurements) in conjunction with a continuously updated High Definition Radio Frequency (HDRF) Footprint Model of the network. Because RF signatures are available on demand from the RAN for any active handset, this technology can be used to locate any class of handsets (smartphones and feature phones) without the handset's direct involvement in the location process. It compares mobile measurements (signal strengths, signal-to-interference ratios, time delays, and so on) against a georeferenced database of the mobile carriers' radio environment.

The HDRF Footprint of the network is built and updated entirely using call trace logs available from the RAN via the Operations Support System (OSS). There is absolutely no need for calibration drives normally associated with traditional implementations of RFPM.

RFSP is ideal for providing location for the growing opportunity in location-based advertising and other location-based services such as mission critical, security and safety applications.

As operators around the world start to make plans to deploy 5G, Comtech will stay ahead of the technology curve and be ready to help operators deploy RFSP solutions for 5G RAN's.

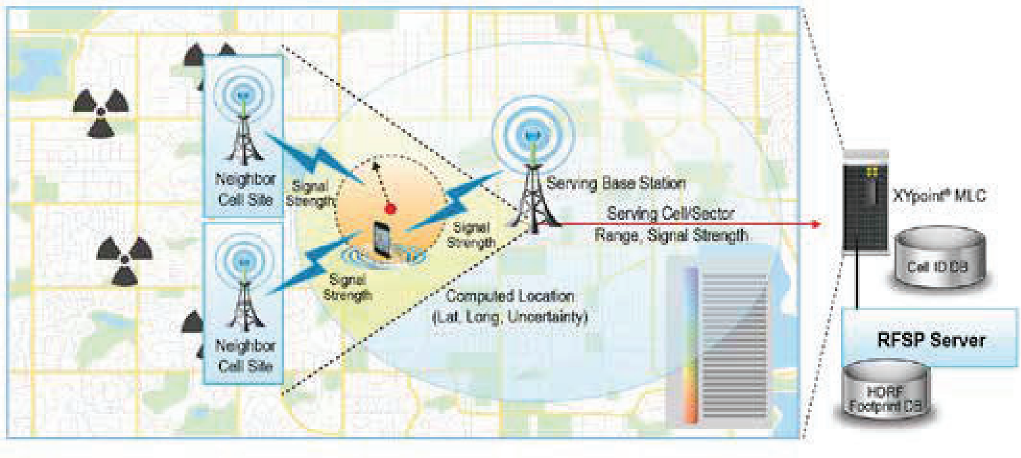


Figure 2. RFSP Deployment Example

- RFSP is ideal for providing location for the growing opportunity in location-based advertising and other locationbased services such as mission critical, security and safety applications.

- Eliminates the need for drive testing.

2.4.1 RF Signatures

A handset's RF signature is the fundamental measurement source on which its location is computed. RF signature refers to a set of measurements made by the handset (and RAN) and is reported to the RAN.

Although used in the location determination procedure, RF signatures are not location-specific measurements. They are made for the normal operation of a handset within a RAN. For example, RF signatures can be used to synchronize transmission time between a handset and a base station, or to implement power control and to coordinate handovers. What is important is that RF signatures are available on demand from the RAN through 3GPP-specified protocols. The contents of the RF signature, however, can vary depending on the type of RAN Access Type (RAT) to which a handset is connected.

In 2G-RAN, the RF signature comprises the following:

- GSM Timing Advance (TA) – Computed by the GERAN, it is the amount of time a mobile is advised to advance its transmission to ensure its signals arrive at the base station on time. TA provides a range of the mobile from the serving Base Transceiver Station (BTS).
- RXLEV – The power level measurements from one or more neighbor cells which are measured by a handset and reported to the GERAN periodically for handover decisions

In 3G-RAN, the RF signature comprises the following:

- Round Trip Time (RTT) – This is the time taken by the Wideband Code Division Multiple Access (WCDMA) reference signal (common pilot channel) to make the round trip from the Node B to the UE and back. It is computed by the Node B.
- Rx-Tx – Measured by the UE; this is the amount of time that a handset waited from the instant when it received the reference signal to when it transmitted it back to the Node B. The RTT and Rx-Tx together provide a range of the UE from the Node B. In soft handover state, a UE may be connected to more than one Node B. In such cases, more than one RTT may be available from the UTRAN.
- Received Signal Code Power (RSCP) – Is a measure of the signal strength made by the UE.
- Common Pilot Channel (CPICH) Ec/No – Is a measure of the signal quality made by the UE.
- Pathloss – Is a signal degradation indicator and is the difference between transmitted and received signal power levels.

In 4G-EUTRAN, the RF signature comprises the following:

- LTE Timing Advance – Provides a range of the mobile from the serving E-Node B.
- Reference Signal Received Power (RSRP)/Reference Signal Received Quality (RSRQ) – Measured by the UE and reported to the E-Node B neighbor cell signal strength measurements.

With the most current 5G Standards release (Release 15) the only measurements available are from LTE. Comtech expects initial 5G network deployments to be tightly coupled with 4G, hence, 4G-LTE-RFSP will be able to support 5G mobile devices, since all 5G mobiles will also have 4G connections. Once Release 16 standards are finalized for 5G, RFSP will be enhanced to include support native 5G network nodes.

The more accurate this model, the greater the accuracy of the computed locations based on that model

The HDRF Footprint Model is built and updated using the RF signatures of all the UE's in the RAN coverage area. These are parsed from the RAN Trace Logs available from the RAN OSS Systems.

During a location determination process, a location platform collects one or more sets of RF signatures from the UE spaced at specific configurable time intervals. RFSP is then invoked with these RF signature measurement sets to estimate location.

2.4.2 High Definition RF Footprint Model

RFSP relies on building and maintaining a High Definition RF (HDRF) Footprint Model. The HDRF Footprint accurately models the RF state of the entire RAN and provides the basis on which location is computed. It consists of the range patterns and power level measurements that may be seen at any given point in the network's coverage area. The more accurate this model, the greater the accuracy of the computed locations based on that model.

The HDRF Footprint Model of the entire network is built and maintained on an ongoing basis independent of any location request that may happen and uses RAN trace logs as the primary source. RAN trace logs are reports of any radio activity by any user connected to that RAN. Examples of RAN trace logs include RRCConnectionRequest, RRCConnectionSetup, RRCMeasurementReport, RRCReconfigurationRequest. Information from these logs is used, along with other inputs such as the Base Station Almanac and Road Vectors, to accurately build and maintain the HDRF Footprint.

RAN trace logs are provided by the Radio Access Networks via their Operations Support System (OSS). An SFTP-based interface is often used, that is, RAN trace logs are periodically batched and transferred via SFTP to a location platform solution.

Depending on the size of the network and the number of subscribers, only a configurable percentage of subscriber activity trace logs are used to build the HDRF Footprint. It is assumed that MNOs will make their RAN OSS interfaces available to the RFSP platform, regardless of the vendor.

2.4.3 High Level RFSP Call Flow

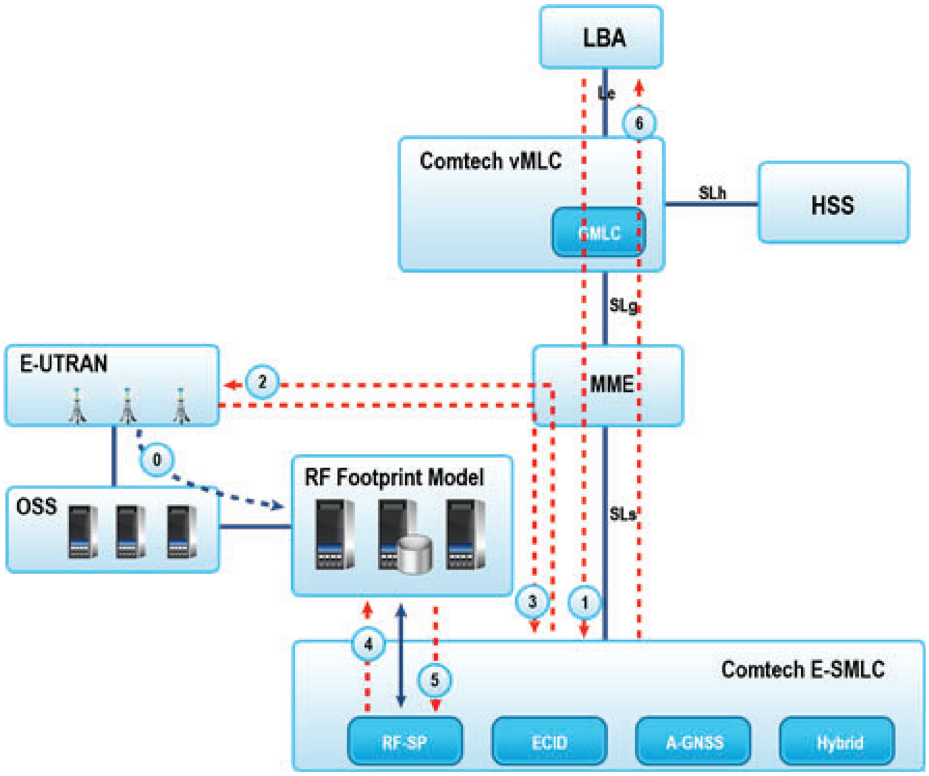


Figure 3. High-Level RFSP Call Flow

The call flow in this section is an example of RFSP as it functions in an LTE Control Plane network to locate a target UE connected to the E-UTRAN. This is an illustrative call flow that highlights the key points. Actual messages and details may vary.

2.4.4 Location Computation Engine

The RFSP location computation engine within the system computes location using the HDRF Footprint Model and the RF signatures.

For each reported RF signature, the range measurement, neighbor cell signal measurement and initial candidate points are all combined using an AI-based model to compute the optimal positioning of the UE.

2.5 RFSP Advantages

RFSP offers a unique ability to offer high accuracy positioning for all applications, independent of the measurements available on the UE.

In addition to offering positioning, RFSP has many other advantages for wireless operators, including:

1. RFSP is secure and precise enough to address government mandates related to law enforcement, emergency response services and security monitoring.
2. RFSP allows MNOs the ability to offer location technologies and solution for commercial applications such as turn-by-turn navigation, localized advertisements and a variety of IoT solutions in several vertical industries including banking, technology, real estate, healthcare and transportation.
3. RFSP can be deployed in any wireless network for locating handsets and other mobile devices connected to generations of Radio Access Networks.
4. RFSP works in conjunction with existing infrastructure without requiring replacement.

3. Conclusion – Comtech's Radio Frequency Signature Processing (RFSP)

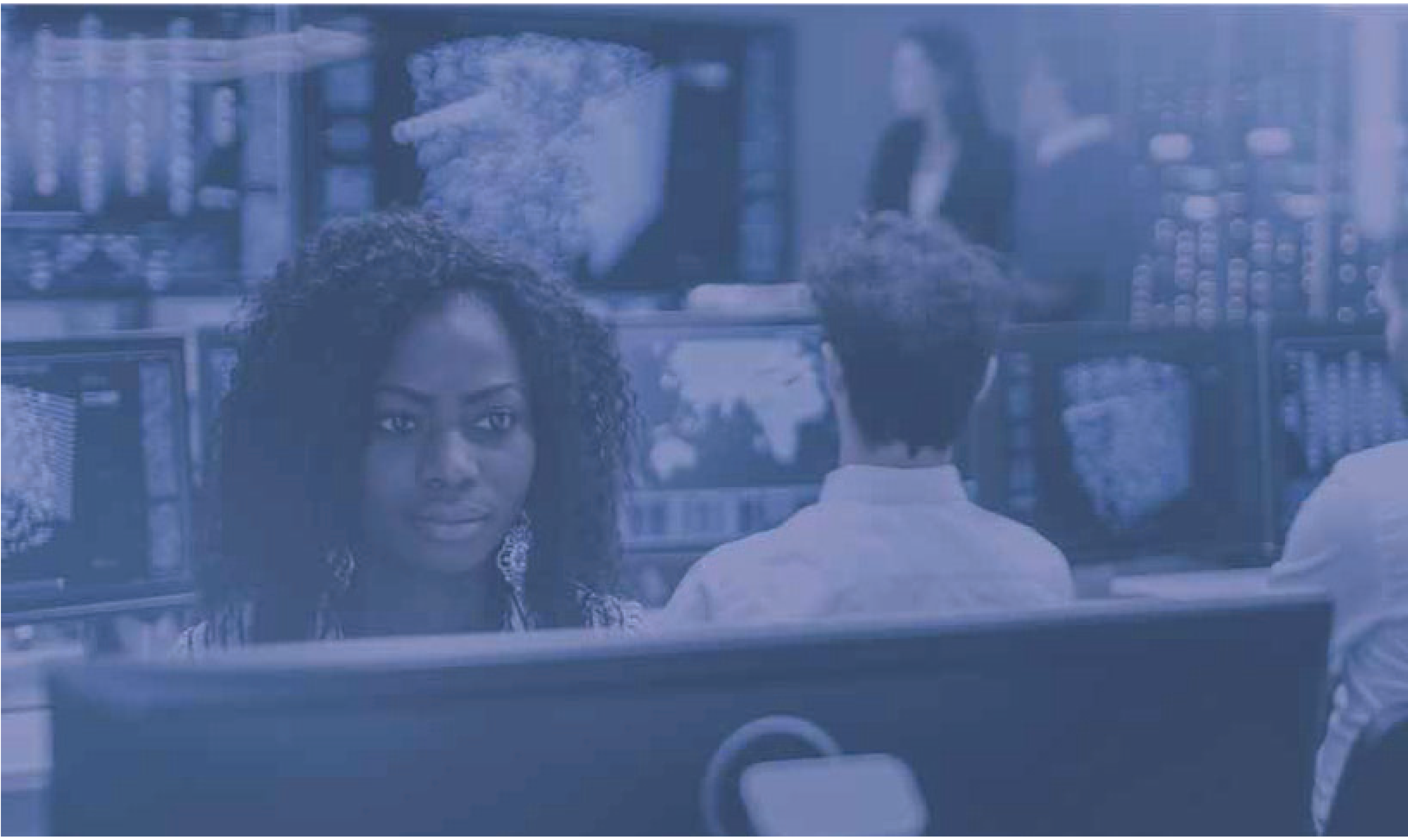
The evolving landscape of location technology is creating challenges for MNOs and complicating their efforts to provide accurate and secure location-based services. To resolve these issues, Comtech created the RF Signature Processing (RFSP) location solution. It is a highly accurate and scalable location solution that requires no changes to the UE or the RAN base stations. The solution is available on Comtech's virtual Mobile Location Center (vMLC) platform and the key characteristics of this precise location technology include:

- RFSP is a highly accurate and scalable location solution that requires no changes to the UE or the RAN base stations

- Can precisely locate any handset

- Able to locate mobile devices connected to 4G-LTE and 5G-NR networks both using standards-based messaging and architecture.
- Available as an option on the 4G-E-SMLC and 5G-LMF per 3GPP Control Plane Location Services (LCS) definition and on the SUPL Location Platform (SLP) in accordance with OMA SUPL 2.0 standards.
- Can precisely locate any handset using measurements procured from the mobile device, whose participation is not required.
- Immune to OEM and OS evolving restrictions to RF environmental measurements.
- Able to locate a handset in environments where A-GNSS either fails or yields poor quality of service (QoS), such as deep indoors or dense urban environments.
- Comtech's RFSP does not require the initial or recurring drive collection requirement to build an accurate RF model of the network.
- Comtech's RFSP builds and maintains the HDRF Footprint Model entirely using online measurements. By doing so, eliminates high CapEx and OpEx costs.
- The core RFSP platform can be extended to many revenue generating applications. Examples include retail, advertising, network optimization, VIP tracking and many more.

Introduced for MNOs as an additional precise location platform solution, RFSP offers precise and secure location while minimizing impact on their existing network infrastructure.



4. Glossary of Terms

The RFSP location computation engine within the system computes location using the HDRF Footprint Model and the RF signatures.

3GPP	3rd Generation Partnership Project
A-GNSS	Assisted - Global Navigation Satellite System
AMPQ	Apache Message Queue Protocol
BTS	Base Transceiver Station
CID	Cell ID
CPICH	Common Pilot Channel
E-CID	Enhanced Cell ID
GERAN	GSM EDGE Radio Access Network
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile Communications
HDRF	High Definition Radio Frequency
IoT	Internet of Things
MNO	Mobile Network Operator
LBA	Location-Based Applications
LBS	Location-Based Services
LCS	Location Services
LTE	Long-Term Evolution
OEM	Original Equipment Manufacturer
OS	Operating System
OSS	Operations Support System
OTDOA	Observed Time Difference of Arrival
OTT	Over-the-Top
QoS	Quality of Service
RAN	Radio Access Network
RAT	RAN Access Type
RF	Radio Frequency
RFPM	Radio Frequency Pattern Matching
RFSP	Radio Frequency Signature Processing
RSCP	Received Signal Code Power
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SFTP	Secure File Transfer Protocol
SLP	SUPL Location Platform
SMLC	Serving Mobile Location Center
SUPL	Secure User Plane Location
TA	Timing Advance
TDOA	Time Difference of Arrival
UE	User Equipment
UTRAN	Universal Terrestrial Radio Access Network
vMLC	Virtual Mobile Location Center
WCDMA	Wideband Code Division Multiple Access

The evolving landscape of location technology is creating challenges for MNOs and complicating their efforts to provide accurate and secure location-based services. To resolve these issues, Comtech created the RF Signature Processing (RFSP) location solution. It is a highly accurate and scalable location solution that requires no changes to the UE or the RAN base stations.

- We know
- the answer
- to “where”

About Us

The Location Technologies group of Comtech Telecommunications Corp. is a leading provider of precise device location, mapping, public safety, and messaging solutions. Sold around the world to mobile network operators, government agencies, and Fortune 150 enterprises, our platforms allow you to locate, map, track, and message.

275 West Street
Annapolis, MD 21401 USA
Toll Free: 1.800.557.5869
Outside US: +1.410.263.7616

www.comtechlocation.com