FrameRF: From SDR Spectrum Monitoring to Behavioral RF Analysis for TSCM

By Stefano Cangiano

Software Defined Radio has significantly changed the way RF environments can be observed and analyzed. Today, relatively compact SDR hardware can provide visibility across a wide range of frequencies and make sophisticated RF analysis accessible outside traditional laboratory environments.

However, during more than ten years working in Technical Surveillance Counter-Measures (TSCM), I repeatedly encountered the same practical problem:

Seeing a signal is not the same as understanding what is happening.

A spectrum analyzer or SDR application can show that RF energy exists at a particular frequency and at a particular moment. For a TSCM operator, however, the important questions usually come afterwards.

What type of activity is this?

Is it expected in this environment?

Is it persistent or intermittent?

Did it appear only after a specific event?

Has its behavior changed?

Does it correspond to a known wireless technology?

And, ultimately, does it deserve further investigation?

FrameRF was developed around these questions.

It is not intended to replace the SDR or the spectrum analyzer. Instead, the SDR provides the RF visibility, while FrameRF attempts to organize that information into a behavioral and operational context that can assist a TSCM investigation.

The SDR as the RF Sensor

At the lowest level, FrameRF begins with SDR-based observation of the radio-frequency environment.

The SDR is essentially the sensor.

Depending on the module and the investigation being performed, RF activity is observed across frequency ranges associated with technologies such as cellular networks, Wi-Fi, Bluetooth/BLE, DECT and conventional radio transmissions.

Traditional spectrum observation is extremely useful. It allows an operator to identify carriers, measure relative signal levels, observe bandwidth and recognize many familiar RF patterns.

But there is an important limitation when the objective is surveillance detection.

A spectrum display primarily answers:

“What is happening right now?”

A TSCM investigation often needs to answer:

“What happened during the last several minutes or hours, and how did that activity behave over time?”

That distinction became one of the fundamental ideas behind FrameRF.

From Spectrum Observation to RF Events

Instead of treating the RF environment exclusively as a continuously changing spectrum display, FrameRF treats relevant observations as events that can be recorded and compared over time.

Conceptually, the process can be represented as:

RF observation → event detection → classification → temporal analysis → behavioral context → operator investigation

Frequency and signal level remain important, but they are only part of the information available to the operator.

Time becomes another important dimension.

For example, consider two signals detected on the same frequency at similar power levels.

One remains continuously present for several hours.

The other appears for approximately thirty seconds, disappears, and returns only when a particular activity occurs inside the monitored environment.

From a conventional spectrum snapshot, the two observations may initially appear similar.

From a behavioral perspective, they are very different.

FrameRF therefore records activity in a way that allows the operator to examine **when a signal appeared, how long it remained active, whether it returned and how its activity relates temporally to other observations**.

This historical component is particularly useful for intermittent transmitters.

Why Intermittent Signals Matter in TSCM

Modern surveillance devices do not necessarily transmit continuously.

A device may remain silent for long periods and communicate only after receiving a command, detecting movement, establishing a network connection or reaching another predefined condition.

This creates a fundamental problem during a conventional sweep.

Imagine a cellular GPS tracker hidden inside a vehicle.

The tracker may contain a GSM/LTE modem but remain largely inactive while the vehicle is stationary. When the ignition is switched on or the vehicle begins moving, the device may register with the cellular network or transmit information.

If the operator examines only a static moment of the RF spectrum while the device is inactive, there may be little to investigate.

The situation changes when RF activity is considered as a timeline.

An operator can observe the environment before the vehicle is started, activate the vehicle and then examine what changed.

The relevant question becomes:

“What RF activity appeared at the same time as this physical event?”

This does not automatically prove that a newly observed transmission belongs to a surveillance device. Correlation is not identification.

But it provides the operator with something extremely valuable: **a reason to investigate a particular event instead of treating every signal in the environment equally.**

Behavioral Analysis Rather Than Automatic Verdicts

This distinction is important.

FrameRF is not designed to declare automatically that every unusual transmission is a bug or surveillance device.

Real RF environments are far too complex for that assumption.

Offices, hotels, vehicles and urban environments may contain dozens or hundreds of legitimate wireless devices. Mobile phones generate background activity. Bluetooth devices advertise periodically. Wi-Fi clients connect and disconnect. Cellular networks continuously change their behavior.

Therefore, an anomaly should be treated as an **investigative indicator**, not as proof of a threat.

FrameRF attempts to reduce the amount of raw RF information that the operator must interpret manually by highlighting behavior that may deserve attention.

The final assessment remains part of the TSCM process.

Different Technologies Require Different Analysis

Another design principle behind FrameRF is that RF activity should not always be interpreted generically.

A cellular transmission does not behave like a Bluetooth Low Energy advertisement.

A DECT device does not behave like a Wi-Fi access point.

A conventional analog RF transmitter presents another completely different situation.

For this reason, FrameRF separates the analysis into technology-oriented modules.

The objective is not simply to create different graphical representations of the same spectrum. Each module attempts to present information that is useful for the particular RF environment being examined.

Cellular

The cellular environment is especially challenging because legitimate activity can be extremely dense.

FrameRF organizes observations according to elements such as technology, frequency range and operator allocations where applicable, while preserving the temporal component of detected activity.

During a TSCM operation, this can help distinguish ordinary persistent cellular activity from events that appear under particular conditions.

Again, the system does not assume that cellular activity equals surveillance.

The purpose is to provide context.

Wi-Fi

Wi-Fi investigations involve more than locating RF energy around 2.4, 5 or 6 GHz.

Access points, clients and their relationships can provide considerably more operational information than a spectrum trace alone.

FrameRF therefore approaches Wi-Fi as an environment of identifiable wireless entities and relationships, allowing the operator to examine infrastructure and client activity rather than simply viewing energy within the Wi-Fi bands.

This becomes useful when investigating unexpected access points, hidden networks or devices whose presence does not correspond to the known infrastructure.

Bluetooth and BLE

Bluetooth Low Energy presents another challenge.

Many modern objects continuously or periodically produce BLE activity: smartphones, wearables, sensors, vehicle components, tracking devices and IoT equipment.

Simply detecting Bluetooth therefore provides very little information by itself.

The useful question is whether a particular device is expected, persistent, newly introduced or behaving differently from the surrounding devices.

Again, **context matters more than detection alone.**

DECT and Conventional RF

Other modules address technologies such as DECT and conventional radio transmissions.

In these cases, frequency knowledge, expected allocations, signal strength and temporal behavior can

be combined to help the operator distinguish normal environmental activity from signals requiring closer inspection.

A strong local transmission appearing where no corresponding legitimate transmitter should exist is very different operationally from a known broadcast signal received at normal levels.

Monitoring Changes the Investigation

One of the concepts I consider particularly important is the difference between performing a short RF sweep and observing an environment over time.

A sweep provides a sample.

Monitoring provides behavior.

FrameRF therefore includes a monitoring approach that allows RF observations to accumulate and subsequently be examined through post-analysis.

This makes it possible to establish what might be considered an operational baseline.

What is normally present?

What appears every few minutes?

What disappears overnight?

What appeared for the first time today?

What happened at 14:32 when a particular event occurred?

These questions are difficult to answer from a single spectrum screenshot.

They become much easier when RF observations are preserved chronologically.

Post-Analysis: Treating RF Activity as a Timeline

The post-analysis component is consequently an important part of the architecture.

Instead of requiring the operator to watch the spectrum continuously and remember every change, FrameRF can preserve relevant observations for later examination.

This changes the operator's relationship with the RF environment.

The spectrum is no longer only something that is watched.

It becomes something that can be **reviewed**.

This is particularly useful when an event is discovered retrospectively.

Suppose an operator notices suspicious activity at a certain time. Rather than attempting to reproduce the event immediately, the operator can return to the corresponding period and examine what RF activity was observed around it.

The timeline can therefore become an investigative tool in its own right.

From Detection to Physical Investigation

Software analysis alone is not the end of a TSCM investigation.

Once FrameRF highlights an RF event or source that deserves further attention, the operator still needs to determine its origin.

This is where conventional field methodology remains essential.

Signal-strength changes, controlled movement through the environment and directional/localization techniques can be used to move from a software observation toward the physical source.

FrameRF includes tools intended to support this stage, but the principle remains deliberately operator-centered:

the software provides evidence and context; the operator performs the investigation.

This is an important distinction because RF environments contain ambiguity.

A tool should help reduce that ambiguity, not hide it behind an automatic red or green indicator.

SDR Hardware and a Modular Approach

Another consequence of this architecture is that FrameRF should not be understood as being defined by one particular SDR receiver.

Different RF tasks have different requirements in terms of frequency coverage, instantaneous bandwidth, sensitivity and acquisition strategy.

The SDR layer can therefore be considered part of a larger modular architecture.

The important element is the separation between **RF acquisition** and **operational interpretation**.

This also reflects one of the reasons SDR technology is so useful for TSCM: the radio hardware can evolve while much of the higher-level analysis methodology remains applicable.

What FrameRF Is — and What It Is Not

Perhaps the easiest way to explain FrameRF is to define the distinction explicitly.

FrameRF is **not intended to replace a professional spectrum analyzer**, and it is not a device that magically identifies every transmitter in an environment.

Spectrum analyzers and SDR applications remain extremely valuable tools, particularly when detailed examination of modulation, bandwidth and signal characteristics is required.

FrameRF addresses another layer of the problem.

It attempts to answer questions such as:

When did this activity begin?

Has it been seen before?

How frequently does it occur?

What technology or RF environment is associated with it?

Did its behavior change when something happened in the physical environment?

Is this observation sufficiently unusual to justify further investigation?

In other words, it attempts to convert part of the RF environment from a collection of instantaneous signals into an **investigative history**.

SDR as a Foundation for Behavioral RF Analysis

Software Defined Radio made FrameRF possible because it provides flexible access to the RF environment.

But the SDR itself is only the beginning of the process.

After years of practical TSCM work, I became increasingly interested not simply in detecting more signals, but in extracting more operational meaning from the signals already visible to us.

That is the idea behind FrameRF.

The SDR provides the RF visibility. FrameRF provides the behavioral context.

And for TSCM, sometimes the most interesting question is not:

“What signal is this?”

but:

“Why did it appear now?”

Author: Stefano Cangiano
TSCM Specialist and developer of FrameRF