Software-defined radios point way for simpler direction finding

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

Advances in hardware and software are making it increasingly practical for open-source analysts to carry out radio direction finding. *Tony Roper* examines the impact the new tool is having on open-source analysis

Key Points

- The development of software to automate the use of time difference of arrival (TDoA) analysis using networked software-defined radios (SDR) is making direction finding (DF) increasingly practical as a tool for open-source analysts.
- DF can be used as another tool for corroboration or to identify previously unknown transmitters, although at present the level of accuracy possible can be limited and is far below the capabilities of governments and militaries.
- The future effectiveness of this technique is likely to be dictated more by the number of SDRs that are available for use around the world than by software or hardware limitations.

Identifying the location of a radio transmitter is a core capability of military and government signals intelligence units. However, open-source analysts have encountered challenges in replicating this capability. Although the relevant physical properties of electromagnetic waves and the mathematical underpinnings of the processes used to identify transmitter sites are well understood, the infrastructure and technology required are beyond the means of most non-government organisations.

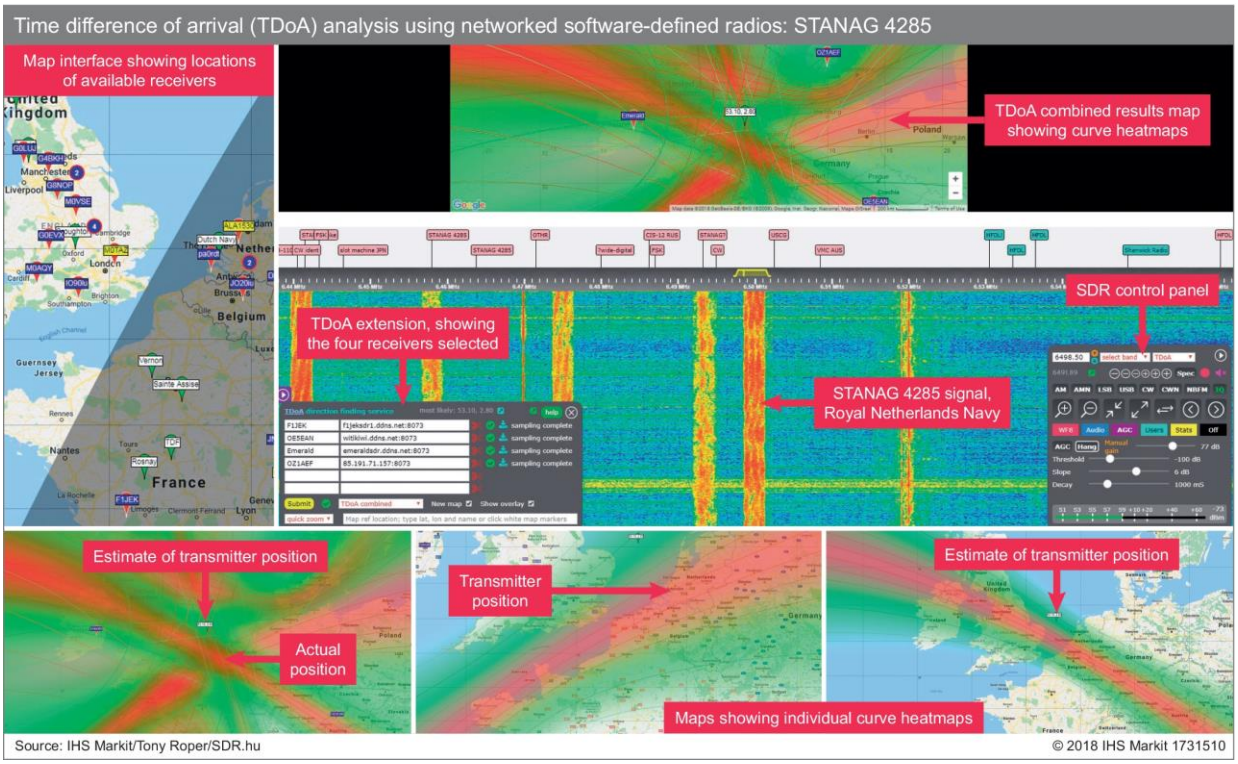
Amateur radio monitors have made use of direction finding (DF) and triangulation methodologies, but the process has traditionally been complicated, involving networks of monitors tuning their radios to the same frequency at the same time and using antennae and other equipment to generate an accurate azimuth bearing on the signal being received. This data would then be centrally collated and plotted to determine a calculated position for the site. Commercial off-the-shelf technology is available, such as the WinRadio WD-3300 DF system. However, this is a high-performance piece of equipment and its cost reflects its intended use by government agencies and militaries.

The development of new software for an existing network of online software-defined radios (SDRs) incorporating global navigation satellite system (GNSS) timestamps has rapidly changed this situation in 2018. It is increasingly practical for an open-source analyst with an internet connection to conduct rudimentary DF.

SDR proliferation

The KiwiSDR is a standalone SDR, priced at under USD300, incorporating the community-supported BeagleBone Black single-board computer. This SDR can be connected to a network and either used privately or shared online. The SDR receives signals in the frequency range of 10 kHz–30 MHz, covering the very low, low, medium and high frequency (VLF/LF/MF/HF) bands. The system also includes a software Global Positioning System (GPS) receiver, which can also receive other GNSS signals, such as the European Galileo system and the Japanese Quasi-Zenith Satellite

System (QZSS). This has two benefits: it enables users to easily share the radio's location and it means the signal data can be timestamped using the GNSS signals.



Time difference of arrival (TDoA) analysis using networked software-defined radios: STANAG 4285 (IHS Markit/Tony Roper/SDR.hu)

1731510

Publicly shared KiwiSDRs can be accessed through an open-source website called SDR.hu (other SDRs that have the capability to be shared online can also be used via this interface). Up to eight users can listen to different frequencies on each KiwiSDR at the same time. SDR.hu features a map-based interface that uses the GPS data to identify the position of the radio. This map and interface is provided by the OpenWebRX Project, created by open-source enthusiast, engineer, and radio amateur, András Retzler. This means that an analyst with an internet connection has access to hundreds of time-stamped SDRs located around the world, making it possible to carry out relatively accurate DF using time difference of arrival (TDoA) methodology.

Bearing down

TDoA measures the time-of-flight differences of a signal received at different locations. The basic principle is that the difference in the arrival time of a signal at two receivers, obtained by cross-correlating the two signals, can be used to calculate a hyperbola of possible locations for the transmitter. Conducting measurements from more than two receivers enables the calculation of multiple hyperbolae, and the point at which these intersect identifies the location of the transmitter. This technique is also known as multilateration (MLAT) and it has been used successfully by aviation enthusiasts to triangulate the position of aircraft that broadcast Automatic Dependent Surveillance-Broadcast (ADS-B) signals without GPS positions, such as military aircraft.

Open-source software needed to carry out the calculations required to conduct TDoA using radio signals is available on software development platform GitHub, including a program written in GNU

octave by physicist Christoph Mayer. Additional software is required to collate the data and plot it visually on maps. In July 2018, John Seamons, the developer of KiwiSDR, incorporated Mayer's program into the KiwiSDR software as an extension.

An analyst can select a frequency of interest and then open the TDoA extension. This brings up the map showing the location of other SDRs. The user can then select up to six SDRs for the calculation, with a minimum requirement of three if a position is to be calculated. If these SDRs have an available channel, and if they are receiving a GNSS signal, they are automatically tuned to the desired frequency. The software then records a sample of the signal from the selected SDRs and carries out the TDoA calculation.

The process takes under a minute to carry out and produces a heatmap showing the calculated hyperbolae. Theoretically, the point at which the curves intersect is where the transmitter site is located. The software also outputs the approximate position of the transmitter, although in cases where there is not a strong fix this information can be less useful for the analyst than the heatmaps of the curves. The process is easily repeatable, enabling the analyst to conduct multiple calculations using SDRs in different locations, with the aim of producing a more accurate fix.

In most case studies conducted by *Jane's* , multiple plots were required to narrow down the area of the transmitter. Moreover, the accuracy of the identification will depend on the frequency of the system. At very low frequencies, such as those in the long wave band, the radio wave follows the curvature of the Earth (the ground wave). In the HF band, as well as the ground wave, the radio waves are also propagated by reflecting off the ionosphere (the sky wave).