Troubleshooting GNSS Timing Problems—Three Unusual Real-World Examples

SyncServer® S600 time server with BlueSky™ technology logs GNSS satellite tracking data and local RF noise to provide a baseline look back in time for alarm correlation.

The most difficult problems to troubleshoot are the ones you cannot see. You cannot see GNSS satellites or local RF interference. Yet the absence of the first and the presence of the second can cause a multitude of problems for GNSS receivers.

Our SyncServer S600 Stratum 1 GNSS-referenced network time server with BlueSky technology enables the viewing and recording of satellite and local RF interference activity at the GNSS antenna. You can correlate the server's alarms to local RF activity to speed up problem identification and ensure a swift resolution.

Our BlueSky technology provides tools to detect, protect and analyze GNSS signals:

- ***Detection*** **involves analyzing the GNSS signals, and the data carried on those signals, for any unintentional or nefarious jamming or spoofing activity that triggers an alarm**
- ***Protection*** **is how the SyncServer time server responds when an event is detected, and what measures it takes to protect the integrity and accuracy of the timing outputs**
- ***Analysis*** **provides the tools to identify what may have happened, and when, to correlate possible local events that triggered the alarm**

Example #1: Is Your Antenna in the Right Location to Track Satellites?

Antenna mounting location significantly influences the ability to track enough GNSS satellites as they transit the sky in their medium Earth orbits. BlueSky technology's *Cumulative Site Survey* (see Chart 1 below) is built over a few days to show satellite coverage. Sometimes called a heat map, this polar plot shows if satellite coverage is relatively uniform around the antenna position, as it should be, or if areas of the sky are blocked. Red sections in the plot indicate where satellites are frequently seen, blue sections indicate where they are rarely seen, and black sections indicate where they are never seen. Chart 1 shows a good antenna location on the left

and a questionable antenna position on the right that could indicate there are not enough satellites to accurately maintain the time.

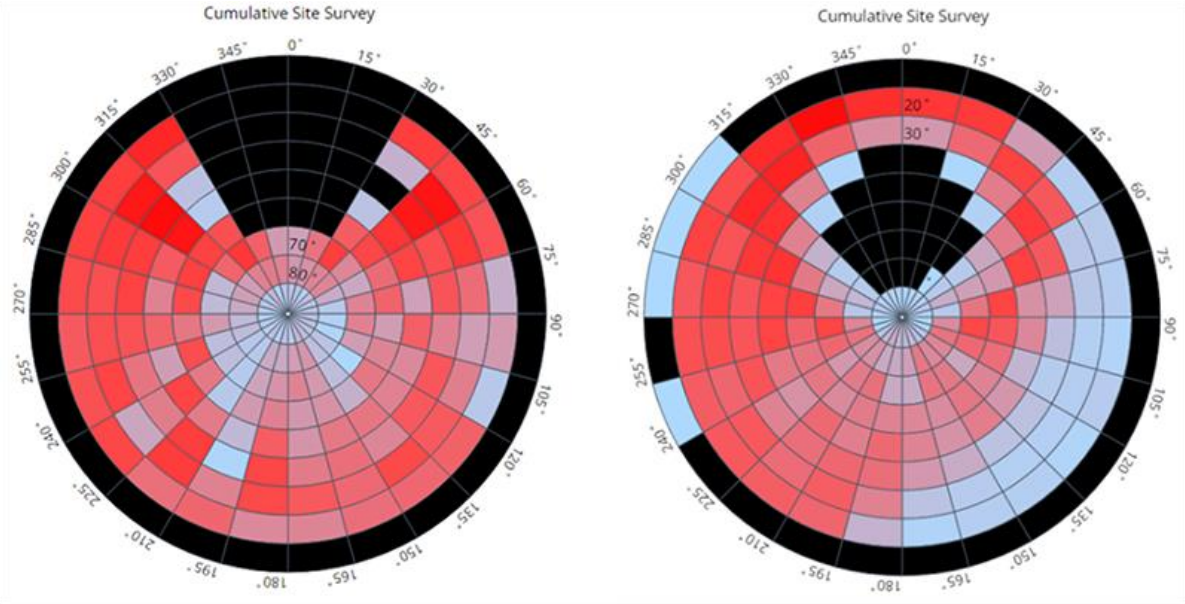

Chart 1: A good antenna location on the left and a questionable antenna location on the right

The antenna on the right is mounted on a balcony railing where both the building and an adjacent hill are blocking satellites toward the east (blue sections). This location is so far north that there are parts of the sky over the North Pole region, as shown in black, where there are no GNSS satellites, ever.

Also, because of the far-northern latitude, all visible satellites will be at low elevation angles. In these types of installations, the best remedy is to mount the antenna on the roof with a better view of the sky, if possible, and simultaneously track multiple GNSS constellations such as GPS, GLONASS and Galileo, to provide more satellites overall from which to compute the accurate time.

Example #2: Can Local RF Interference Jam Satellites?

Many GNSS satellites can be viewed at any given time as they orbit the Earth. Chart 2 below, which is the composite bar chart from our BlueSky technology, displays the number of GPS, Galileo and GLONASS satellites tracked through a window. This chart shows the number of visible satellites in the sky every two hours. But there is more, or you could say less, to this chart than meets the eye.

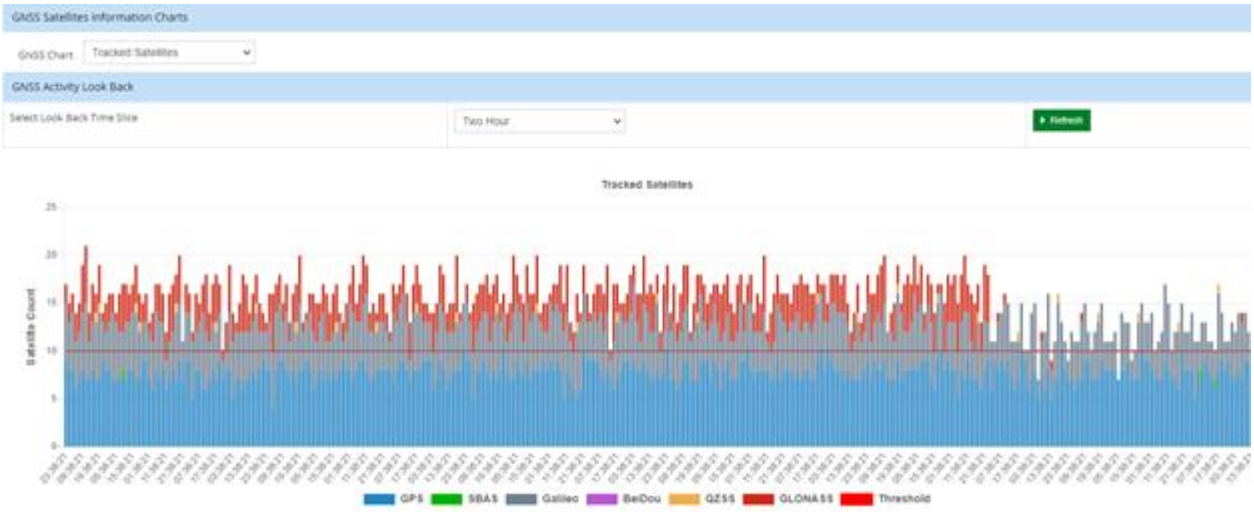

Chart 2: GLONASS satellites being jammed

On closer inspection, you can see that the GLONASS satellites (indicated in red) effectively disappeared for several days, which is represented on the right side of the chart. This drop in satellites immediately triggered an alarm. It is highly unlikely the satellites ceased to broadcast, or merely vanished, so something else must have happened to cause the GNSS receiver to unlock from the GLONASS satellites.

A review of the 30-day log of recorded data revealed exactly when the GLONASS satellite unlock occurred. It was not difficult to correlate the unlock to the switching on of a new cable modem/Wi-Fi® router that was located near the GNSS antenna resting on a nearby windowsill.

The cable modem, with 2 GHz and 5 GHz Wi-Fi speeds, jammed the nearby GNSS receiver by overpowering the GLONASS satellite signals with some sort of RF sideband noise. In this case, local RF interference, rather than a malicious jammer, was responsible for this alarm.

Example #3: Can Periodic Local RF Interference Cause Problems?

Pattern recognition is often a clue to resolving all sorts of network and RF interference problems. The BlueSky technology's *Continuous Wave (CW) Jamming Chart*, shown in Chart 3 below, records the GNSS Automatic Gain Control (AGC) setting of the GNSS receiver. The AGC is a good indicator of how the receiver is compensating for local RF noise. You can observe some sort of cyclical interference in the chart below.

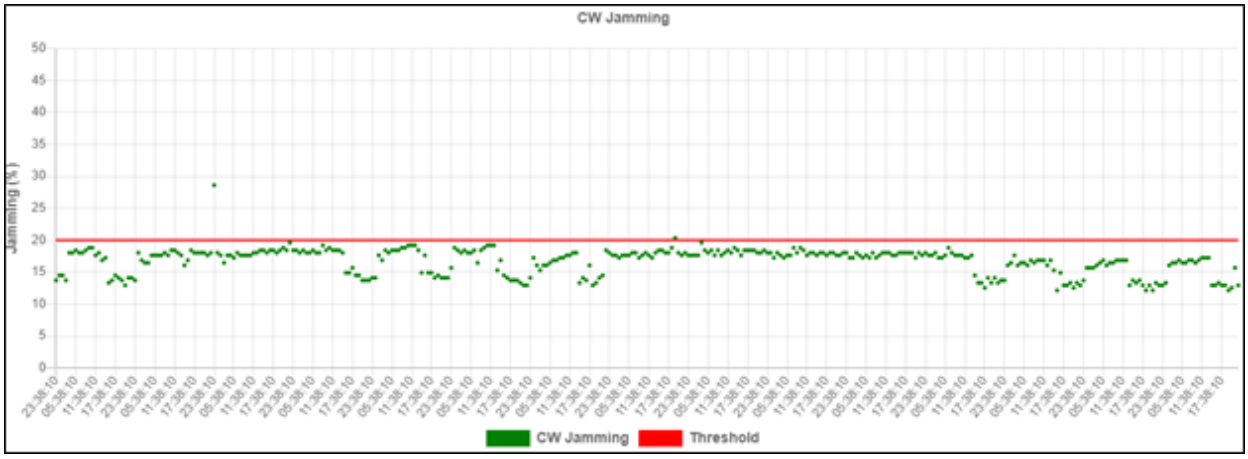

Chart 3. Periodic interference measured by the GNSS receiver

Using the BlueSky technology's historical look back of recorded data, the time slice chart indicates that interference took place when I was in the office where the GNSS antenna was sitting on a nearby windowsill. The GNSS receiver's AGC was adjusting to an increase in RF noise. The culprit was my smartphone.

The chart shows that when I'm in the office during the day, the AGC is adjusted to where CW jamming is below 15%, but on nights and weekends it is above 15%. If the jamming interference was substantially greater from the phone or any jamming device, the GNSS receiver would eventually unlock from tracking satellites, sending alarms as it triggered my alarm limit (20%) and lost satellites.

The takeaway here is that sometimes a user may report frequent GNSS unlock alarms. BlueSky technology's ability to look back in time can help identify if there is a pattern associated with something in the local RF environment.

A famous example of this type of pattern was the daily GPS jamming of the Newark Liberty International Airport. A truck driver, who was trying to hide his location from his employer, was operating a GPS jammer as he drove by the airport.

Protection Comes in Two Very Important Forms: Localization and Response

Localization is the ability to customize the alarm thresholds for your local RF environment. Using the SyncServer time server's BlueSky technology, if you record the local RF observables for a week or two, you can observe some relative maximums or minimums for the normal RF values for your antenna location. Alarm thresholds can then be set according to those levels.

There's no need to be a GNSS expert; just look at the data. In both Charts 2 and 3

above, you can see the red line indicating the alarm thresholds I set by looking at the historical data. In Chart 2, if the total satellite count drops too low, the SyncServer time server will send an alarm. In Chart 3, if the CW jamming interference gets too high, it will send an alarm.

The other aspect of protection is the response to an alarm. The SyncServer time server implementation is very flexible. The response can be to do nothing, which allows you to use BlueSky technology to just monitor the GNSS observables and RF values and inform you if something has happened.

The other choices are to disqualify the GNSS receiver and either fall back to another time source or go into holdover on the installed oscillator. You can also automatically go back to getting time from GNSS if the external alarm condition clears (like when I walked out of the room with my smartphone), or just stay unlocked from GNSS until you choose to manually reenable the GNSS tracking. All the while, BlueSky technology will continue to record GNSS and local RF data.

Key Takeaways

- **The SyncServer time server's BlueSky technology provides the graphical tools to easily characterize the local GNSS environment to set meaningful alarm thresholds and subsequent SyncServer time server behavior.**
- **The charts and graphs provide insights into satellite availability based on antenna location, as well as a historical look back of data that is useful for fine tuning alarm thresholds**
- **The historical data is valuable for identifying when a jamming or spoofing event occurred and possibly correlating it to known changes in the local RF environment**

Intentional GNSS jamming and spoofing are emerging security threats to critical infrastructure and ongoing business operations that rely on accurate timing. The real-time, intelligent RF signal and data analytics provided by the SyncServer time server's BlueSky technology adds the necessary layer of protection to safeguard the integrity of ongoing time and frequency operations.

- **Click here for more information on BlueSky technology inside the SyncServer S600/S650 time server**
- **Click here for more information on the SyncServer S600 time server**
- **Click here for more information on the stand-alone BlueSky GNSS Firewall that provides the same visibility and protection for critical infrastructure with**

embedded GNSS receivers

Paul Skoog, Feb 9, 2022