HOW TO DEFEND AGAINST JAMMING AND SPOOFING AT SEA

THREATS WE FACE

In recent years occurrences of GPS jamming and spoofing have become increasingly common, most notably at sea. In June of 2017 there was a mass spoofing attack in the Black Sea, where over 20 maritime vessels began reporting a position at an inland airport off the Russian coast, over 25 nautical miles from their true location[1]. In November of 2018 the U.S. Maritime Administration issued an expanded advisory for GPS disruptions in the Middle East as multiple reports of GPS jamming were received in the Mediterranean and Red Sea[3]. Most recently in August of 2019 The U.S. Maritime Administration again issued an advisory to ships in the Persian Gulf and Strait of Hormuz after ships began reporting incidents of GPS jamming and spoofing[4]. This recent attack is suspected to be caused by Iran, who aims to seize commercial vessels when they unintentionally enter Iranian waters[4]. Since May of 2019 there have already been 6 attacks against commercial vessels in this region[4]. The threat of GPS jamming and spoofing attacks are real and here today. Most commercial vessels are not currently equipped to combat these threats and the need to protect against them and avoid unwarranted seizures among other issues is more urgent than ever. The following sections explore a product developed by Orolia Defense and Security (Orolia); ThreatBlocker, a cost-effective, easy to integrate and easy to use platform that combats GPS jamming and spoofing threats by utilizing innovative software and hardware to guarantee assured navigation.

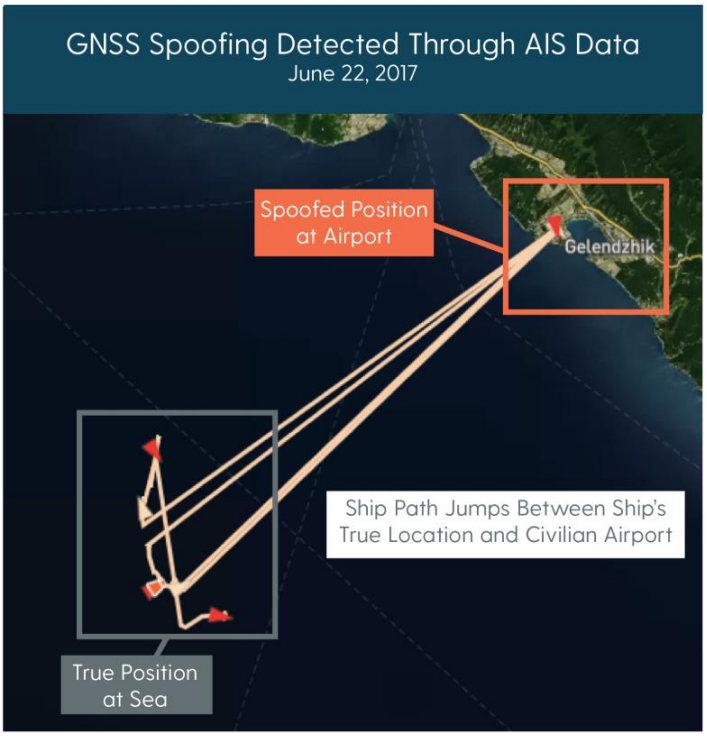

Figure 1: Image depicting the GPS Spoofing attack in the Black Sea[2]

PROTECTED GPS SOLUTION

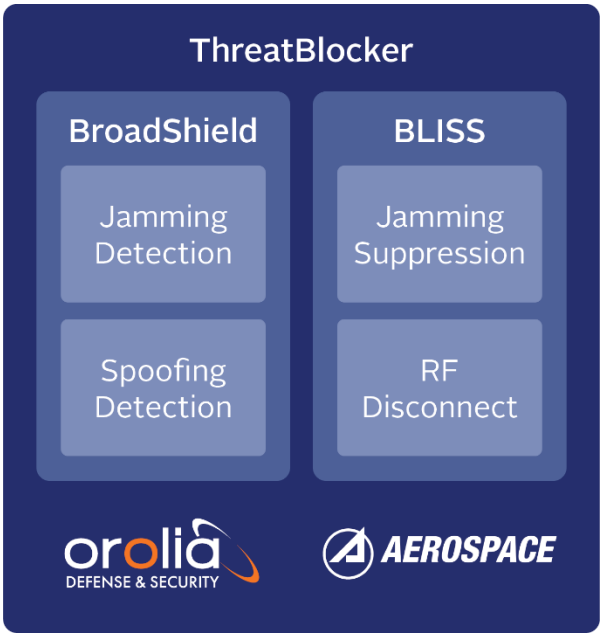

Figure 2: ThreatBlocker High Level Breakdown

Protecting against GPS jamming and spoofing consists of two components, threat detection and threat mitigation. Orolia Defense & Security (ODS) combines these components into a single product, ThreatBlocker. ThreatBlocker leverages ODS's BroadShield and Aerospace's Blind Interference Signal Suppression (BLISS) technologies. BroadShield is an algorithm set that utilizes GPS receiver data to provide GPS jamming and spoofing detection. BLISS is a set of algorithms comprised of digital signal processing (DSP) techniques that are used to mitigate jamming signals. Together they provide a robust solution to protect against threats posed to GPS reliant platforms. A high-level breakdown can be seen in Figure 2. ThreatBlocker is an in-line solution, installed between your existing GPS antenna and GPS receiver. This makes the implementation extremely easy, cost effective and risk adverse. There are no new antennas or receivers to integrate onto the vessel, just place ThreatBlocker in line and you are protected. Featuring a wide range power input of 9-36 VDC and a rugged chassis built to the IP67 environmental rating, ThreatBlocker is ready for integration on many maritime platforms out of the box. Figure 3 shows the default configuration of the device. ThreatBlocker operates on the GPS L1 and L2 frequency bands, the two most common GPS frequencies used for navigation. ThreatBlocker not only detects when jamming is present in the environment but can give accurate jamming to signal ratio (J/S) levels in decibels (dB) for both L1 and L2 frequency bands, providing unparalleled situational awareness. As seen in Figure 2, there is also an RF Disconnect component to ThreatBlocker. You can configure ThreatBlocker such that it cuts off the GPS signals coming from the output when spoofing is detected forcing the vessel to rely on alternate navigation methods such as an inertial navigation system (INS). This prevents the vessel's navigation from becoming corrupted by deceptive GPS signals, which can result in what is seen above in Figure 1. ThreatBlocker contains 8 indicator LEDs on the front panel which gives the user a direct visual indication of detected threats and unit status. From the Ethernet port shown in Figure 3 a WebUI is accessible which gives plots of threat detection and internal receiver

metrics against time, which can be adjusted from 1 hour to 7 days. You can edit system settings, update the firmware and download the data logs from this WebUI. The data logs are human readable .csv files which can be used for post processing. You can connect ThreatBlocker to a network and manage/monitor multiple systems that are setup across a port or on a ship remotely from any machine on that network. ThreatBlocker features a remote API which can be used to send status updates to external systems. This API data can tie into other on-board systems such as warning indicators or alarms that alert the crew of GPS interference.

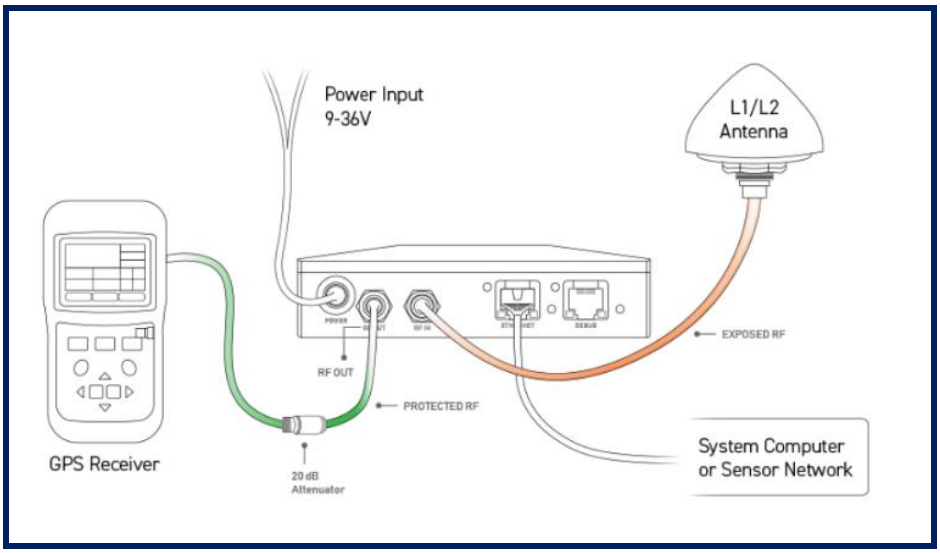

Figure 3: In-Line Configuration of ThreatBlocker

Figure 4: Front View of ThreatBlocker

Figure 5: ThreatBlocker WebUI During a Live Field Test

SPECIFICATIONS

Size	144mm x 164mm x 32mm (WxDxH)
Weight	840 Grams
Power	9-36 VDC
Environmental Rating	Built to meet IP67
Inputs/Outputs	• Power: 2-Pin Locking • RF Input: SMA or TNC • RF Output: SMA or TNC • Data 1 &2: RJ45 Ethernet Jack
L1/L2 Bandwidth	56 MHz

HOW IT WORKS

BroadShield

BroadShield can detect jamming signals and their relative power levels in the environment using only GNSS receivers. This is radically different than typical jamming detection applications which require special hardware or a spectrum analyzer (and often a human in the loop). Jamming detection is done using the information provided through the GNSS receiver's output message set. Orolia has developed, tested and patented algorithms that use this data to determine if interference signals are present in the environment. Since the data used for jamming detecting comes after digitizing the radio frequency (RF) signal, no RF calibration is required nor are there specific limitations as to the type of antenna hardware required*. The jamming detection in BroadShield can be loosely compared to a standard commercial off the shelf (COTS) power meter however, BroadShield requires little to no calibration, offers significantly higher dynamic range and is able to provide a representative spectrum view. These algorithms have been rigorously tested in the lab and in the field for the past 11 years and continue to advance and conform to new and emerging threats.

BroadShield can detect spoofing based on the data that is received and processed by the GNSS receiver. BroadShield is not processing the RF signal or characterizing various RF characteristics, rather it uses the GNSS receiver output data sets to determine if spoofing is present. For this to work properly, the GNSS receivers must be able to track and process the spoofed signals. Algorithms are continuously processing the output data from each receiver and returning a penalty score to the core engine which compares the penalty to a threshold. Once the threshold is reached, spoofing is triggered, and the system is notified.

BLISS

BLISS is a digital processing technique to suppress jamming signals. The BLISS firmware runs on an FPGA embedded into a system-on-a-module (SOM). On the SOM is a processing unit, RF upconverter, RF downconverter, FPGA, and all required filters/time synchronization components. BLISS was designed to specifically mitigate and reduce the interference power passed to downstream receivers for real-world jamming waveforms. BLISS processes the digitized RF environment and suppresses the jamming waveforms with up to 40dB of protection. Since BLISS processes the signals at the digital level, there is no reliance or dependency on antennas or direction at which the signals were received. Figure 6 shows a breakdown of the ThreatBlocker architecture, this serves as a good visual for how the RF signals are handled in the device from input to output.

*may require information related to the gain of the antenna if it is not a standard antenna

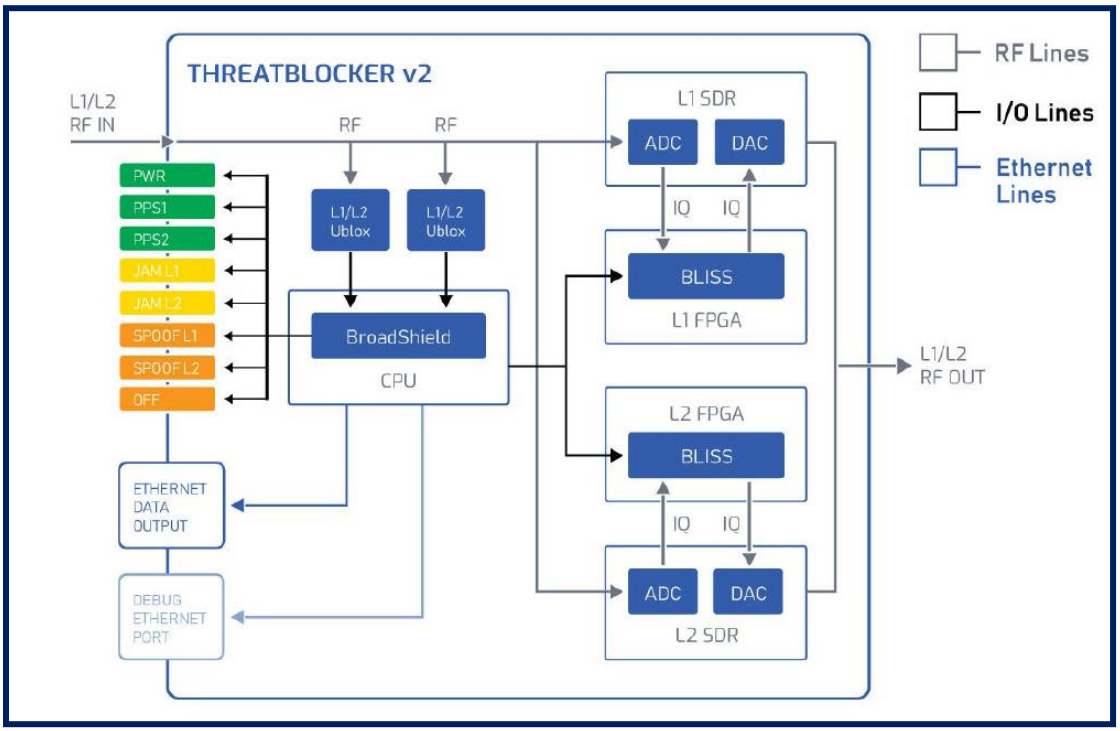

Figure 6: ThreatBlocker Architecture

REAL WORLD TESTING

ThreatBlocker is a relatively new product to hit the market, making its introduction in early 2018, since its inception ThreatBlocker has been tested against various threats at various Over The Air (OTA) government sponsored test events such as the GPS Testing for Critical Infrastructure (GET-CI) among others. Figure 7 illustrates the jamming to signal ratio plotted real time on a mapping software platform. The software components within ThreatBlocker have a much longer history. BroadShield has been tested at similar government sponsored test events dating back to 2008. These tests are designed to emit real-world threat signals that test our systems. We leverage these events to

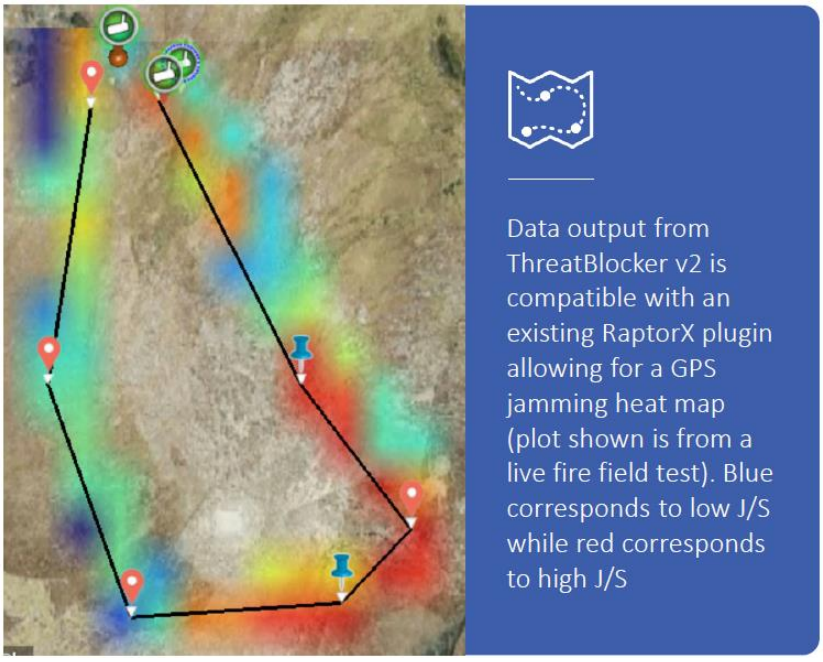

Figure 7: ThreatBlocker Performance Map Overlay at Live Fire Field Test

ensure our algorithms are performing correctly and match what is seen in lab testing. Figure 8 below shows results from an OTA field test in which ThreatBlocker successfully detected and suppressed jamming signals. The vehicle protected with ThreatBlocker was able to navigate for an additional 30km compared to the vehicle without ThreatBlocker.

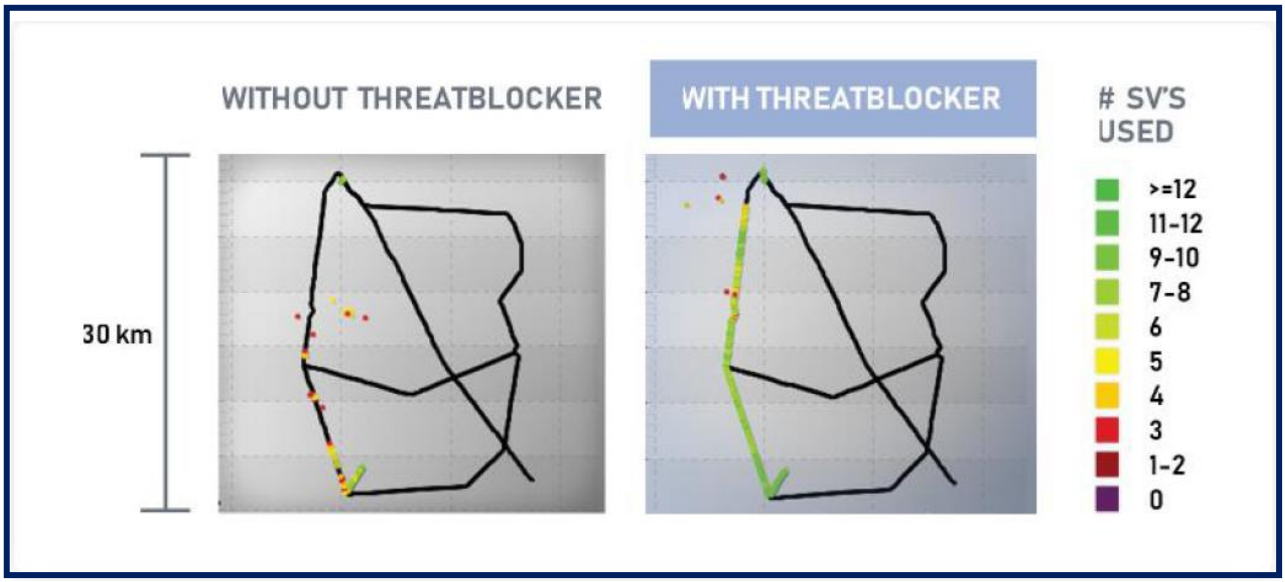

Figure 8: ThreatBlocker Suppression performance at Live Fire Field Test

CONCLUSION

GPS jamming and spoofing attacks are on the rise and have proven to pose a great risk to vessels at sea. Spoofing has caused vessels to report incorrect locations, jamming has caused navigation systems to go down, and the result is vessels drifting into hostile waters unknowingly. These accounts have made it clear that the navigation equipment installed on today's vessels are vulnerable and not equipped to handle todays threats. The technology used to generate jamming and spoofing signals is getting cheaper and easier to acquire, putting GPS reliant systems more at risk than ever before. ThreatBlocker provides a solution to combat and protect against jamming and spoofing attacks. Providing field proven, best in class threat detection and jamming suppression, an easy to integrate form factor and intuitive GUI, ThreatBlocker is a top-notch solution for assured navigation. With ThreatBlocker, you'll have the awareness of when your GPS

systems are being targeted and the tools to protect them. ThreatBlocker is here and available today, ready to defend and protect.

For more information, contact sales@oroliads.com

ENDNOTES

1. https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
2. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf
3. https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/
4. https://www.gpsworld.com/iran-jams-gps-on-ships-in-strait-of-hormuz/