METAMAGNETICS
ADVANCED FERRITE-BASED SOLUTIONS

AUTO-TUNE FILTER™ FOR ADAPTIVE MITIGATION OF GPS THREATS

$30 WORTH OF EQUIPMENT PUTS NATIONAL SECURITY AND A $122B INDUSTRY AT RISK

Background

The reliance on global positioning system (GPS) networks represents one of the greatest national security risks today. A vast number of consumer, industrial, and military devices rely on GPS to provide not only location but, more importantly, synchronization. The backbone of GPS networks is the ability to communicate extremely precise time information (to millionths of a second) worldwide, enabling synchronization. GPS networks act as global timekeepers and have their own time designation called "GPS system time". Cell phone towers, Wi-Fi networks, railroad systems, emergency response units, electrical power grids, traffic signals, and even financial markets all depend on precise time information transferred via GPS. In the United States alone, 3.3 million jobs, currently generating $122.4 billion in annual economic activity, rely on GPS and this reliance is growing steadily with GPS equipment sales, which rose 75% to 122 million units per year from 2005 to 2010.

Figure 1 A commercially available $30 car cigarette lighter plug-in GPS jammer shut down Newark airport in August of 2013. Today, a wide variety of models are available from $30 to $500 and capable of jamming GPS, 4G LTE, WiMax, WiFi, etc. (Figure adapted from cellphonejammeroutlet.com and intelligent-aerospace.com).

The Problem

As dependence on GPS technology grows, so does the risk to national security because current systems are relatively easy to disrupt or deceive. For example, in 2007, downtown San Diego was accidently jammed by a naval training exercise that disrupted GPS systems in the region. This incident caused significant damage, including malfunction of the regional flight tracking and harbor navigation systems, loss of cell phone service, and ATMs to stop dispensing cash. The city was temporarily thrown into a state of chaos. Inexpensive GPS jammers have since become increasingly available in the public marketplace. While the sale and operation of GPS jammers is forbidden by the FCC it is very difficult to prevent these small and inexpensive devices from being imported illegally into the US. In 2013, a New Jersey man, in an attempt to conceal his personal use of a GPS-tracked

480 Neponset Street
Suite 12B
Canton, MA 02021
(781) 562.0756
mtmgx.com

company vehicle, plugged a $30 GPS jammer into the cigarette lighter and drove along an interstate that passed Newark Airport. The jammer interfered with GPS signals reaching the air-traffic control tower, which caused disruption of flight tracking information and activation of backup systems. This event publicized the vulnerability of current GPS systems, how they can be exploited, and why our reliance on these systems is one of the greatest risks to national security. The problem doesn't end there, other forms of wireless communications such as 4G LTE, WiFi, and WiMax networks can all be easily disrupted using low-cost commercial-of-the-shelf equipment.

Our Solution

We have developed an adaptive and highly selective filter technology that mitigates jamming threats. Auto-Tune Filter (ATF) components respond by attenuating high-power in-band interferers while allowing the low power GPS signals to propagate unaltered. The ATF can be easily incorporated into a GPS module behind the antenna and in front of the receiver as shown in figure 2. Signals arriving from the antenna are processed by the receiver that typically contains various fixed filter stages to remove any out-of-band noise and interference and are amplified by the programmable gain amplifier (PGA). The signals are then converted to digital format by the analog-to-digital converter (ADC) and are correlated with known pseudo-random noise code (PRNC) sequences to determine if they are authentic and can be used in the calculation of a navigation solution.

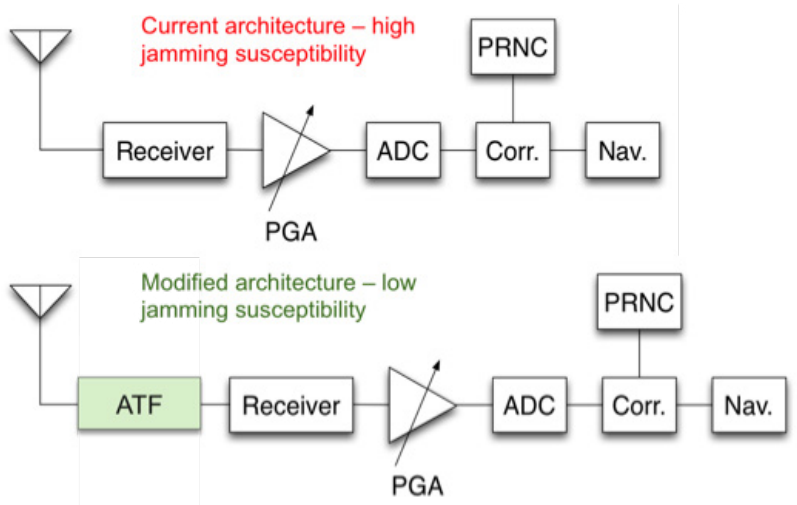

Figure 2 A simplified block diagram of a GPS receiver (Figure adapted from U. Hunkeler et al., "Effectiveness of GPS-jamming and counter-measures," ICL-GNSS 2012). Figure 2 A simplified block diagram of a GPS receiver (Figure adapted from U. Hunkeler et al., "Effectiveness of GPS-jamming and counter-measures," ICL-GNSS 2012).

GPS signals are transmitted from satellites in space and arrive at the Earth surface with a very low power (-166 dBw). GPS receivers are designed to be highly sensitive to detect these signals within background noise and then extract, amplify, decode and process the information they carry to determine position and time. These highly sensitive receivers, ADCs and correlators are very easy to overwhelm using low power and low cost commercially available or easily producible jamming devices that emit signals in the same frequency range as the GPS signals.

The completely passive, low-cost, and compact ATF attenuates all signals that exceed the pre-determined power level of GPS signals. It does so in a highly selective manner, wherein in-band intentional and unintentional jamming signals of different spectral, power, or temporal content are attenuated by >20 dB while the already weak phase modulated GPS signals propagate with relatively low attenuation. Test result data of an ATF in the presence of different types of jammers is shown in figure 3. The significant improvement in jamming resilience is evidenced by the >20 dB increase in the ratio between the received GPS signal power level and that of a jamming signal for

different jamming signal configurations. This power ratio has to remain above a certain level to allow for the reception of the Coarse/Acquisition (C/A) code. In addition to the low cost and passive nature of this approach it can be easily retrofit into existing commercial and military systems as shown schematically in figure 2. It is highly effective against distributed jamming, a situation where multiple low power geographically spread out jammers are utilized to jam GPS systems within a certain area. This approach is also versatile enough to counter a wide variety of jammer threats, as evidenced from the data presented in figure 3.

Jammer Type	Jammer Characteristics	C/A Loss Reduction
CW	Centered on L1	30 dB
FM-CW	df/dt = 100 Hz Period = 10 msec Range = 20 MHz	22 dB
FM-CW AM-CW	df/dt = 75 Hz Period = 13 msec Range = 20 MHz df/dt = 2 Hz Period = 50 msec Range = 20 MHz	22 dB 24 dB
AM-CW BPSK	Centered on L1 Duty Cycle = 1 kHz Modulation = 50%	24 dB 24 dB
BPSK Gaussian noise	1 MHz chip 2 MHz Bandwidth	24 dB 24 dB
Gaussian noise	Centered on L1 2 MHz Bandwidth	24 dB

Figure 3 Measured reduction in jamming effectiveness (as determined by C/A loss) of the ATF in response to a variety of jammer signal types (Figure adapted from R. S. Littlepage, "Impact of interference on civil GPS," Proc. 55th ION Meeting, 1999).

Inexpensive but effective jammers for a variety of wireless communications bands are also available commercially. These devices can disrupt cellphone communications, wireless networks, and a variety of other systems and therefore represent a threat to national security. Our ATF technology is capable of mitigating these threats as well by protecting sensitive radio frequency receivers in wireless communication systems from being overwhelmed by various sources of electromagnetic interference.

Other Solutions

A number of other options are available to counter the GPS jamming threat. Some of these options have to do with improving the entire GPS network by increasing GPS signal levels or developing GPS waveforms that are more difficult to jam. These are major infrastructure improvement projects that are extremely expensive and cannot provide immediate relief of the jamming threat. Certain operational workarounds and supplemental capabilities, such as careful mission planning and training, use of inertial measurement units, as well as maps and compasses can be used to augment the GPS system capabilities in complex or contested environments. A number of companies are offering user equipment improvements to provide a near-term solution to the GPS jamming problem. Antenna arrays with controllable radiation patterns can provide adaptive nulling and beam forming capability to negate certain sources of interference or increase the gain in the direction of a known good source of GPS signals. These approaches are still relatively expensive, require sophisticated hardware and complex software algorithms, are difficult to deploy on certain compact, weight and power sensitive platforms, and are not easily retrofit into existing systems. They are not very effective against a distributed jammer threat because the number of interferers they are capable of negating is limited by the number of antenna elements used in the system. These solutions and workarounds do nevertheless provide a viable solution for many scenarios and applications.

Summary

The Metamagnetics' ATF technology is a low cost, compact, passive, and highly versatile solution to mitigate a variety of jamming threats to GPS and wireless communications system. These components can be retrofit to existing systems and incorporated into new systems being designed today to provide 20 dB or more improvement to the threshold signal to noise ratio required by GPS receiver electronics to acquire and process the signals from satellites. Because this approach doesn't rely on negating specific interferers by varying the GPS antenna radiation pattern it is highly effective against both centralized and distributed jamming in both military and commercial systems. With the abundance of jamming equipment available for sale for as low as $30, the threat to US national security and economy is severe and urgent. Beyond just positioning, the National Institute of Standards and Technologies (NIST) receives over 6 billion requests per day for time synchronization with their atomic clocks. This demand has been growing at a rate of 5% per month for the past 15 years with no indication of decreasing. The majority of these requests are used for synchronizing mainstream consumer devices, which are becoming increasingly abundant and are increasingly relied upon in everyday life. The susceptibility to GPS jamming attacks continues to grow. The technology to effectively counter these attacks is available today.

[1]PR Newswire. "Study Shows Interference with GPS Poses Major Threat to U.S. Economy." June 22, 2011.

[2]Pham, Nam D., "The Economic Benefits of Commercial GPS Use in the U.S. and the Costs of Potential Disruption," NDP Consulting, June 14-15, 2011.

[3]The Science Channel. "How To Collapse A Superpower." Through The Wormhole. June 11th, 2014