Photo courtesy of Pexels

Tackling GNSS interference

Defence forces have become increasingly dependent upon satellite to enhance their operational capabilities in recent decades. From intelligence, surveillance and reconnaissance, through to communications in the field and location services, satellite has become essential for everyday operations. As technologies have advanced and become more widely-accessible and affordable, intentional satellite interference has evolved into a pressing threat.

Satellite interference is both common, and rare. According to Bob Potter at Kratos: "Some 93 percent of communication satellites suffer from interference." However, as emphasized by Martin Jarrold at the GVF: "When you look at the overall amount of satellite traffic going around the world between Earth and space on a day by day basis, only a small fraction is affected by interference."

Most interference is unintentional, and can be attributed to human error; incorrect frequency, poor installation, equipment failure, pointing errors, all contribute to unintentional interference. And while unintentional interference is problematic in itself, and a significant problem within defence forces as education and training budgets are cut, intentional interference is a significant and growing problem today. "We're working in a congested, contested and competitive environment," confirmed Squadron Leader Chris Dunn of the Air Warfare School at RAF Cranwell.

Global navigational satellite services (GNSS) have become ubiquitous in everyday life. Many of us have become used to being able to grab a phone off the table, searching for the nearest Mexican restaurant, and then mapping the fastest route there via car, walking, or local transport. Even 15 years ago, being able to do that would have seemed amazing. GNSS have also become absolutely essential throughout the defence sector, being utilised for various military operations and precision-guided munitions. So, what happens when GNSS malfunction with no warning? For consumers, it's incredibly inconvenient, but for defence forces, it's the difference between operational failure and success; it's literally life and death.

GNSS jamming

A lot of people in the satellite sector dislike the word 'jamming.' They feel it's an inaccurate representation of the situation, and intentionally inflammatory. However, when an agent or entity is intentionally blocking satellite signals, rare as that may be, it's a major problem for everyone involved.

Today, demand for anti-jamming GNSS devices is growing rapidly. GNSS anti-jamming systems detect and cancel the external narrowband noise and jamming signals, and mitigate interference to allow satellite signals to reach the receiver. Until recently, this anti-jamming technology was only feasible for expensive assets such as strategic aircraft and ships, but as size, weight and power (SWaP) improvements have evolved, these devices are becoming increasingly ubiquitous.

Of course, anti-jamming technology isn't the only answer. The satellite sector is well-versed in developing solutions for a whole host of challenges, and interference is one of the big ones. In targeting intentional interference specifically, many people laud high throughout satellites (HTS) as a great stop-gap. The smaller spot beams, in addition to providing enhanced coverage and frequency efficiency compared with traditional satellites, also provide built-in protection by design with low-probability of intercept (LPI) and jamming resilience. Then there's the US Government's Protected Tactical Waveform (PTW), which is designed with frequency-hopping spread spectrum (FHSS) to provide greater anti-jamming capabilities and will be capable of operating over a wide variety of satellite platforms.

The US Government understands GNSS jamming is a

C-COM

SATELLITE SYSTEMS INC.

World's Leading Designer & Manufacturer of Mobile
Auto-Acquire Satellite Antenna Systems

Works Anywhere, Deployed Everywhere

iNetVu®

by C-COM

Reliable • Cost-Effective • Durable

For the most critical communications

Photo courtesy of Pexels

considerable and growing threat. “Our force structure today is built around the assumption that we have GPS and we have satellite communications. We are very lethal when we have those things,” said Colonel Richard Zellmann, Commander of the 1st Space Brigade based in Colorado. “But when you start taking away those combat multipliers, we need to go back then to the days of the industrial-age army where you have to have three times as many people as the adversary does.”

Indeed, the US Government has already begun to place more emphasis on training warfighters in more traditional skills; reading paper maps, navigating by the stars with the help of sextants, and the use of physical map boards to monitor troop locations on the ground. The Defence Advanced Research Projects Agency (DARPA), meanwhile, has announced plans for a new generation of precise navigation and timing tools that work without GPS. Inertial navigation systems, consisting of a series of sensors and gyroscopes, could be used to calculate the location of aircraft and missiles, while ground-based devices known as pseudolites (pseudo-satellites) that beam GPS-like signals, already used in the commercial sector, are another option going forwards.

GPS spoofing

While products capable of resisting jamming and/or delivering alternatives when GNSS is jammed are becoming increasingly advanced, new challenges are arising. Indeed, we’re now looking at an era when GPS-spoofing has become reality.

Jamming GNSS is problematic enough for defence forces; it removes locational capabilities, but it is also easy to detect, and there is usually an alarm in place. Spoofing GPS is a whole different game. “Jamming just causes the receiver to die, spoofing causes the receiver to lie,” commented consultant David Last, former President of the UK’s Royal Institute of Navigation. If you don’t know to look for spoofed GPS, how can you identify it? And even if you are aware of the risk, identifying a spoofed GPS is extremely difficult right now.

June 2017 saw the US Maritime Administration file an incident report wherein a ship near Novorossiysk Port in Russia found that its GPS placed it at Gelendzhik Airport, some 32km inland. After confirming the navigation equipment was working correctly, the ship’s Captain contacted some 20 other nearby ships, who found that their AIS traces placed them all at the same airport.

According to *New Scientist*, while the incident is yet to be confirmed, experts fear it is the first documented case of GPS misdirection.

Todd Humphreys of the University of Texas has reportedly warned of the danger of GPS spoofing for years, and in 2013 demonstrated how a superyacht with state-of-the-art navigation could be lured off-course using GPS spoofing. Commenting on the June 2017 incident, Humphreys stated: “The receiver’s behaviour in the Black Sea incident was much like during the controlled attacks my team conducted.”

Indeed, many experts are debating whether Russia is experimenting with a new type of electronic warfare. In the last 12 months, alleged GPS spoofing has been causing problems for receivers on phone applications in Moscow; a fake signal which allegedly centres on the Kremlin relocates everyone’s GPS signals to Vnukovo Airport, some 32km away. The scale of the problem became apparent when huge numbers of people began playing Pokémon GO, which relies on GPS to operate. Spoofing the Kremlin’s GPS signal, of course, means that would-be attackers would be unable to strike the planned location with anything using GPS navigation; guided bombs, drones, and missiles all rely on the navigational technology.

According to experts in the field, GPS spoofing has become much easier in recent years; a system can be built with commercial hardware and software from the Internet, for a very reasonable price (less than US$300). In addition, the power requirements are extremely low; a 1W transmitter can spoof the GPS of any object within line of sight. Accordingly, GPS spoofing may soon become a significant problem with benign mischief-makers and hostile forces alike getting in on the action.

Methods of detection

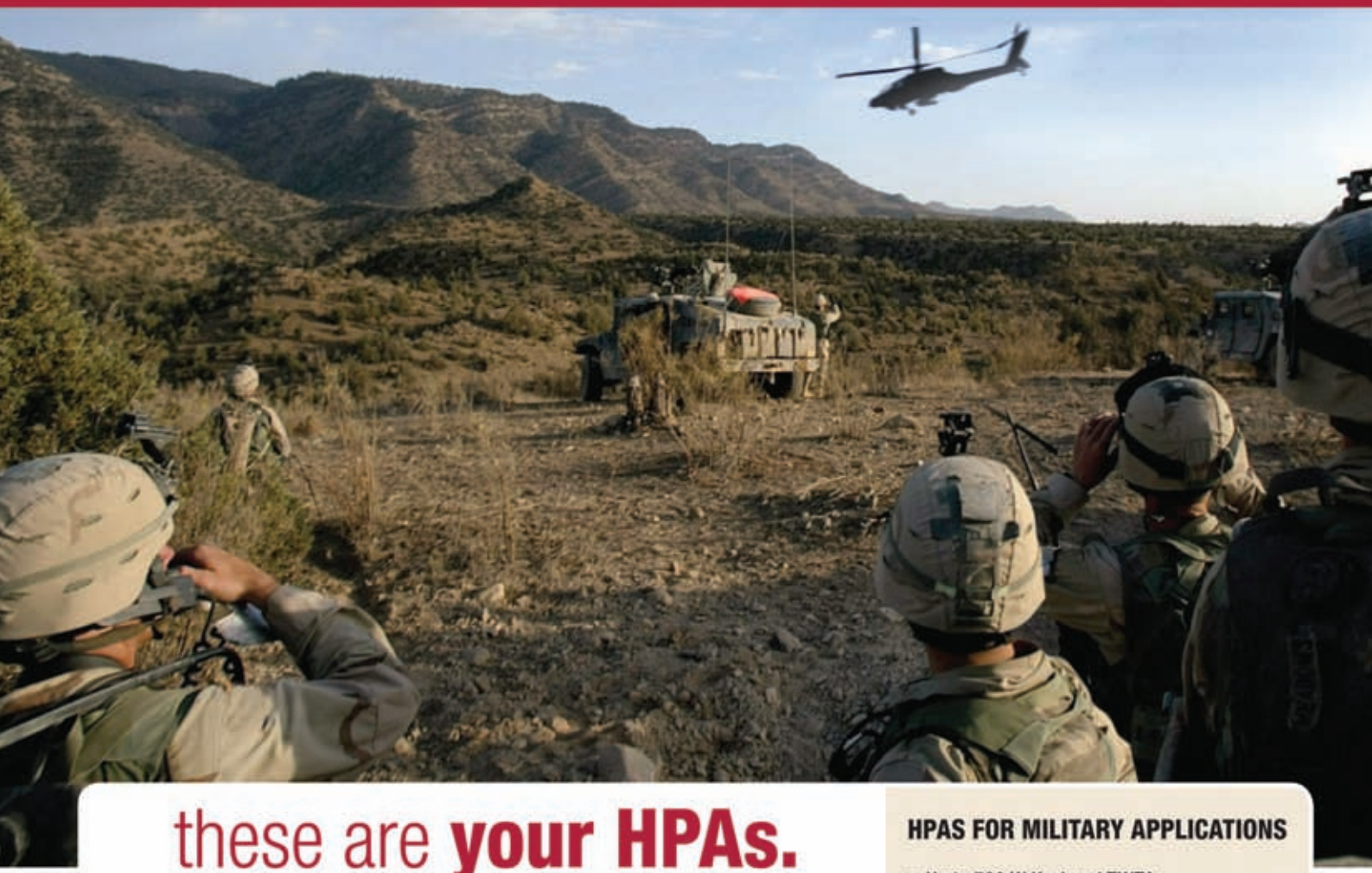
While GPS spoofing is a new and significant threat, there are certainly solutions available, with more under development at academic institutions and within commercial organisations.

In December 2017, Boeing filed a patent incorporating blockchain for an onboard backup and anti-spoofing GPS (OBASG) system that could be utilised if an aircraft’s primary system becomes unreliable or non-functional.

The patent indicates that blockchain data could be used as a back-up record of information if the anti-spoofing system detects a threat. In case location data is spoofed, or else not received, position data can be retrieved from the blockchain storage module.

All the information GPS would normally provide would

If this is **your office...**



these are **your HPAs.**

Superlinear® TWTAs
LEFT: 2.5 kW X-band
CENTER: 750 W Ku-band TWTA

Solid State BUCs
RIGHT: 160 W peak Ka-band GaN BUC

HPAS FOR MILITARY APPLICATIONS

- Up to 700 W Ka-band TWTAs
- SuperLinear® TWTAs in Ku- and Ka-band, delivering 25 to 540 watts of linear power
- C- and Ku-band HPAs for troposcatter applications
- 400 to 750 W C-, X-, and Ku-band indoor and outdoor TWTAs
- 2500 W SuperLinear® and CW X-band TWTAs
- X-, Ka- and Ku-band GaN BUCs

Warfighters shouldn't have to fight against their equipment.

That's why CPI amplifiers feature better efficiency and unmatched reliability even in the harshest of climates, keeping you connected anywhere at any time.

CPI offers:

- Better efficiency
- High reliability
- Rugged designs
- TWT, solid state and klystron technology
- Linearizer, BUC, and integral switch control options
- More than 20 service centers worldwide
- 24/7 technical support

For more information, please visit **www.cpii.com/satcom**, contact your local sales representative, or call us at **+1 (650) 846-3803.**

Download our new app!
Search: CPI Satcom

Download on the App Store

GET IT ON Google Play

CPI
Communications & Power Industries

satcom products

instead be provided by the blockchain, allowing pilots or unmanned aerial systems (UASs) to navigate safely.

Meanwhile, researchers at South Carolina's Clemson University have received US$1 million from the National Science Foundation to fortify computers and devices against cyberattacks associated with timekeeping, with a focus on GPS spoofing.

"The impact of our research will be to make sure the timing service is more reliable," said Yongqiang Wang, an Assistant Professor of Electrical and Computer Engineering at the University. "In a network where time has to be aligned, such as the internet, cellular communication networks, and power systems, if the time on one device goes wrong, then there could be catastrophic consequences. So, we want to provide secure timing solutions, by securing the two most commonly used time distribution approaches, GPS receivers and NTP."

Wang's team plans to counteract GPS spoofing by establishing a server at Clemson University; every 10 seconds, two GPS receivers in Clemson and Anderson will sample secret code embedded in GPS signals and upload them to the server. Users in other locations in the USA will be able to access those samples to verify that the signals they receive are actually coming from the satellite source, rather than a GPS spoofing device.

The researchers will test their project on several battery-powered sensors deployed along the Savannah River to measure flooding and water quality as part of the Intelligent River Project. **GMC**

Photo courtesy of Thales

SpacePath COMMUNICATIONS

Best in class - size, weight and power performance

Outdoor High Power Amplifiers

- 1250W, 750W, 400W, 180W
- C, X, Ku, DBS, Ka, Q & V bands

Indoor Touch Screen Amplifiers

- 1250W, 750W, 400W
- C, X, Ku, DBS & Ka-band
- 1:1 & 1:2 Systems

1.5kW Ku/DBS System

Outdoor HPA Systems

- 1:1, 1:2 Redundant & power combined systems
- Small, lightweight
- Easy maintenance
- Quick Installation

2.5kW Ku/DBS System

Outdoor SSPBs

- Ka-band 10, 20, 40W
- Ku-band 16-200W
- C-band 40-400W

Come see us at:

CommunicAsia
Stand Number: 1W3-03

ib 2018
Stand Number: TBA

Spacepath Communications www.space-path.com / +44 1256 760525