The Next Generation of Secure Position, Navigation and Timing Technology

November 2017

GENERAL DYNAMICS
Mission Systems

Contents

One of the first handheld radios with embedded GPS was the AN/PRC-112, multi-mission radio made by General Dynamics

Executive Summary

It's a modern convenience. And it's so ubiquitous, we take it for granted. Using the nation's global position system or GPS, we expect to be able to navigate our way to new destinations, find the least congested route to work and know exactly what the weather will be at any given time during the day. If the GPS on our devices failed us, we'd be lost, late and thoroughly inconvenienced.

Now imagine if GPS wasn't just about convenience, but about protecting our men and women serving in all branches of the U.S. military and an integral part of their mission success.

GPS on the Battlefield

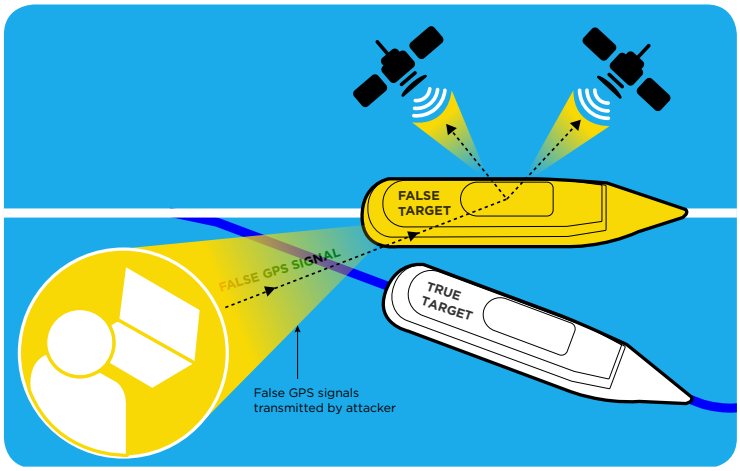
The U.S. military first began launching GPS satellites in the 1970s. It was during the Gulf War in 1991 that the technology proved itself as an invaluable battlefield tool. GPS was instrumental in a successful ground campaign in a terrain that was unfamiliar and provided few identifiable landmarks by which soldiers could base navigation.

Vulnerabilities of GPS

Today, our armed forces use GPS in almost every aspect of their missions, from mapping routes with precision to coordinating operations, to weapons targeting. But, as we've learned with other technologies, dependence can lead to vulnerabilities. And GPS has begun to show its vulnerabilities with the rise of jamming and spoofing tools in the hands of threat actors.

Jamming is the act of blocking or inferring with GPS signals by masking them with what equates to white noise. Jamming is not a new threat and is relatively easy for adversaries to execute. Fortunately, it is also obvious when it occurs so counter measures can be initiated rather quickly.

Spoofing is a newer threat that requires a more technically savvy threat actor but is also more difficult to detect. Spoofing requires that the adversary accurately mimic the GPS signal and give the GPS receiver false location information. And although spoofing is more difficult to achieve, it is an increasing threat due to the availability of commercial hardware and open source software that can be found on the internet.



An attacker can easily send false signals creating a false target.

In fact, earlier this year, there was a report that vessels operating in the Black Sea were receiving erroneous GPS fixes. No cause was identified but the effected ships had to react when they realized their navigation and timing information was wrong.

A 1980's design of a Navstar Satellite.

Staying Ahead of the Threat

Luckily, as threats evolve and new vulnerabilities make themselves known, there are people committed to staying ahead of those who would threaten the missions of our men and women in uniform. And that's where General Dynamics Mission Systems (GDMS) comes in.

General Dynamics has been developing and launching the technology needed for GPS for more than 30 years and has had its equipment aboard every GPS satellite since the 1980s. This wide breadth of experience makes General Dynamics uniquely qualified to deliver the next generation of GPS technology.

Innovating For More Resilient PNT

The Department of Defense is now focused on satisfying the need to provide assured position, navigation and timing (PNT) – or assured PNT – and GDMS is innovating to answer that call by developing new antenna designs, power amplifiers, receivers, waveform generators, and related capabilities that are more resilient to threats.

For example, the jamming threat can be overcome with stronger transmitted signal strength and with receiver antennas that are "smarter" and can differentiate authentic signals from those that are just noise.

Improving the authentication of GPS signal sources and cross-checking those sources to ensure legitimate positioning, navigation and timing information reduces the threat of 'spoof' signals.

One of the challenges with securing GPS is the complex nature of the technology and the ecosystem that supports it. John Liebetreu, Chief Engineer, Space Electronics and Communications for GDMS says that this ability to secure an entire system is what sets GDMS apart. "Resiliency also relies on encryption technologies applied to the GPS signal itself, as well as on communications between satellites and across the entire GPS constellation. This is a core expertise for General Dynamics."

Innovative, Accurate AND Secure

While there is no argument that the security of GPS is paramount, GDMS also believes in the need to continually innovate to make the technology itself better as well as secure.

Sentinel M-code GPS Receiver

"Our innovations in digital technologies also improve the accuracy of information transmitted and received by the satellite and across the constellation," says Liebetreu. "We continue to invest in a wide range of GPS technologies and capabilities to improve the precision of GPS information, while strengthening the system's resiliency."

In 2017, General Dynamics introduced the Sentinel® M-code GPS receiver providing precision positioning, velocity and time information for Low-earth orbit and geostationary Earth orbiting satellites. It is a 64-channel receiver with dual antennas is the only government approved M-code receiver. The Military, or M-code generation of GPS receivers was initiated by the U.S. Air Force as part of its modernization of the GPS Block III satellites.

GDMS manufactures the only government approved M-code receiver.

What's Next

Considering the rising threats, what's the future of GPS and its usage by the military? "We are collaborating closely with U.S. military research organizations and universities to develop promising next generation navigation technologies, like on-orbit reprogrammable digital waveforms," says Liebetreu It's all part of the company's strategy to work alongside thought leaders and customers to forge new paths in technology with the goal of keeping all of us safer.