

1.Executive Summary

Modern Uncrewed Aerial Systems (UAS) technology faces significant challenges in contested environments, including high detectability and low survivability. Hundreds of autonomous systems are lost daily on the modern battlefield, putting operators and missions at risk. Adversaries leverage two primary methods of detection: energy detection, which identifies signals distinct from background noise; and feature detection, which analyzes signal frequency, bandwidth, and modulation to pinpoint targets of interest.

Jamming is the most common attack against a UAS. Autonomous systems are vulnerable to barrage jamming (jamming *any* signal on a common UAS channel) and reactive jamming (targeting a specific UAS signal of interest identified via feature detection). Each type of attack can deny access, degrade trust in the system, and decrease mission effectiveness.

Current state-of-the-art methods used to address adversarial jamming capabilities, like Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), are inadequate for ensuring mission survivability and effectiveness. FHSS, which rapidly changes, or hops, signal frequencies within a certain bandwidth, can be easily overcome by high-bandwidth receivers. DSSS, which spreads signal energy across a certain bandwidth, is vulnerable to cyclostationary attacks and relies on GPS or other positioning, navigation, and timing (PNT).

Rampart Communications, Inc. has developed the StrataWave™ UAS Radio to help the US military and its allies assert UAS dominance in contested environments. The StrataWave™ UAS radio offers Low Probability of Detection (LPD) and anti-jamming capabilities, GPS /PNT independence, and requires minimal size, weight, and power (SWaP) constraints compared to other current state-of-the-art technologies. Increase the survivability and effectiveness of your UAS capabilities in denied, defended, and contested environments, and secure your battlefield advantage with Rampart's StrataWave™ UAS Radio.

2.The Current UAS Threat Landscape

Current commercial and defense UAS radio manufacturers are producing state-of-the-art solutions that are easily disabled by adversaries' increasing Electronic Warfare (EW) capabilities. Until now, no technological advancements have comprehensively addressed the known and weaponized vulnerabilities of UASs, and in many cases the defenses impose compromises in capability.

In the ongoing Russia-Ukraine war, EW is ubiquitous on the battlefield. Russia's advantages in troop numbers, ammunition supplies, and mass-produced UASs are enhanced by company-echelon EW equipment that continues to thwart Ukraine's UAS capabilities. Russia's EW strains Ukraine's limited inventory of UASs and hinders battlefield tactics. While Russia's EW operations are still the subject of intense study, what is clear is that they are able to interfere with Ukrainian drones without impacting their own—a challenge Ukraine has not yet overcome.

Without true innovation, the US and allied autonomous systems will continue to be detected and disabled, putting their operators and missions at risk. To be detected, is to be targeted, is to be killed.

Detectability

In Radio Frequency (RF) communications, signals emit energy and other quantifiable attributes, called "features," such as center frequency, bandwidth, and modulation type. Signal detection thus requires two interdependent technical processes: energy detection and feature detection.

Energy detection is the ability to distinguish a signal from background energy. This ability depends on three factors: the sensitivity of detection equipment; the intensity of energy in the signal; and the intensity of background energy. Because an adversary can always improve equipment sensitivity, and background energy is an environmental constraint, reducing signal power is the only adjustment in the control of the UAS operator.

Modern approaches attempt to reduce energy detectability by lowering the total signal energy output. However, this trade-off results in a reduced operational range, limiting the system's versatility for diverse missions. Additionally, signal detection is contingent upon an adversary being within transmission range, which places the burden of assessing threat proximity on the end user. Consequently, these limitations highlight the need for

alternative methods that do not compromise range or rely on user-based threat assessment.

Feature detection is the act of distinguishing between a signal and the background environment using patterns or structures within the signal or patterns present upon manipulation of an observation of the RF environment. While more complex than energy detection, feature detection techniques are now widely accessible.

Existing state-of-the-art waveforms produce numerous detectable features, and with analysis, adversaries can determine the existence of human-made signals within background energy. These features, once detected, leave UAS systems vulnerable to jamming, intercept, and other types of attacks.

Barrage Jamming

Barrage Jamming, also known as “blind” jamming, increases the noise level at a receiver, preventing it from receiving any signals. This method does not require specific targeting; an adversary can jam a common UAS channel, effectively blocking communication in that channel, without knowing if signals of interest are present. Although historically resource intensive, technological advancements have made barrage jamming easier and cheaper. Portable and readily available barrage jammers make this attack easier than ever to implement.

Smart Jamming

Smart jamming is one of the best-known types of EW attack and involves an adversary transmitting a jamming signal that exploits the features or structures of a target waveform. This attack requires both detection and analysis to identify the vulnerable features. Smart jamming is far more effective against targeted features and requires less power, making it more portable. Examples include jamming UAS control channels, matched modulation jamming, and vendor-specific jammers. Smart jamming prevents communication with a UAS, often resulting in its loss in adversarial territory and contested environments. One report claims Ukraine loses around 10,000 drones per month¹, a significant strategic, tactical, and financial setback that can greatly diminish battlefield advantage. The US and allies need UAS radios that are less detectable and more resilient in the face of smart jamming.

¹ <https://www.forbes.com/sites/davidhambling/2023/05/22/ukraine-drones-losses-are-10000-per-month/>

Current State-of-the-Art

To contend with the increasing availability of detection equipment, companies have developed mitigations like Frequency Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS) to counter the threat of energy/signature detection and jamming. However, both are based on outdated assumptions of adversarial capabilities and often succumb to interference attacks, resulting in expensive equipment loss and mission failure while imposing additional constraints on capabilities and complexities of operations.

Newer spreading technologies attempt to create 'featureless waveforms,' but suffer from several key complications, including: radios that require specialized hardware; computational inefficiencies leading to large resource requirements for meaningful capability; and reliance on external dependencies like GPS or special clocks. Consequently, these technologies are often impractical, unnecessarily complex, and ineffective for both current operations and long-term support in field deployments.

FHSS

Frequency Hopping Spread Spectrum (FHSS) is a technique that avoids interference or interception by varying the center frequency of RF transmission, as shown in figure 2.1 below. FHSS is effective against narrowband jammers or unintended receivers that don't know the transmitter's hopping sequence. FHSS is particularly effective when multiple frequency hopping transmitters operate simultaneously within the same bandwidth that share the same external characteristics.

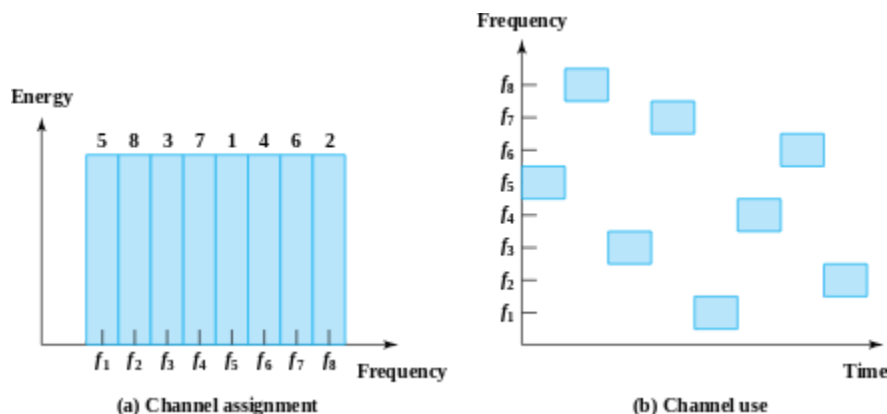


Figure 2.1 Title²

However, when deployed as the primary anti-jam (AJ) mitigation, FHSS can be countered with high bandwidth jammers or a set of receivers simultaneously capturing a range of frequencies as the transmitter hops. FHSS is also often degraded or inoperable without GPS/PNT. FHSS can be used as a signature to target signals of interest.

DSSS

Direct Sequence Spread Spectrum (DSSS) is a technique that mitigates interference by spreading the signal energy across a wide bandwidth, thus attempting to avoid detection and targeting altogether. Narrowband jammers struggle to detect and deny DSSS signals as they only interfere with a small percentage of the total signal energy.

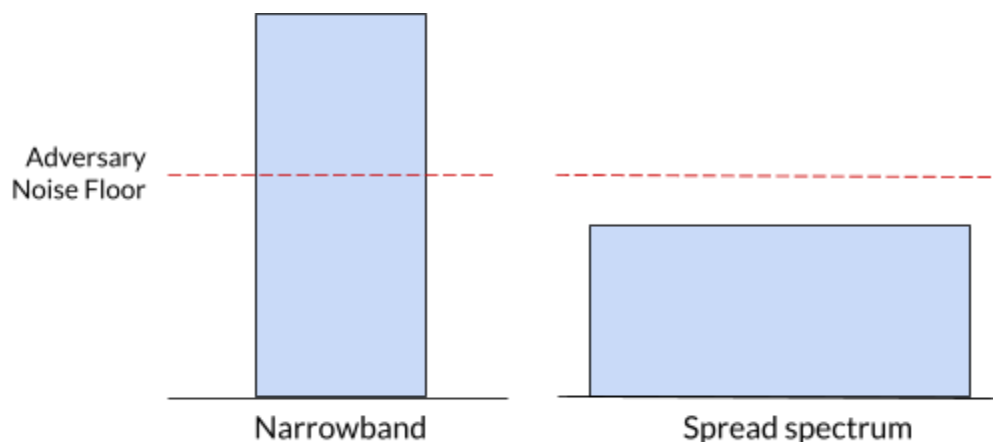


Figure 2.2 Narrowband and Spread spectrum signals with identical energy output

DSSS is a common technique in commercial communications for allowing multiple transmitters to share the same bandwidth using non-interfering spreading sequences. Relevant to contested RF environments, it also reduces detectability by spreading the total power of the signal across a wide bandwidth, lowering the peak power of the signal and limiting detection using standard radiometric techniques. However, for the same reasons that a DSSS signal is still detectable and useful in a commercial setting, DSSS (even low power DSSS) can be detected via a time-repeating pattern of the spreading code, a feature called cyclostationary. DSSS also relies on GPS/PNT, making it vulnerable to GPS jamming, rendering the system inoperable.

² Stallings, William. 2013. *Data and Computer Communications*, 10e. Pearson.

UAS Application

Current state-of-the-art UAS energy and signature mitigation techniques are inadequate and expensive for critical missions in EW environments. FHSS is vulnerable to energy detection and GPS/PNT jamming, while DSSS spreading sequences can be detected, recovered, fingerprinted, and jammed. Relying on these state-of-the-art solutions risks losing UAS assets to adversaries. The US and allies need a solution that reduces energy detectability, resists reactive jamming, and operates independently of GPS/PNT to increase mission success and survivability for UASs and their operators.

3. StrataWave™ UAS Radio

Secured UAS Communications

For mission success in the most contested environments, Rampart Communications has developed the StrataWave™ UAS Radio to provide secure and resilient communications for uncrewed systems. Featuring low probability of detection, anti-jamming, GPS-independent communication, and leading-edge encryption, it ensures mission-critical connectivity and survivability for UAS operators.

Benefits

Enhancing Mission-Critical Communications in Contested Environments

As adversaries employ increasingly sophisticated EW techniques, including jamming, detection, and signal exploitation, the need for resilient, low-detectability communications solutions is more critical than ever.

Our advanced UAS Radio technology is specifically designed to withstand and operate in harsh electromagnetic environments, providing users with exceptional EW resilience and survivability. This is achieved through:

- **Anti-Jam and Low Probability of Detection (LPD) Waveforms:** Our waveforms reduce observable transmission power by a factor of 30 compared to conventional non-spreading waveforms. This significantly decreases the likelihood of detection, geolocation, and targeting by adversaries, enhancing operational survivability for both personnel and platforms.
- **Physical Layer Resilience:** Unlike traditional systems that rely heavily on costly and resource-intensive methods, our approach physically fortifies the radio's ability to resist jamming, ensuring connectivity even in highly contested environments.

GPS-Independent Communications for Assured Connectivity

The increasing use of GPS jamming and spoofing techniques in both tactical and strategic environments creates serious vulnerabilities for systems dependent on Global Positioning System (GPS) signals for synchronization and positioning. Our technology directly addresses this threat by:

- **Eliminating the Need for GPS Receivers:** By removing reliance on GPS for timing and positioning, our radios operate independently of GPS signals, rendering GPS jamming and spoofing attacks ineffective.

- **Assured Communications in GPS-Denied Environments:** Whether operating in urban canyons, heavily forested areas, or contested battlefields, users can maintain secure and uninterrupted connectivity without depending on external navigation systems.

In the face of rapidly evolving threats and increasingly congested and contested electromagnetic environments, our advanced communications technology delivers **assured, secure, and resilient connectivity** that operators can trust. Combining **industry-leading anti-jam performance, GPS independence, and operationally validated encryption**, our solution empowers operators to maintain mission-critical communications even in the presence of active electronic warfare threats.

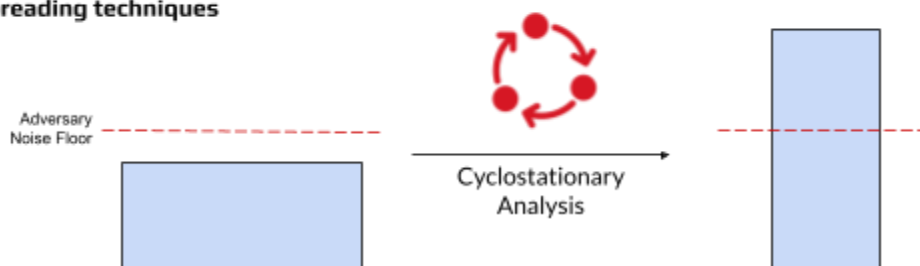
Novel Technology

The StrataWave™ UAS Radio is a Software Defined Radio (SDR) equipped with the Rampart FortisLink™, a secure spread spectrum waveform which mitigates energy detection and incorporates Rampart's cryptographic physical layer encryption.

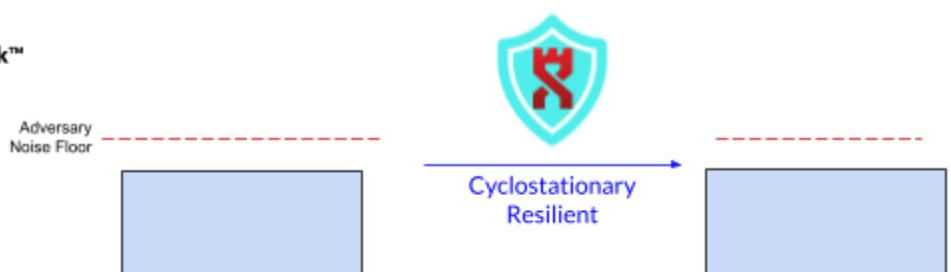
How FortisLink™ Works

StrataWave™ UAS radio is equipped with FortisLink, an ultra low-signature waveform that simultaneously reduces observable energy to avoid alerting jammers to the presence of communications signals, while also being resilient to those jammers' effects.

DSSS +other spreading techniques

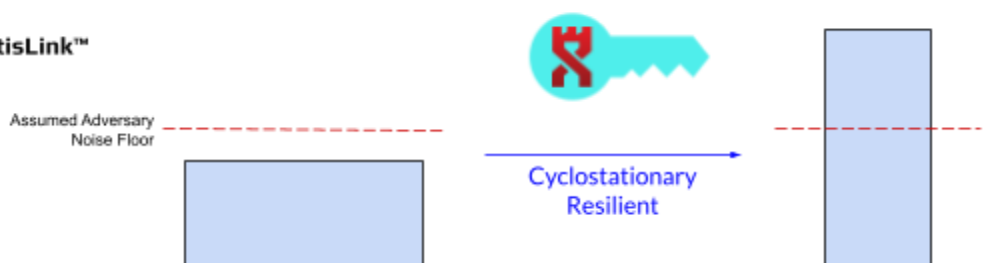


FortisLink™



The only way for a receiver to detect a FortisLink™ signal or access the data it is transmitting is with a cryptographic key. Adversaries can not gain any information about a FortisLink™ signal using cyclostationary analysis.

FortisLink™



Best-in-Class Physical Layer Encryption and Trusted Validations

Security is foundational to our system design, with encryption implemented directly at the physical layer to provide robust protection against interception and exploitation. Our encryption technology is supported by:

- **Independent Technical Validations:** Our technology has undergone rigorous technical reviews and assessments conducted by MITRE, the Navy Research Laboratory (NRL), and the U.S. Army DEVCOM (Combat Capabilities Development

Command), demonstrating both technological credibility and advanced security features.

- **Operational Validation:** Real-world operational testing and evaluations conducted by USSOCOM and other national security organizations confirm the system's effectiveness in highly dynamic, threat-rich environments.
- **55 Registered Patents:** Our intellectual property portfolio reflects entirely revolutionary innovation in secure communications.

Unparalleled Survivability

Rampart's StrataWave™ UAS Radio is specifically engineered for EW-contested environments, prioritizing Low Probability of Detectability (LPD) and Jamming (LPJ). It is optimized to minimize detection by reactive jammers, who target signals of interest based on energy threshold or waveform signatures. Even in scenarios where detection or persistent jamming is unavoidable, StrataWave™ UAS Radio is designed for exceptional resilience, enabling it to withstand and operate through in-band interference and rapidly re-establish communications after any temporary disruption, all without dependency on GPS or other external PNT systems.

The StrataWave™ UAS Radio significantly increases mission effectiveness and survivability in jamming and EW-contested environments. By outperforming FHSS and DSSS in detectability and resilience, this advanced radio delivers superior capabilities without compromising SWaP or data throughput.

Product Architecture



Rampart's StrataWave™ Modem leverages a software defined based architecture with quality industry components combined with a custom RF Front End (RFFE) to achieve higher performance optimization for specific UAS use cases. The Flexible RFFE is purpose built to accommodate a choice of two available bands while maintaining a small form factor. The StrataWave™ UAS Radio also offers an upgradeable platform that can accommodate new waveforms as they become available.

Specifications

Dimensions: 6.13" x 1.75" x 3.15"

I/O: Ethernet (RJ 45)

Data Rate: 500 kbps

Security Level: 256-bit Physical Layer Encryption

Voltage Range: 7-36v DC

Operating Bands: UHF, VHF

Transmission Range:

Frequency (MHz)	Estimated line of sight (LOS) Range (km)

300	223.80
400	137.00
500	95.00
900	37.35
1300	25.85
2450	12.23

Drone Integration

StrataWave™ connects to the UAS platform via IP/Ethernet and supports common protocols such as MAVLink. The StrataWave™ chassis has an 8P8C ("RJ45") socket. This suite of protocols is compatible with many commercial flight controller boards, including Pixhawk 4/5/6X.

Use Cases

Superior UAS Command and Control

Uncrewed and autonomous systems are essential in modern warfare, and command and control (C2) of those assets is critical for battlefield effectiveness. Today's threats to reliable C2 outpace defenses, leading to low survivability, and a high material and effort cost to sustain operations. With StrataWave™ UAS radio, our military will communicate with better resistance to jamming and a better ability to recover connectivity in contested environments.

Assured Communications in EW-contested Environments

Jamming and signal exploitation are company-echelon capabilities in the 21st century battlefield. Artificial Intelligence (AI) has enabled the adversary to quickly identify and fingerprint RF communications, rapidly turning RF emitters into targets, even with mitigations like frequency hopping and encryption. StrataWave™ UAS radio puts our military back in control—eliminating exploitation and measurably reducing the effectiveness of state-of-the-art EW tools, resulting in a higher rate of mission success.

Global, Secure, and Flexible UAS Communications

The rapid advancement of adversary capabilities leaves the US and its allies in a constant race to stay one step ahead. Even with state-of-the-art and defense-in-depth solutions, today's UAS communication systems fall short, leaving valuable mission data unprotected. The cryptographic and LPJ protection capabilities of the StrataWave™ UAS Radio, delivers the security needed for current and future missions. This enables reliable global communication and US and partner forces to remain mobile and flexible enough to carry out our global peacekeeping mission.

4. Conclusion

Modern warfare is increasingly dependent on autonomous systems to augment and extend battlefield power. The current state-of-the-art in UAS communications are inadequate for establishing superiority in today's complex threat landscape or defending against a well resourced and determined adversary. Rampart's StrataWave™ UAS Radio rewrites the rules for UAS communications in contested environments. By leveraging our proprietary FortisLink waveform, Rampart simultaneously reduces energy and signature, enhances resilience to jamming, operates independent of GPS/PNT, and significantly outperforms existing state-of-the-art UAS communication technologies. With Rampart's StrataWave™ UAS Radio, confidently extend your mission into the most challenging environments.

Increase the survivability and effectiveness of your UAS capabilities and operators in denied, defended, and contested environments, and secure your battlefield advantage with Rampart's StrataWave™ UAS Radio.

Experience Rampart's Solutions

Rampart is ready to secure your communications against the threats of today and tomorrow. Contact us to explore:

- **Purchasing:** Discuss how to purchase samples for testing or in volume for your group 2 and/or 3 drones.
- **Demonstrations:** Schedule a live demonstration to see the StrataWave™ UAS LPD and LPJ capabilities.
- **Technical Evaluations:** Receive a comprehensive assessment of how StrataWave™ UAS Radio meets your operational and technical requirements.

Future-proof your communications security and gain unparalleled survivability in contested environments with Rampart's solutions.

Contact Information:

Phone: +1 (826) 726-7278

Email: info@rampartcommunications.com

Company Background

Rampart Communications is a privately held U.S. company headquartered in Linthicum Heights, MD. Founded in 2019 by a team with extensive defense and signals exploitation experience. Rampart Communications, Inc. is an early-stage technology company built to revolutionize wireless communication. Our innovative RF radios and waveform technologies are making fundamental advancements in science to enhance the security, reliability, and capacity of communication systems.