A CRFS GUIDE TO

UNPACKING LOW PROBABILITY OF INTERCEPT SIGNALS

And finding them using RFeye DeepView

Written by James Spriet, Raven Whispers &
Jaimie Brzezinski (Signal Discovery section)

CRFS

EXTRAORDINARY
RF TECHNOLOGY

TABLE OF CONTENTS

INTRODUCTION TO LOW PROBABILITY OF INTERCEPT SIGNALS

Low Probability of Intercept (LPI) signals represent a sophisticated class of technology that is pivotal for enhancing the stealth and efficacy of modern communication and radar systems. By design, these signals are engineered to minimize their detectability by enemy sensors and interception systems, making them a foundation in Electronic Warfare (EW) and secure communications.

Definition & purpose

LPI signals are intentionally crafted to be challenging for receiving systems to detect and analyze. They incorporate advanced techniques to achieve this low visibility, including emission control to minimize power output, narrow-beam antennas to focus the signal and reduce side-lobe leakage, and modulation strategies that spread the signal's energy across a broader frequency spectrum. These characteristics ensure LPI signals can perform their intended communication or radar functions while remaining hidden from hostile detection systems.

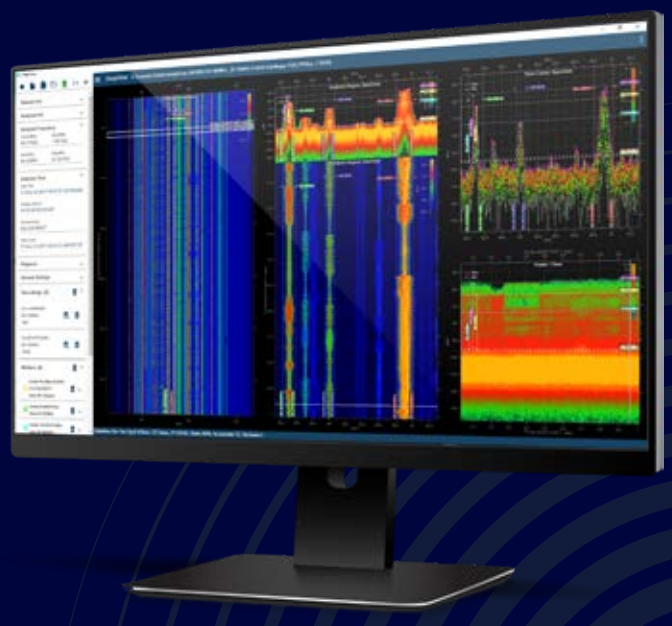
The purpose of LPI signals extends beyond mere evasion of detection. They are integral to maintaining the integrity and security of communications, particularly in environments with high potential for interception or jamming by adversaries. LPI signals are crucial for covert operations in military operations, ensuring that communication and radar emissions do not compromise the mission. LPI technologies safeguard against eavesdropping for secure communications, ensuring that sensitive information remains confidential.

Critical role in military & secure communication applications

The strategic advantage LPI signals offer in military contexts cannot be overstated. They enable forces to conduct surveillance, coordinate movements, and engage in EW without revealing their position or intentions to the enemy. This capability is critical for modern warfare, where electronic surveillance and signal intelligence play pivotal roles in battle outcomes.

LPI signals provide a layer of security for secure communication applications that traditional encryption alone cannot offer. While encryption secures the content of a communication, LPI technologies protect the existence of the communication itself. This dual-layer approach is indispensable in diplomatic communications, corporate espionage prevention, and any scenario where the mere detection of communication can have significant consequences.

LPI signals are foundational to modern communication and radar systems, offering a blend of stealth and security unmatched by other technologies. Their development and implementation reflect the ongoing evolution of EW and secure communication strategies, highlighting the continuous need for advancement in signal processing and emission control techniques.



Characteristics of LPI Signals: Modern detection systems now emphasize the capability to discern and analyze signals that stand out from ambient noise levels, thanks to enhanced sensitivity and sophisticated analytical techniques. This shift towards identifying signals above the noise floor is critical, as it enables more reliable detection and analysis, paving the way for the development of automated detection systems. These systems utilize advanced statistical analysis to identify patterns within large datasets, marking a significant step forward in the continuous effort to enhance the security and efficacy of communication and radar systems.

Emission Control in LPI Systems: In LPI technologies, emission control is crucial. This strategy involves minimizing the transmitter's power to the lowest effective level, thereby reducing the signal's detectable range. Simultaneously, LPI systems employ brief signal durations, limiting the time enemy sensors have to identify and process the emissions. These methods collectively enhance the stealth of communications and radar operations, embodying the strategic and complex design of LPI systems for secure and covert functionality.

Narrow-Beam Antennas: Narrow-beam antennas are common within LPI technologies. By directing the signal within a focused beam, these antennas minimize energy dispersion in non-targeted directions, enhancing power efficiency and significantly reducing detection risks by unintended receivers. Additionally, the design features, like suppressed side lobes, curtail signal leakage beyond the main beam path, further augmenting the LPI characteristics.

Low Power Output: The low power output of LPI signals is integral to their design. By emitting signals at power levels just above the noise floor, LPI systems make it challenging for enemy receivers to distinguish between the LPI signal and ambient RF noise. This low-power emission is crucial for operations where stealth is paramount, as it allows for communication and radar detection without alerting adversarial detection systems to the presence or location of the emitter.

Modulation Techniques: Modulation techniques play a significant role in the effectiveness of LPI signals. By spreading the signal across a wide frequency range (spread spectrum) or rapidly changing frequencies (frequency hopping), LPI signals become much harder to detect and decode. These techniques distribute the signal's energy in such a way that any single frequency band contains only a small portion of the signal's power, thereby diminishing its detectability.

The characteristics of LPI signals, ranging from emission control and the use of narrow-beam antennas to low power output, advanced modulation techniques, and reduced signal duration, underline their strategic importance in modern warfare and secure communications. These features collectively ensure that LPI signals maintain their integrity and purpose in environments where the risk of detection and interception is high, safeguarding sensitive information and operations.

TECHNIQUES FOR ACHIEVING LPI

To achieve LPI characteristics, sophisticated techniques are employed to minimize the detectability of signals. These techniques are foundational to the strategic advantage that LPI signals provide, especially in military and secure communication contexts.

Frequency Hopping: Frequency Hopping involves dynamically changing the transmission frequency of a signal over time. This technique is designed to complicate detection and interception efforts by adversaries. The signal evades fixed-frequency monitoring systems by hopping across a spectrum of frequencies in a pseudo-random sequence known only to the transmitter and the intended receiver. Frequency hopping can be categorized into slow and fast hopping, depending on the rate of frequency change. Slow hoppers change frequencies less frequently, allowing multiple bits of information to be transmitted on one frequency before hopping to the next. On the other hand, fast hoppers change frequencies more rapidly, often several times within a single bit of information, greatly complicating interception efforts.

Chirping (Sweeping): Chirping or frequency sweeping involves rapidly changing the signal's frequency across a wide band. Unlike frequency hopping, which jumps between discrete frequencies, chirping smoothly transitions through a range of frequencies during the transmission. This technique spreads the signal's energy across a broad spectrum, reducing the power at any single frequency and making the signal harder to detect against background noise. Chirped signals are particularly challenging for receivers tuned to narrow frequency bands, as the signal's frequency moves too quickly to be captured effectively.

Direct Sequence Spread Spectrum (DSSS): DSSS spreads a signal over a wide frequency band by modulating the transmitted signal with a pseudo-random sequence of bits known as chips. This sequence is much faster than the base information signal, spreading the signal's energy across a wider bandwidth. The spread signal appears as noise to unintended receivers not synchronized with the pseudo-random sequence. DSSS signals resist intentional jamming and interception because they require a receiver to know the pseudo-random sequence used to spread the signal to spread and decode it effectively. This technique also allows multiple transmissions to occupy the same frequency band without interfering with each other, known as Code Division Multiple Access (CDMA).

Each technique, frequency hopping, chirping, and DSSS, employs a different strategy to spread the signal across the frequency spectrum or rapidly change its characteristics. The common goal is to minimize the likelihood of detection and interception by making the signal blend in with the background noise or evade detection methodologies. These techniques form the core of LPI signal design, offering enhanced security and stealth for military operations and secure communications.

CHALLENGES IN DETECTING LPI SIGNALS

Detecting and intercepting LPI signals pose significant challenges due to their inherently stealthy characteristics. These challenges stem from the advanced techniques LPI signals employ to minimize their visibility and the complexities involved in signal processing for detection.

Low visibility & spread spectrum characteristics

LPI signals are designed to blend into the background electromagnetic environment, making them nearly indistinguishable from the noise. This low visibility is a fundamental challenge for electronic surveillance and interception systems, which rely on distinguishing signals from noise to detect and analyze them. By spreading their energy across a wide frequency range or rapidly changing their characteristics, LPI signals significantly reduce the signal-to-noise ratio (SNR) at any single frequency or point in time, complicating detection efforts.

Frequency hopping challenges

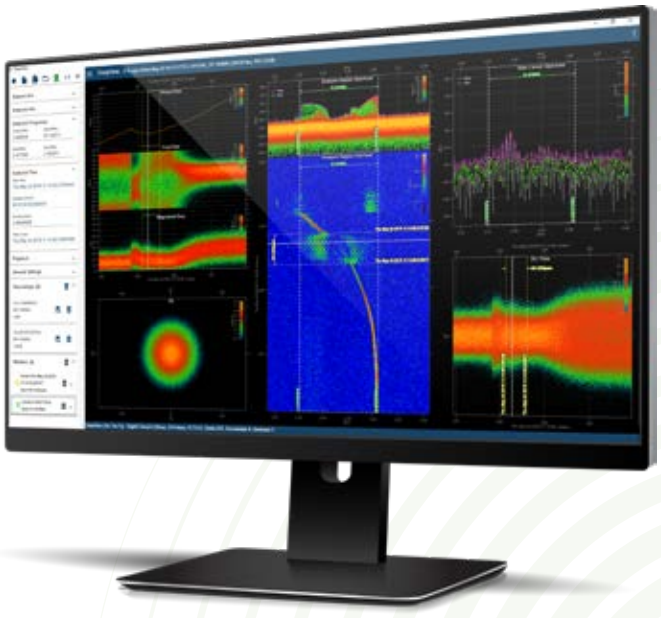
Frequency hopping signals change their operating frequency over time following a pseudo-random sequence. Detecting such signals requires receivers to predict or quickly follow these frequency changes. The randomness of the hopping pattern, especially in secure military applications where the pattern does not repeat for an extended period, demands sophisticated analysis techniques and fast-tuning receivers. The rapid changes challenge traditional interception methods, as the receiver must identify and tune to the new frequency within a fraction of the hopping period to capture the signal effectively.

Chirping (sweeping) signal detection difficulties

Chirped signals, which sweep across a wide frequency band at high rates, present another set of detection challenges. The sweeping action means that the signal's frequency constantly changes, making it difficult for narrowband receivers to capture the signal for any significant duration. Detecting such signals requires wideband receivers or specialized processing techniques to track rapid frequency changes.

Direct Sequence Spread Spectrum (DSSS) detection hurdles

DSSS signals are spread over a wide frequency band using a pseudo-random code, significantly lowering their power spectral density. This spreading makes them appear as background noise to receivers not synchronized with the spreading code. Detecting DSSS signals necessitates receivers that can despread the signal using the correct pseudo-random code, a challenging task without prior knowledge of the code used.



The trade-off of sensitivity versus bandwidth

The trade-off between sensitivity and bandwidth is a fundamental challenge in detecting LPI signals. Wideband receivers, necessary for capturing spread spectrum signals, inherently have lower sensitivity due to the increased noise bandwidth. This necessitates a delicate balance between having a wide enough bandwidth to capture the spread spectrum signal and maintaining sufficient sensitivity to detect the signal above the noise.

Increased complexity of receivers and processors

The techniques used to achieve LPI characteristics necessitate advanced signal processing capabilities in receivers. This includes Fast Fourier Transforms (FFT) for frequency analysis, sophisticated direction-finding techniques for locating the signal source, and the ability to process signals spread over a wide bandwidth or rapidly hopping across frequencies. The requirement for such advanced processing capabilities significantly increases the complexity of the receiver systems, requiring specialized hardware and software to detect and intercept LPI signals effectively.

The challenges in detecting and intercepting LPI signals are substantial, driven by the signals' low visibility, advanced modulation techniques, and the inherent trade-offs in receiver design. These challenges underscore the need for continuous advancements in electronic warfare technology to counter the evolving LPI signal strategies.

RFeye Nodes: Advanced detection tools for LPI signals

To effectively tackle the substantial challenges in detecting LPI signals, RFeye Nodes stand out as highly sensitive RF sensors tailored for this purpose. These nodes feature noise figures ranging from 8.5 to 16 dB, optimizing their sensitivity for low visibility environments where LPI signals typically operate. Furthermore, their phase noise at 1 GHz with a 20 kHz offset is notably low at -126 dBC/Hz, enhancing their ability to distinguish signals from the close-in interferers — a crucial factor in LPI signal interception.

Capable of sweeping from 9 kHz to 40 GHz with a 100 MHz instantaneous bandwidth (IBW), RFeye Nodes are designed to quickly adapt to the broad frequency ranges typical of frequency hopping or chirping LPI signals. This wide sweeping range and fast tuning capability ensure a high probability of intercepting even the most elusive signals.

When integrated with RFeye DeepView forensic analysis software, RFeye Nodes not only capture but also allow for detailed statistical analysis of pulse properties and the recording of I/Q data. This advanced functionality enables comprehensive analysis and detection of LPI signals, providing critical insights that are necessary for effective electronic surveillance and threat mitigation in modern electronic warfare environments.

COUNTERMEASURES & DETECTION STRATEGIES

Countermeasures and detection strategies against LPI signals involve a combination of advanced techniques and methodologies to enhance the capability of detecting such elusive signals. These strategies are crucial for EW and Signals Intelligence (SIGINT) operations, aiming to neutralize LPI signals' advantages regarding stealth and resistance to interception and jamming.

Optimized search strategies

Optimized search strategies involve sophisticated signal search algorithms that can rapidly scan across wide frequency ranges to identify signals of interest. These strategies may include predictive analysis to anticipate frequency hopping patterns or to identify the likely frequency bands of chirped signals. The aim is to reduce the search time and increase the probability of detecting LPI signals amidst a crowded electromagnetic spectrum.

Energy detection

Energy detection techniques focus on identifying subtle changes in the ambient electromagnetic environment that may indicate the presence of LPI signals. This approach relies on high-sensitivity receivers that detect signals with very low power levels. Advanced filtering and signal processing algorithms enhance the ability to distinguish LPI signals from background noise despite their low SNR.

Signal processing methods

Signal processing methods are integral to the detection and analysis of LPI signals. These methods include:

Fast Fourier Transform (FFT): FFT algorithms are used to analyze the frequency spectrum of captured signals, allowing for the identification of spread spectrum signals that may be hidden within a wide bandwidth.

Time-Frequency Analysis: This technique is useful for analyzing signals that change their frequency characteristics over time, such as frequency hopping or chirped signals. It provides a dynamic view of the signal's behavior across frequency and time domains.

Matched Filtering: In situations where the characteristics of a potential LPI signal are known or can be estimated, matched filtering techniques can be employed. This method maximizes the SNR by correlating the received signal with a template of the expected signal.

Cognitive Radio Techniques: Cognitive radio techniques involve intelligent algorithms that can adaptively search for and process LPI signals based on learning from the environment. This approach can dynamically adjust search parameters and processing techniques to improve detection performance.

Challenges

Implementing these countermeasures and detection strategies faces several challenges:

High Computational Requirements: The advanced signal processing techniques required for detecting LPI signals demand significant computational resources, which may limit their deployment in real-time systems.

Dynamic Signal Characteristics: The adaptive nature of LPI signals means that detection strategies must continuously evolve to keep pace with changes in signal design and transmission strategies.

False Alarms: The low visibility of LPI signals increases the likelihood of false alarms, where benign signals or noise are mistakenly identified as LPI signals. Balancing sensitivity and specificity is a critical challenge.

Countering LPI signals requires a multifaceted approach that combines optimized search strategies, energy detection, and sophisticated signal processing methods. Despite the inherent challenges, advancements in these areas are essential for maintaining the effectiveness of EW and SIGINT capabilities against stealthy communication and radar systems.

FINDING LPI SIGNALS WITH SIGNAL DISCOVERY: STATISTICAL ANALYSIS OF LARGE DATASETS

RFeye DeepView is a forensic signal analysis software for advanced signal monitoring and measurement, enabling users to glean information from a large amount of data. Users can reliably record and capture RF signals (I/Q data), which can be analyzed and further processed.

Due to their wide bandwidth and highly complex, low-power characteristics, LPI signals are challenging to intercept. However, the Signal Discovery feature of RFeye DeepView allows users to efficiently carry out statistical analysis of large datasets—allowing them to identify anomalies that can reveal an LPI signal more quickly.

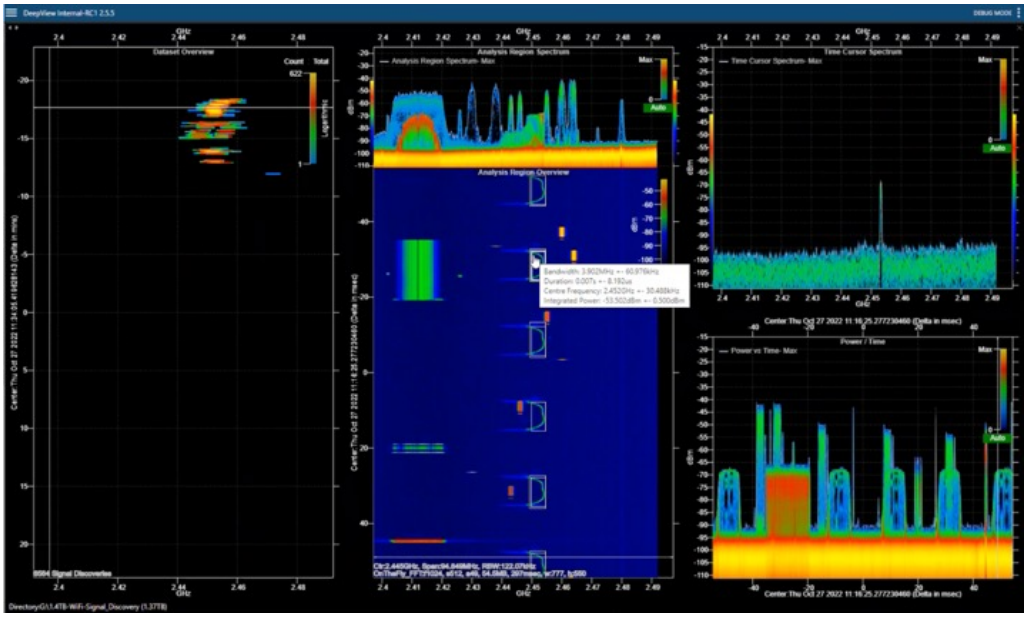
How does Signal Discovery work?

Modern communication revolves around pulses and power. Signal Discovery gives EW and SIGINT operators who want to identify and geolocate an unknown transmission visibility and the ability to understand pulse parameters more clearly.

Recording I/Q data over a long duration creates a database of pulse descriptors; however, this results in a sea of analog information. Signal Discovery allows operators to view all this information and make sense of it statistically by searching for hotspots. By querying the database for a particular pulse type in real-time, users can quickly access those specific pulse types from the whole recording, which would not have been possible had they searched manually.

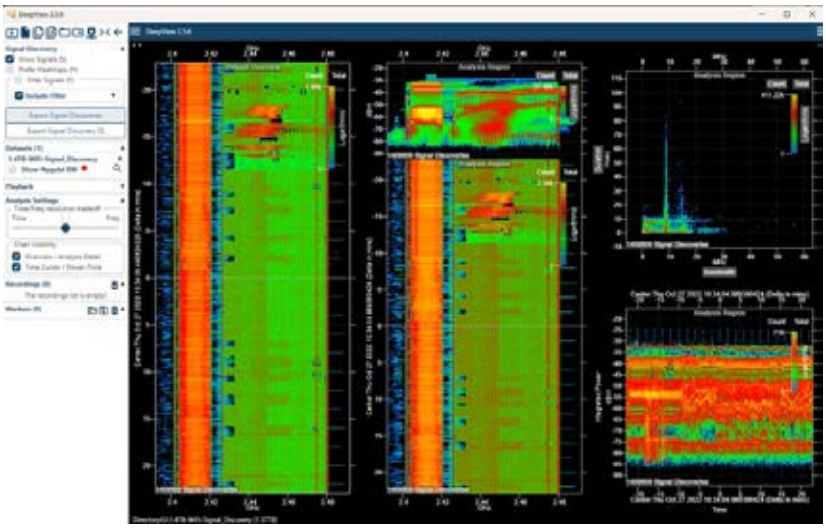
Essentially, Signal Discovery allows users to identify statistical anomalies by discriminating between what they expect and what they do not expect. They can then quickly zoom into patterns of signals to reduce the number of signals from over a million to one hundred.

>>> ***Image 1:*** *When hovering over the signal, Signal Discovery shows the pulse descriptor*



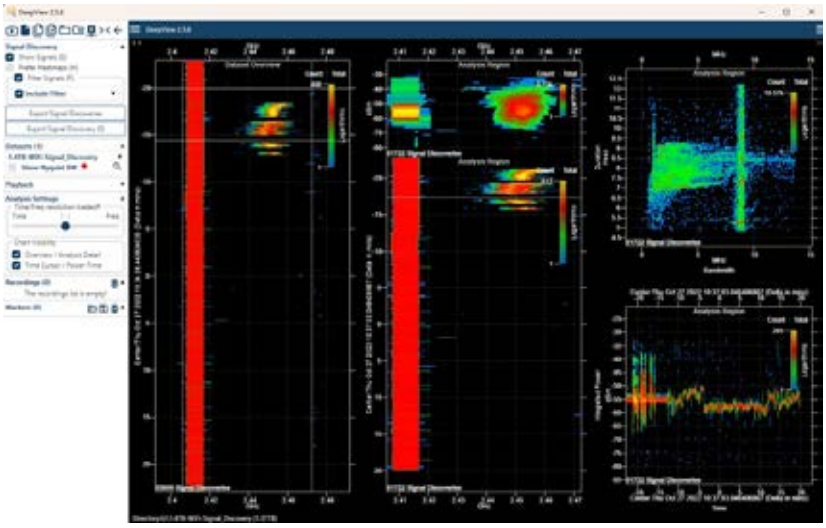
Example: discovering a signal in a crowded Wi-Fi band (2.4 GHz)

With a statistical view, users can see all signals in the spectrum. The top right box in Image 2 shows signal hotspots that are combinations of pulse bandwidth and pulse duration. However, no human operator can analyze 1.4 million signals. Signal Discovery allows the user to select a hotspot area of interest, reducing the number of signals to 51,722.

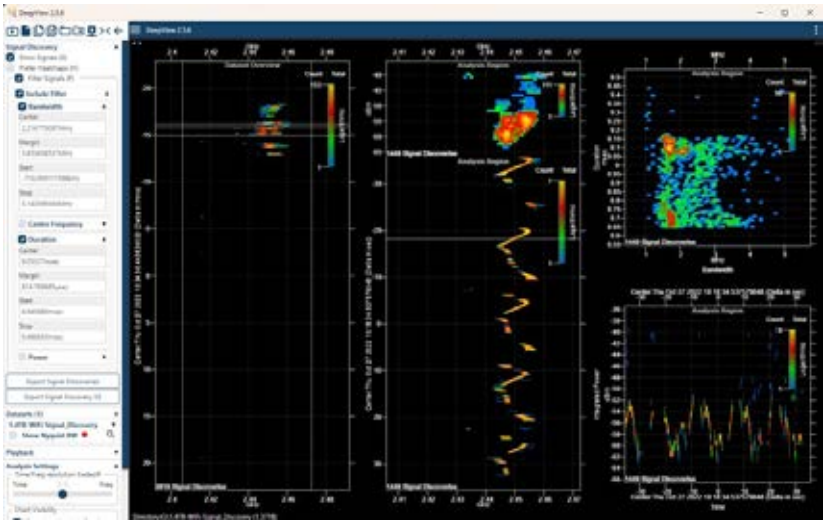


<<< ***Image 2:*** *The flexible view displays the frequency, time, power, bandwidth, pulse duration, and pulse repetition rate of the signals*

Identifying an unexpected statistical hotspot allows the user to see patterns and identify something relevant. By continuously zooming into hotspots of interest (which isolates signals of interest), users can reduce the number of signals and see statistically similar signals.

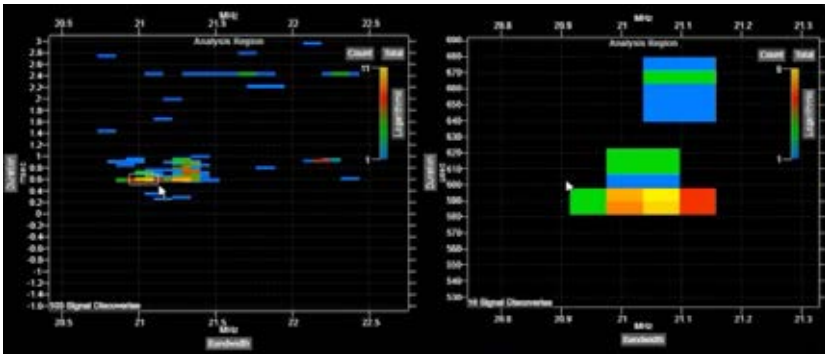


<<< ***Image 3:*** *Choosing a hotspot area reduces the number of signals to 51,722*



<<< ***Image 4:*** *Further filtering reduces the number to 1449 signals*

Users might see statistical patterns based on time of day or specific days—patterns that are unlikely to have been noticed without the ability to zoom into areas of interest.



<<< ***Image 5:*** *Further filtering of signals in the dataset*

The images above show how confining the view to certain statistical parameters further reduces the number of signals from 103 to 16.

Once the user has a manageable number of signals, further analysis can be carried out of these signals to identify a particular transmitter. While the Signal Discovery feature does not tell the user the nature of these signals, we statistically expect to see certain types of signals when looking in a specific band.

After using Signal Discovery to identify LPI signals of interest, users can use DeepView to analyze those signals further.

If a SIGINT or EW operator identifies an enemy signal, they can build a detector against that signal. When loaded into real-time spectrum monitoring software RFeye Site, detectors look at a signal's frequency, power, and time characteristics, and when they find a match, they will automatically trigger a workflow geolocation to geolocate the emitter.

REAL-WORLD APPLICATIONS OF LPI TECHNOLOGIES

Real-world applications of LPI technologies span both military and civilian domains, showcasing these systems' versatility and critical importance. Their development and the countermeasures they inspire represent a dynamic interplay of technological advancement and strategic adaptation.

Military applications

Secure Communications: In military operations, secure and undetectable communications are paramount. LPI technologies enable forces to communicate without revealing their location or intentions to adversaries, which is essential for covert operations and strategic maneuvers. Frequency hopping and Direct Sequence Spread Spectrum are widely used to mask signals, making it difficult for enemy forces to intercept or jam communications.

Radar Systems: LPI radars use advanced modulation techniques to spread their emissions over a wide frequency band, significantly lowering the probability of detection by enemy Radar Warning Receivers (RWRs). This capability is crucial for surveillance and reconnaissance missions, allowing military assets to gather intelligence while minimizing the risk of being discovered.

Navigation Systems: While not exclusively military, the Global Positioning System (GPS) is a prime example of LPI technology in use. The GPS signals are spread spectrum, making them inherently resistant to interference and difficult to detect, providing critical positioning information for a wide range of military applications.

Civilian applications

Wireless Communications: In the civilian sector, LPI technologies underpin various forms of wireless communication. Spread spectrum techniques, such as those used in Wi-Fi and cellular networks, ensure reliable service in congested electromagnetic environments by reducing interference and enhancing privacy.

Commercial Navigation: Commercial aviation and maritime industries benefit from LPI technologies through enhanced radar systems that offer improved detection capabilities while reducing the radar's visibility to others. This is crucial for safety in busy airspaces and congested sea lanes.

Dynamic nature of LPI signal development

The development of LPI technologies is a continuous cycle of action and reaction. As new LPI techniques are developed, so are the methods for detecting them. This ongoing evolution drives technological innovation in both offensive and defensive capabilities. For instance, the advancement in spread spectrum and hopping techniques has led to the development of more sophisticated signal processing algorithms and detection systems designed to counter these measures.

The counter-development efforts focus on creating more sensitive receivers, advanced signal processing techniques, and artificial intelligence algorithms capable of identifying and analyzing LPI signals amidst a sea of noise. This cat-and-mouse game underscores the strategic importance of electronic warfare and signals intelligence in modern military and security contexts.

LPI technologies are vital in military and civilian applications, offering secure, reliable communication and sensing capabilities essential for operational success and safety. The dynamic interplay between LPI signal development and countermeasure innovation continues to drive advancements in electronic warfare, signals intelligence, and communication technologies.

Future directions in LPI signal technology

The landscape of LPI signal technology is marked by relentless innovation and strategic countermeasures. As the digital and electromagnetic domains become increasingly contested, the future of LPI technologies is set to evolve in ways that will further enhance their stealth, resilience, and effectiveness. The perpetual arms race between signal stealth technologies and detection capabilities drives this evolution.

Future advancements in LPI technologies

Enhanced LPI Signal Detection: Modern detection systems now emphasize the capability to discern and analyze signals that stand out from ambient noise levels, thanks to enhanced sensitivity and sophisticated analytical techniques. This shift towards identifying signals above the noise floor is critical, as it enables more reliable detection and analysis, paving the way for the development of automated detection systems. These systems utilize advanced statistical analysis to identify patterns within large datasets, marking a significant step forward in the continuous effort to enhance the security and efficacy of communication and radar systems.

Machine Learning and AI Integration: Integrating machine learning and Artificial Intelligence (AI) into LPI systems is expected to revolutionize how these signals are generated, modulated, and encrypted. AI could enable dynamic adaptation of signal characteristics in real-time, based on the detection threats present in the environment, making LPI signals even more difficult to detect and decode.

Quantum Communication: Quantum technologies promise a significant leap in secure communication. Quantum Key Distribution (QKD) and entanglement-based systems could offer inherently secure communication channels that are immune to interception. For LPI technologies, quantum advancements could mean the development of signals that are not only LPI but also quantum-secure against eavesdropping.

Advanced Spectrum-Sharing Techniques: As the electromagnetic spectrum becomes increasingly crowded, future LPI technologies will likely leverage more sophisticated spectrum-sharing techniques. These could involve cognitive radio capabilities that dynamically select frequencies, modulation schemes, and power levels to minimize detectability while optimizing bandwidth use.

Enhanced Modulation and Coding Schemes: The development of new modulation and coding schemes inherently resistant to interception and analysis will be a crucial area of focus. These advancements may include more complex forms of spread spectrum, frequency hopping, and time-hopping techniques that provide even lower visibility and greater resilience against jamming and detection.

The Ongoing Arms Race

The future of LPI signal technology is inextricably linked to the ongoing arms race between stealth technologies and detection capabilities. As LPI techniques become more sophisticated, so do the methods and technologies designed to detect them. This includes:

Improved Signal Analysis Tools: Detection systems will likely employ more powerful signal analysis tools capable of processing vast amounts of data in real time, utilizing deep learning algorithms to identify patterns indicative of LPI signals.

Advanced Sensor Technologies: Developing sensors with enhanced sensitivity and selectivity will be crucial in detecting the subtle signatures of LPI signals. This may include deploying distributed sensor networks that can triangulate signal origins with high precision.

Cross-Domain Detection Strategies: Future detection strategies may integrate information from multiple domains (cyber, space, and traditional EW sensors) to identify and counter LPI signals, leveraging data fusion and analytics to overcome the stealth advantages of LPI technologies.

The future of LPI signal technology is poised at the cutting edge of scientific and technological innovation. The continuous interplay between advancing LPI techniques and developing counter-detection strategies underscores the dynamic nature of electronic warfare and secure communications. As both sides of this arms race push the boundaries of what is possible, the strategic importance of mastering the electromagnetic spectrum will only grow, shaping the future of conflict, competition, and cooperation in the digital age.

CONCLUSION

The strategic landscape of modern warfare and secure communications is increasingly defined by the ability to operate undetected within the electromagnetic spectrum. LPI signals stand as a testament to the ingenuity and foresight embedded in today's communication and radar systems, offering a blend of unparalleled stealth, security, and resilience in the digital age. These technologies, by design, enable military and civilian operations to proceed with minimal risk of detection or interception, safeguarding sensitive information and strategic maneuvers against adversarial eyes.

The advancement and implementation of LPI technologies highlight the vital necessity for ongoing adaptation and innovation in modern electronic warfare and communication strategies. As the electromagnetic environment becomes more congested and contested, the evolution of LPI techniques remains a priority for defense planners and communication engineers alike. This evolutionary path is characterized by an ongoing arms race, where advances in stealth capabilities are met with sophisticated counter-detection and interception strategies. The cycle of action and counteraction drives the technological progress that defines the field, pushing the boundaries of what is possible in electronic warfare and secure communications.

Reflecting on this dynamic interplay, it is clear that the importance of LPI signals extends beyond their immediate tactical advantages. They represent a broader commitment to operational security, strategic flexibility, and technological superiority. As we look to the future, the continuous evolution of LPI technologies in response to emerging threats and challenges will undoubtedly play a pivotal role in shaping the outcome of conflicts and the security of communications. In this ever-evolving landscape, the mastery of LPI signals and their countermeasures will continue to be a foundation of electronic dominance and strategic deterrence.

The journey of LPI technologies is far from complete. With each leap forward in detection and counter-detection capabilities, the ingenuity behind LPI signals will be called upon to rise to new challenges. In this ongoing quest for supremacy within the electromagnetic spectrum, the ability to communicate and operate undetected remains a crucial enabler of success, security, and stability in an increasingly complex and interconnected world.

CRFS Inc
Chantilly,
VA, USA
+1 571 321 5470

CRFS Ltd
Cambridge,
United Kingdom
+44 (0) 1223 859 500