SANDIA REPORT
SAND2014-1695
Unlimited Release
Printed March 2014

Radar Operation in a Hostile Electromagnetic Environment

Armin W. Doerry

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2014-1695
Unlimited Release
Printed March 2014

Radar Operation in a Hostile Electromagnetic Environment

Armin Doerry
ISR Mission Engineering

Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185-0591

Abstract

Radar ISR does not always involve cooperative or even friendly targets. An adversary has numerous techniques available to him to counter the effectiveness of a radar ISR sensor. These generally fall under the banner of jamming, spoofing, or otherwise interfering with the EM signals required by the radar sensor. Consequently mitigation techniques are prudent to retain efficacy of the radar sensor. We discuss in general terms a number of mitigation techniques.

Acknowledgements

This report is the result of an unfunded Research and Development effort.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Contents

Foreword 6
Classification 6
1 Introduction 7
2 The Radar Signal 9
2.1 More Power 9
2.2 Less Detectable Waveforms 9
2.3 More Robust Waveforms 10
2.4 Multi-band Operation 10
2.5 Sub-band Channels 10
2.6 Antenna Null Steering 10
2.7 DOA Techniques 10
2.8 Polarization Purity 11
2.9 Cognitive Radar Techniques 11
2.10 Interference Rejection Techniques 11
2.11 Pulse Code Nulling 11
2.12 High-Dynamic Range Receiver 12
2.13 Bistatic Operation 12
2.14 Passive Operation 12
3 The Navigation Signals 13
3.1 More Robust GPS 13
3.2 Transfer Alignment from Higher-Quality Navigator 13
3.3 Additional (Backup) Aiding 13
3.4 Ground-Based Aiding 14
3.5 Radar Processing Sans Motion Measurement 14
3.6 Radar as Navigation Instrument 14
4 The Command, Control, and Communications Signals 15
4.1 More Robust C3 Link 15
4.2 Pre-Planned Mission 15
4.3 On-Board Mission Data Storage 15
4.4 System Cognition 16
5 Conclusions 17
References 19
Distribution 20

Foreword

This report details the results of an academic study. It does not presently exemplify any modes, methodologies, or techniques employed by any operational system known to the author.

Classification

The specific concepts, mathematics and algorithms presented herein do not bear any release restrictions or distribution limitations.

This distribution limitations of this report are in accordance with the classification guidance detailed in the memorandum "Classification Guidance Recommendations for Sandia Radar Testbed Research and Development", DRAFT memorandum from Brett Remund (Deputy Director, RF Remote Sensing Systems, Electronic Systems Center) to Randy Bell (US Department of Energy, NA-22), February 23, 2004. Sandia has adopted this guidance where otherwise none has been given.

This report formalizes preexisting informal notes and other documentation on the subject matter herein. It also presents the results of surveying the open literature.

1 Introduction

Radar is undeniably a useful Intelligence, Surveillance, and Reconnaissance (ISR) sensor. As such, it is to be expected that an adversary may wish to negate or diminish the utility of such a sensor. An adversary's ability to deny the utility of a radar sensor falls under the banner of Anti-Access/Area Denial (A2/AD) capability, and more specifically Electronic Warfare (EW). The universe of denial techniques are collectively described as Electronic Counter-Measures (ECM). Techniques to operate in spite of ECM are termed Electronic Counter-Counter-Measures (ECCM).

Herein we are concerned primarily with ISR radar modes such as Synthetic Aperture Radar (SAR), Inverse-SAR (ISAR), various Moving Target Indicator (MTI) radar modes, and Wide Area Search (WAS) modes. In particular we will generally presume herein that the aircraft is an Unmanned Aerial Vehicle (UAV), although much of the subsequent discussion also applies to manned vehicles.

It is well-known that a radar system is vulnerable on a number of fronts. We emphasize "system" as the totality of what it takes to utilize the radar as an effective ISR sensor. That is, the total system is more than just the sensor itself, i.e. the radar "box."

In this report we discuss at a high level the susceptibility of a radar system to a hostile Electro-Magnetic (EM) environment, and possible measures to mitigate the risk. The intent is to provide a broad overview and some notion of scope to the problem and mitigation concepts.

Accordingly, we recognize that a radar system is susceptible to hostile EM interference and disruption via several mechanisms. These include

1. Jamming/spoofing/interference of the radar signal itself
2. Jamming/spoofing/interference of navigation signals like GPS
3. Jamming/spoofing/interference of the command, control, and communications link(s)

We define these means of disruption as follows.

> Jamming is the overwhelming of a desired signal with another undesired signal meant to disrupt the utility of the desired signal.
>
> Spoofing is the generation of false signals meant to fool the receiver into detecting targets or target characteristics/features that aren't really true. This is also referred to as "Deception Jamming" or "Repeater Jamming."
>
> Interference is any disruptive technique that is not otherwise jamming or spoofing. For the purposes of this report, it includes eliminating sources or otherwise damaging links.

We opine that it makes little sense to barricade the front door while at the same time leaving the back door wide open. Similarly, it makes little sense to address any one of

these enumerated mechanisms while ignoring the other(s). An adversary is not likely to be so cooperative.

The open literature contains a number of books and papers that address the topic of EW against radar systems and mitigation schemes. With no intent to offer a complete bibliography on the topic, we offer a very few samples as representative of the breadth.

> A good introduction on radar jamming is given in a chapter by Farina in the book edited by Skolnik.[1]
>
> Electronic Warfare with respect to SAR is addressed in a book by Goj.[2]
>
> A number of SAR jamming measures are discussed by Wu, et al.[3]
>
> Anti-jamming techniques for SAR are discussed by Rosenberg and Gray.[4]

We further opine that after this report, the reader is advised to engage a literature search on the topic, and be prepared for the avalanche of results.

In the following, we examine the previously enumerated jamming/spoofing/interference mechanisms in more detail, along with mitigation measures, but still only at a cursory level. This report is essentially a compendium of the open literature on the topic.

2 The Radar Signal

Direct jamming/spoofing/interference of the radar signal itself can occur by a variety of mechanisms. These include, but are not necessarily limited to

1. Raising the noise level in the radar data
2. Adding other narrow-band or wideband energy to the ambient spectrum
3. Fooling the radar with artificial coherent target energy, including decoys
4. Chaff and/or other confusers and obscurants
5. Misdirecting/degrading Direction-of-Arrival (DOA) measurements

Mitigation techniques might include one or more of the following.

2.1 More Power

A fundamental measure of radar data goodness is Signal-to-Noise Ratio (SNR). When excessive noise washes out radar data, an obvious remedy is more signal power to burn through the noise.

In the presence of jammers and/or interfering emissions or echoes, the goodness measure becomes Signal-to-Interference-plus-Noise Ratio (SINR). Likewise, more power is usually better if the interfering emissions are additive in nature.

More Effective Radiated Power (ERP) may be had by either greater actual transmitted power, or by increased antenna gain.

In any case, more ERP will allow a greater stand-off distance from the adversary's target, itself useful for a number of obvious reasons.

2.2 Less Detectable Waveforms

We might expect that many countermeasures to radar, or to ISR sensors more generally, are enabled only when an adversary first detects that the sensor is being employed. Consequently, if a radar doesn't 'trip' the countermeasure, then it may not have to deal with it.

This implies that if the radar waveform were less detectable, or identifiable as a radar waveform, then ECM might be avoided. Such radar waveforms are termed Low-Probability of Detection (LPD), or Low-Probability of Intercept (LPI) waveforms. That is, the radar offers some degree of stealth towards an adversary.

That said, we stipulate that it remains rather difficult to completely hide a high-power microwave source in the sky.

2.3 More Robust Waveforms

A radar waveform's susceptibility to spoofing generally depends on the predictability of the waveform. The less predictable that a waveform is, the more robust it is to spoofing. For example a constant Linear-FM (LFM) chirp waveform is very predictable, and hence very susceptible to spoofing. Random waveforms, or waveforms with random features or parameters, are more resistant to spoofing.

In particular, noise and noise-like waveforms have received much attention recently in the radar literature. We offer as entry point into this large body of literature a report by Doerry and Marquette.[5]

2.4 Multi-band Operation

Many ECM techniques, indeed even often-times chaff, are specific to individual radar bands. While one band might be rendered unusable, another band might be clear and available for radar ISR. If a hostile emitter is itself band-limited, the obvious mitigation technique is for a radar to be able to operate on another of a set of multiple radar bands.

2.5 Sub-band Channels

If a hostile emitter is band-limited, ECM might be avoided by operating in a different frequency sub-band. For example, a radar with 3 GHz bandwidth may only require a 1 GHz or less bandwidth for 0.3 m range resolution. Consequently, a 3 GHz band offers at least 3 non-overlapping sub-band channels for this resolution. A 3 GHz band offers at least 15 non-overlapping channels to support 1 m range resolution. If a particular part of a 3 GHz band is being jammed, then radar operation might move to a 'clear' channel.

2.6 Antenna Null Steering

Antennas have directions of zero-response. These are called "nulls". Almost all antennas have them. Hostile emitters in the direction of an antenna null will be severely attenuated. While Active Electronically Steered Array (AESA) antennas are touted as being able to steer nulls towards jammers or other interfering emitters, even mechanical antennas have nulls that can be directed towards hostile emitters, albeit with somewhat less flexibility.

2.7 DOA Techniques

Related to the Antenna Null-Steering techniques, received hostile energy may be evaluated for Direction of Arrival (DOA) with a multi-phase-center antenna. In this manner, spoofed energy might be separable, or at least distinguishable from the desired echo energy. Sidelobe cancellers fall into this category.

2.8 Polarization Purity

A well-known technique to degrade DOA measurements (like monopulse measurements) is to echo a cross-pol response. Consequently, mechanisms to ensure cross-pol rejection may mitigate this technique. Examples include better antennas with respect to cross-pol rejection, or antenna auxiliary equipment like polarization screens.

2.9 Cognitive Radar Techniques

Cognition is generally associated with a mental process that involves awareness, perception, reasoning, and judgment.

A step beyond the previous techniques is for the radar to examine its environment, including the local EM spectrum, and then use some cognition to auto-select the best available operating characteristics. This would certainly include the operating spectrum. It might also further select other radar operating parameters like best useable resolution, specific waveform properties, etc. An entry point into the literature of Cognitive Radar is a book by Guerci.[6]

Essentially, the radar must have some capacity for best deciding 'how' to best accomplish the ISR data collection task requested of it.

2.10 Interference Rejection Techniques

Narrow-band jamming that doesn't overwhelm the radar can be treated like unintentional interference. This energy can be excised with a variety of signal processing techniques.

We exemplify one technique for apodizing the effects of interference in a report by Doerry.[7]

2.11 Pulse Code Nulling

Digital RF Memory (DRFM) based jammer/spoofing technology essentially captures the transmitted signal and reradiates it towards the radar receiver, typically with some delay or modulation attached. The delay might be an amount that is more than one Pulse Repetition Interval (PRI). In fact, for some spoofing characteristics, it needs to be at least one PRI. Consequently the spoofing signal is equivalent to a return from an ambiguous range.

If the pulse latency is known, then pulse phase coding might be employed to effectively null the false spoofing echoes. Such a scheme is described in a report by Doerry[8] to null specific ambiguous ranges, and also described in a paper by Soumekh.[9]

We note that this technique makes use of a corollary to a previously mentioned truism, namely that the more predictable an ECM waveform is, the more susceptible it is to ECCM.

2.12 High-Dynamic Range Receiver

Radar receivers tend to be very sensitive receivers, typically exhibiting some fairly high gain. After all, they are looking for tiny energy reflections from the target. Consequently they are often sensitive to saturation by high-power in-band emissions from nefarious or other external transmitters, especially when aimed towards them by high-gain antennas. This is a dynamic range issue for the radar receiver.

Simply put, receivers with a high dynamic range are less susceptible to saturation than receivers with low dynamic range.

2.13 Bistatic Operation

We offer the basic tenet that high-power jamming/spoofing/interference ECM signals are more odious than low-power jamming/spoofing/interference ECM signals. This implies that from an adversary's perspective, an ECM signal emitted through a high-gain antenna directed at the radar receiver is desirable. However, a high-gain antenna is inherently a narrow-beam antenna, which means that the adversary needs to know the radar receiver location with sufficient accuracy and precision to properly aim the ECM signal's beam towards it.

A radar receiver by itself is inherently passive. So, if the receiver can be separated from the transmitter in a bistatic mode, i.e. located in separated vehicles, then the receiver offers a stealthy target to the adversary. As such, the effectiveness of an aimed ECM signal is diminished.

We note that specialized techniques might be developed to jam bistatic radars, as presented by Wang and Cai.[10]

2.14 Passive Operation

The ultimate in stealthy microwave sensing/imaging operation is to not require any transmitter at all, that is, sensing/imaging based on the radiometric emissions of the target itself rather than reflections of a high-power artificial source. This is termed "radiometry."

Information on Airborne radiometry is extensively published in the open literature.

We note that a subset of radiometry is Synthetic Aperture Radiometry. Essentially, multiple antenna phase centers measure spatial frequencies of received emissions via cross-correlation operations, but different spatial frequencies may be measured at different times as the phase centers change orientation with respect to each other. Information is combined to form the radiometric image. One of the most well-known examples of Synthetic Aperture Radiometry is the Very Large Array (VLA) radio-telescope near Socorro, NM, used for radio-astronomy. The open literature also reveals a number of airborne earth-observing examples as well.

3 The Navigation Signals

Jamming/spoofing/interference of navigation signals like Global Positioning System (GPS) will diminish radar performance by degrading the motion measurement data that the radar often requires to function optimally. Of course, if GPS is eliminated outright, that would also be problematic for many radar modes.

Mitigation techniques to allow radar operation in spite of GPS denial, or other motion measurement degradation, might include one or more of the following.

While we focus here on GPS, we acknowledge that other navigation aids also use radio links, and more generally the comments below are applicable to radio-navigation aids in general.

3.1 More Robust GPS

Clearly one answer is to make the GPS subsystem itself more robust with respect to jamming, spoofing, and interference. Lots of folks are working on this already. Specific techniques are beyond the scope of this report.

A corollary to this is to allow employment of other similar services that might not be suffering the same degradation, e.g. GLONASS, Galileo, etc.

3.2 Transfer Alignment from Higher-Quality Navigator

The principal purpose of GPS for the radar is to keep the Inertial Measurement Unit (IMU) aligned. In the absence of GPS, the radar's IMU may be kept aligned by using the host aircraft's own navigation system, which may include a more accurate and stable navigation-quality IMU, or perhaps a more robust GPS, or perhaps even other navigation instruments. Aligning the radar's navigator to the aircraft's navigator is termed a "transfer alignment."

3.3 Additional (Backup) Aiding

Sometimes even fairly coarse estimates of some position or velocity parameters can be quite useful to enhancing the utility of a radar sensor.

Radar altitude information is particularly useful in simply being able to estimate the necessary depression angle of an antenna for a particular range. For this, a barometric altimeter reading would be enormously helpful.

Radar velocity over the ground can be coarsely estimated with the aircraft's airspeed indicator instruments. This might be sufficiently accurate to allow refinement from radar readings themselves.

3.4 Ground-Based Aiding

Occasions may arise where the ground station for a UAV might have position or velocity knowledge not directly available to the radar itself, be it from ground measurements or from other on-board instruments. Consequently the radar might allow for some manual override, or calibration, of its internal navigator via the command and control link.

3.5 Radar Processing Sans Motion Measurement

Radar data products (SAR images, GMTI detection maps, etc.) may be formed even in the absence of any motion measurement information. Although quality may be degraded, newer signal processing techniques might be employed to mitigate the dependence on GPS in order to maintain sensor utility. The idea is to collect and process the data without any (or very minimal) motion information or compensation, letting any focusing be entirely (or mostly) data driven.

3.6 Radar as Navigation Instrument

The radar itself may be used to augment a vehicle's navigator. For example, a SAR can image known landmarks to ascertain aircraft position error. Techniques have already been demonstrated to maintain antenna angular alignment using SAR images.[11,12]

Furthermore, radar Doppler measurements can be used to measure vehicle orientation and velocity components. In fact, a whole class of radars does exactly this, and are termed "Doppler Navigation" radars. These principles may be exploited even by more conventional range-Doppler radars.

4 The Command, Control, and Communications Signals

Jamming/spoofing/interference of the Command, Control, and Communications (C3) signals will interfere with commanding the radar to do what is desired, or extracting the radar products to a remote operator/user. This is particularly problematic with remote operation, like with a UAV.

Fundamentally, if 'external' C3 signal links are severed, then the utility of a radar system must necessarily depend on 'internal' C3 capabilities. That is, the radar must exhibit useful autonomy. We note that while we are discussing the severance of the C3 link due to an adversary's action, we might also at times wish to disable or suppress our own C3 link to advantage (i.e. radio silence) for stealth reasons.

For the purposes of this report, autonomy means that in the absence of external C3, the radar must still do something useful in spite of the severed C3 connection.

We stipulate that autonomy might mean different things to different people, and comes in many shades of gray. Autonomy may span capabilities ranging from a default operational mode (e.g. revert to a basic GMTI WAS mode) to a fully integrated sensor serving some higher cognitive process or mission (e.g. do what it takes to find vehicles of interest in collaboration with other sensors).

Some particular autonomous functions might include some of the following.

4.1 More Robust C3 Link

Although not an autonomy feature or technique, we would be remiss in not mentioning that one answer is to make the C3 link itself more robust with respect to jamming, spoofing, and interference. Lots of folks are working on this already. Specific techniques are beyond the scope of this report.

4.2 Pre-Planned Mission

Prior to encountering the hostile EM environment, the radar may be queued with a set of preplanned tasks. The corresponding data products would be collected as a default mission in an autonomous fashion in the absence of override instructions from the C3 link.

This is consistent with a philosophy that the radar should always have something to do, even when neglected by the operator.

4.3 On-Board Mission Data Storage

All radar data generated during its mission should be stored in an on-board archive. While absence of the C3 link precludes real-time utilization off-board the vehicle, archived data does facilitate later non-real-time analysis such as forensic analysis. This

on-board archive might even be searchable during flight for exploitation before the aircraft lands, but after having escaped the jamming.

Furthermore, on-board intelligence might exploit this archive for subsequent analysis, such as for Coherent Change Detection (CCD), or Pattern of Life (POL) analysis.

4.4 System Cognition

The principal reason for real-time radar operation is to secure real-time information to make real-time decisions. The significance of the loss of the C3 link might be mitigated if the real-time decision process were on-board the vehicle itself, as part of the larger airborne system. This means that the larger airborne system must exhibit an ability for cognition.

In contrast to the Cognitive Radar Techniques addressed in section 2.9, here we are proposing the radar as part of a larger airborne system be capable of deciding ‘what’ to do given its mission parameters and current circumstances.

5 Conclusions

The following points are worth repeating.

- An adversary's ability to deny the utility of a radar sensor falls under the banner of Anti-Access/Area Denial (A2/AD) capability, and more specifically Electronic Warfare (EW). The universe of denial techniques are collectively described as Electronic Counter-Measures (ECM). Techniques to operate in spite of ECM are termed Electronic Counter-Counter-Measures (ECCM).

- Hardening an ISR radar system to a hostile EM environment involves addressing a number of radio links and dealing with a variety of ECM fronts. These include
  1. the radar waveform,
  2. any navigation radio receivers, and
  3. the command/control/communications links.

- A number of mitigation techniques for each of these fronts were presented and briefly discussed.

"Success depends upon previous preparation,
and without such preparation there is sure to be failure"
-- Confucius

References

[1] Merrill Skolnik, *Radar Handbook*, third edition, ISBN 978-0-07-148547-0, McGraw-Hill, 2008.

[2] Walter W. Goj, *Synthetic Aperture Radar and Electronic Warfare*, ISBN 0-89006-556-7, Artech House, Inc., 1993.

[3] X. F. Wu, DAI Da-hai, WANG Xue-song, "Study on SAR Jamming Measures," 2007 IET International Conference on Radar Systems, Edinburgh, UK, 15-18 Oct. 2007.

[4] L. Rosenberg, D. Gray, "Anti-jamming techniques for multichannel SAR imaging," *IEE Proc. - Radar Sonar Navig.*, Vol. 153, No. 3, pp. 234-242, June 2006.

[5] Armin W. Doerry, Brandeis Marquette, "Shaping the Spectrum of Random-Phase Radar Waveforms", Sandia Report SAND2012-6915, Unlimited Release, September 2012.

[6] Joseph R. Guerci, *Cognitive Radar: The Knowledge-aided Fully Adaptive Approach*, ISBN-13: 978-1596933644, Artech House Remote Sensing Library, 2010.

[7] Armin W. Doerry, "Apodized RFI Filtering of Synthetic Aperture Radar Images," Sandia Report SAND2014-1376, Unlimited Release, February 2014.

[8] Armin W. Doerry, "SAR Ambiguous Range Suppression", Sandia Report SAND2006-5332, Unlimited Release, September 2006.

[9] Mehrdad Soumekh, "SAR-ECCM Using Phase-Perturbed LFM Chirp Signals and DRFM Repeat Jammer Penalization," 2005 IEEE International Radar Conference, pp. 507-512, 9-12 May 2005.

[10] Wenqin Wang, Jingye Cai, "A Technique for Jamming Bi- and Multistatic SAR Systems," IEEE Geoscience and Remote Sensing Letters, Vol. 4, No. 1, pp. 80-82, January 2007.

[11] Brandeis Marquette, John Miller, J. Doug Jordan, Ted Kim, Armin Doerry, "SAR Image Feedback for Improved Inertial Measurement Unit Alignment", Proceedings of the 2010 IEEE Radar Conference, pp. 684-688, Crystal Gateway Marriott, Washington DC, USA, May 10 -14, 2010.

[12] Armin W. Doerry, "Estimating IMU Heading Error from SAR Images", Sandia Report SAND2009-0183, Unlimited Release, March 2009.

Distribution

Unlimited Release

1	MS 0519	J. A. Ruffner	5349	
1	MS 0519	A. W. Doerry	5349	
1	MS 0519	L. Klein	5349	
1	MS 0532	J. J. Hudgens	5240	
1	MS 0899	Technical Library	9536	(electronic copy)

Sandia National Laboratories