Risk Management Approaches to Spectrum Coexistence Assessments for Spectrum Sharing

Kalle R. Kontson
Johns Hopkins University
Applied Physics Lab
Laurel, MD, USA
Kalle.Kontson@jhuapl.edu

James (Emery) Annis
Johns Hopkins University
Applied Physics Lab
Laurel, MD, USA
Emery.Annis@jhuapl.edu

Steven Jones
Johns Hopkins University
Applied Physics Lab
Laurel, MD, USA
Steven.Jones@jhuapl.edu

Jerry Hampton
Johns Hopkins University
Applied Physics Lab
Laurel, MD, USA
Jerry.Hampton@jhuapl.edu

Howard McDonald
Defense Spectrum Organization
DISA
Annapolis, MD, USA
Howard.j.Mcdonald6.civ@mail.mil

Joy Cantalupo
Defense Spectrum Organization
DISA
Annapolis, MD, USA
Josephine.m.Cantalupo.civ@mail.mil

Anthony Rennier
Foundry Inc.
Severn, MD, USA
Trennier@foundryinc.com

Mike DiFrancisco
Virginia Tech Applied Research Corporation
Arlington, VA, USA
Mike.DiFrancisco@vt-arc.org

Mike Somerville
Peraton
Annapolis Junction, MD, USA
MSOMERVI@peraton.com

Tom Shanholtz
Peraton
Annapolis Junction, MD, USA
TShanhol@peraton.com

Donna Krizman
Peraton
Annapolis Junction, MD, USA
DKrizman@peraton.com

Abstract— **This paper addresses the application of risk-management based spectrum coexistence assessments. The legacy spectrum management tools and methods applied by the Department of Defense (DoD) are mostly designed to apply deterministic approaches to support worst-case (i.e., zero-risk) coexistence analysis and planning. This will not be adequate to enable practical coexistence in sharing scenarios, whether the sharing is cooperative or non-cooperative. This paper examines the application of a Risk Management Framework (RMF) approach to coexistence in a contested/congested spectrum environment. DoD's on-going work in the Advanced Wireless Service (AWS-3) spectrum transition is serving as a use case. Overall trends in regulation, policy and standards for analyzing and managing risk associated with entering a spectrum coexistence scenario are reviewed. It describes the use of random variables, probability density functions and cumulative distribution functions as a basis for representing the parameter space to quantify coexistence risk.**

Keywords—spectrum sharing, risk, AWS-3, RMF

I. INTRODUCTION

The Department of Defense (DoD) established a DoD Electromagnetic Spectrum Strategy that embraced and emphasized spectrum sharing as a key enabler for global operational flexibility and effectiveness [1]. This strategy has recently been echoed by federal regulators and is recognized in the push toward a National Spectrum Strategy. Spectrum policy/regulatory frameworks must evolve to enable sharing technology advances and support new agile capabilities for a more contested/congested operational environment. The DoD legacy spectrum management tools and methods are mostly designed to apply deterministic approaches to support worst-case (i.e., zero-risk tolerance) coexistence analysis and planning. This will not be adequate in the future to enable practical coexistence in sharing scenarios, whether the sharing is cooperative or non-cooperative.

In their role as a leading coexistence management tool builder, the Defense Information Systems Agency (DISA) Defense Spectrum Organization (DSO) has begun an effort to retool the existing portfolio of capabilities to add more statistical/stochastic analytics to the overall toolbox. This initiative focuses on application of a Risk Management Framework (RMF) approach to coexistence analysis. The foundation for retooling to apply RMF principles to the spectrum management domain can be attributed to overall trends in regulation, policy and standards for managing risk, to include recent IEEE publications and industry trends. The use of random variables, probability density functions (PDF) and cumulative distribution functions (CDF) has been identified as a basis for representing the parameter space for quantifying the risk of unwanted effects in spectrum sharing scenarios. Expressions of fundamental parameters embedded in our spectrum management tools for coexistence analyses (such as predicted interference power, or signal-to-interference-plus-noise ratio) are being adapted to express results as PDFs and CDFs. Through a concerted effort to apply such stochastic analysis tools, DSO is adding a whole new RMF-based toolset to the spectrum management toolbox. The end goal is to extend our ability to realistically quantify risk in the unavoidable trade-space introduced by spectrum sharing.

II. THE COMPELLING CASE FOR RMF IN SPECTRUM SHARING

Spectrum coexistence in a shared environment is analogous to driving on public roads, flying in shared air space or sailing in open waters. Everyone assumes some acceptable level of risk. Spectrum sharing is implemented and controlled by set of electromagnetic spectrum (EMS) rules of engagement. Those rules can vary widely depending on the level of control imposed by the sharing parties and the capabilities of systems operating in the spectrum. On one extreme is what might be characterized as “spectrum anarchy”, where any user can decide to use the spectrum in any way and any time without coordinating or asking permission from any other users, or obeying any rules at all. Most of us would agree that that kind of sharing does not work very well in most circumstances. On the other hand there are a variety of possible regulated and managed sharing schemes that have evolved and been proposed for an uncontested, cooperative sharing scenario. Most of these sharing schemes involve a combination of regulations and standards along with some hardware/software behaviors that together impose structured rules on all shared users. All users must agree to and accommodate an expression of confidence that the EMS rules of engagement will protect their interests to an acceptable level of risk. A key facet of EMS sharing is: **All parties to EMS resource sharing must be willing accept some risk as part of the EMS rules of engagement; otherwise, it does not work**.

The RMF-based coexistence analytics initiative is based on adopting a risk management approach to spectrum coexistence in a contested/congested environment, under the assumption that this approach yields more efficient and effective spectrum utilization. Risk of harmful electromagnetic effects can be attributed to both cooperative and non-cooperative actors including sharing among multiple DoD actors as well as between DoD and commercial actors. Whenever a shared resource is being managed, and the availability of that resource is an essential ingredient of success in system performance, there is a finite likelihood that unavailability of that resource would lead to system failure. In realistic systems engineering flawless performance is not guaranteed, and failure is always an option.

RMF principles are derived from a recognition that risk is inevitable in nearly all endeavors. The amount of risk that is considered acceptable is dependent on the consequences of failure. This relationship between consequences and likelihood of failure is captured in a Risk Matrix, as shown in Figure 1.

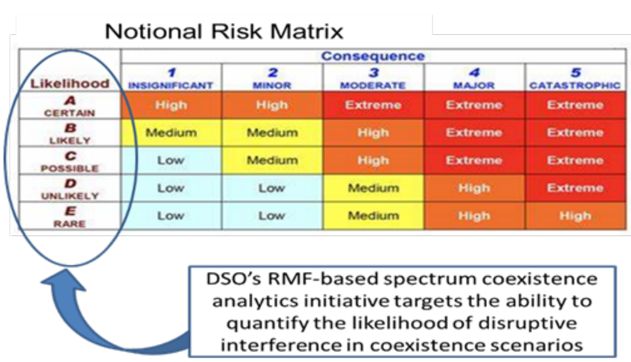


Fig. 1. RMF-based coexistence analytics are focused on the capability to quantify the likelihood that some adverse EM spectrum conditions would disrupt the performance of a spectrum-dependent system.

An underlying rationale for this initiative is that DoD system reliability has always been an issue; and risk of RF interference and outage has always been a factor in systems design, even in cases where sharing was explicitly disallowed. For a risk analysis, DoD system performance risk and required confidence levels may vary with multiple factors, such as:

- Situational factors: weather, equipment failure, RF interference, personnel availability, maintenance schedules, logistics, tactical posture, adversary condition…. and electronic/cyber attack
- Cost factors: valuation of failure; sunk cost
- Non-monetized consequences: risk to lives, strategic standing, impact on military strength and readiness

The FCC TAC Spectrum and Receiver Performance Working Group, has suggested a three step method for analyzing radio interference hazards (See "A Quick Introduction to Risk-Informed Interference Assessment" [2].)

1. make an inventory of significant harmful interference hazard modes (Defined in IEEE 1900.2) [3];
2. define consequence metric for severity of hazards;
3. assess the likelihood and consequence of each hazard

Risk is always present and the amount of risk tolerance is both variable and dependent on the situation at hand. Consequences of interference can change with the situation, and in accordance with the reasoning behind the Risk Matrix, the tolerance for risk of disruptive interference (or likelihood of harmful interference) should be adjusted accordingly.

An essential requirement for implementing RMF-based coexistence analytics is establishing a capability to quantify likelihood. Spectrum policy/regulatory frameworks are in the beginning stages of evolving to balance competing access objectives and enable sharing technology advances. The frameworks must support new agile capabilities for successful coexistence in a more contested/congested operational environment. Agility in all parameters related to coexistence posture are in play; the ability of systems and individual user equipment to adapt and adjust to coexistence conditions is most effective when the set of parameters is comprehensive. An adaptive participant in a spectrum sharing scenario is most effective at avoiding degradation due to interference when it can adjust its power, bandwidth, frequency, error correction coding, data rate, and so on. The complete set of parameters in both the physical domain and logical domain listed in IEEE 1900.2 can be applied to enhance coexistence [3].

Practically, a more limited set of parameters dominate the analysis. Regardless of how many parameters are being manipulated to achieve coexistence, the dynamics of the coexistence scenarios will demand statistical approaches. There is simply too much going on to address coexistence in a strictly deterministic manner. The tools and data sources we use to assess coexistence must have the capability to handle stochastic analytics. Products from stochastic analyses produce results such as shown in Figure 2.

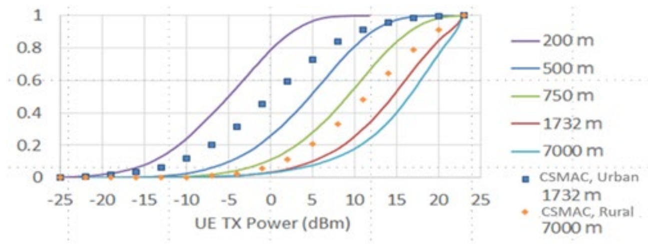


Fig. 2. Representative AWS-3 parameter analysis results: CDF showing the cummulative probability of power transmitted by LTE user equipment (UE) for sectors at various eNodeB intersite distances. [4]

In order to fit neatly into the familiar RMF instantiations, the quantified results of a stochastic analytical approach can be translated into the likelihood depicted in Figure 1, above. A key and critical distinction is that the EMS coexistence analysis **does not address consequences**. DSO's expertise and purview extends only to the question of: **how likely is it that a disruptive interference condition exists? It is not DSO's intent to determine what happens to the mission if it does exist**. Whether that disruptive interference condition has high or low consequences is determined by the operator or the commander; and the consequences are going to vary with and be dependent on the situation and scenario.

Given the increasing trend in both regulatory and commercial sectors to embrace spectrum sharing as a means to alleviate the spectrum crunch, it is imperative to equip the DoD spectrum community with RMF-based tools to perform analysis of increased fidelity involving highly complex systems. Otherwise, as is the case with any shared resource, unreasonable demands and expectations for risk mitigation will lead to inefficient and ineffective use of that resource.

III. Regulatory and Policy Underpinnings

Some of the key documents and actions that affect overall trends in regulation, policy and standards for managing spectrum coexistence risk are itemized below. This is the context for applying RMF-based coexistence analytics.

A. *Risk Management Framework (RMF) – DoD Instruction (DoDI) 8510.01, NIST Special Publication 800-37*

These documents lay out the foundation for applying RMF to maintain confidentiality, integrity, or availability of information being processed, stored, or transmitted by DoD systems. Assured spectrum access and interference risks attach to the "availability" requirement in this framework [5] [6].

B. *Regulatory Trends: FCC and NTIA*

FCC has been active in pursuing spectrum sharing actions and regulatory provisions. Among the prominent actions are the regulations for AWS-3, the Citizens Broadband Radio Services (CBRS) in the 3.5 GHz band, and multiple products from the FCC Technological Advisory Council (TAC); such as the Sharing Opportunities Working Group White Paper on Interference Limits Policy, which advocates "Risk-informed Interference Assessment" [7] [8] [2] [9] .

NTIA's Commerce Spectrum Management Advisory Committee (CSMAC) has addressed the role of risk and the use of statistical characterization in risk assessments as an essential feature of coexistence management in spectrum sharing use cases, such as DoD transition and sharing in AWS-3 bands [4].

C. *Industry Trends*

Review of industry activities demonstrates an active involvement in sharing architecture implementation: WinnForum 3.5 GHz coexistence WG, mmW mobile and FSS spectrum sharing, LTE and WiFi spectrum sharing [10].

D. *Standards Bodies*

The major standards organizations have placed spectrum sharing and risk-assessment-based coexistence squarely on the "to do" list. For example, IEEE P1900.2 embraces application of probability-based approaches, and consideration of features throughout the waveform protocol stack when assessing spectrum coexistence [3]. Similarly, 3GPP emphasizes sharing as a feature in 5G networks.

IV. Retooling to Meet the Need: Quantifying Risk in Coexistence Scenarios

The DSO RMF-based coexistence analytics initiative represents a key strategic shift in how DoD approaches spectrum resource management. The key driver for RMF-based analytics is to address the ability to quantify risk posed by variability, dynamics and aggregate effects (multiple emitters) in contested/congested EMS scenarios.

DSO has begun developing RMF-based coexistence analytics to upgrade existing spectrum management tools and apply statistical methods to the problem of spectrum management to support the DoD vision for spectrum sharing. The key is to be able determine the probability of failure (or probability of success) in achieving a measurable, quantifiable performance criterion. Spectrum management tools need the capability to quantify the level of risk associated with entering a spectrum coexistence scenario so that the risk tolerance can be modified or matched according to the consequences of spectrum-dependent system failure as a function of the situation.

DSO is working on upgrading the toolbox for analyzing and planning for coexistence among DoD systems to support the DoD vision for spectrum sharing. These tools are currently being applied to peacetime sharing scenarios, but eventually may be extended to operational use cases to enable risk-informed decisions for alternative courses of action (CoAs). Coexistence issues extend to cooperative sharing, and non-cooperative events (EW; offensive & defensive cyber ops). Developing the next generation of tools to be able to quantify the attendant risks in electromagnetic spectrum interactions can empower the spectrum community to enable Joint Electromagnetic Spectrum Operations (JEMSO) concepts and architectures.

The DoD DSO vision is to develop the tools to quantify the effect that coexisting system interference may contribute to the overall risk of test, training or operations that depend on DoD spectrum-dependent system performance; consistent with principles of RMF and IEEE P1900.2.

This approach applies the use of random variables, PDFs and CDFs as a basis for representing the parameter space, enabling the expression of the probability of achieving a specific state relative to an interference protection criterion (IPC). The approach enables us to quantify statistics for fundamental parameters used in coexistence analyses, such as aggregate interference power (I) or signal-to-interference-plus-noise ratio (SINR). Spectrum management tools are adapted to express results as PDFs and CDFs. For example, interference power is comprised of stochastic factors represented as random variables in the interference equation to accommodate the variability inherent in RF systems performance. Through mathematical relationships we can isolate and quantify the contribution of each factor to overall risk. There may be covariance among some variables; they may not be independent. The approach applies these principles to both desired and interference signals to quantify variability, and generate CDFs.

Quantifying distributions of stochastic factors allows us to develop deeper understanding of what drives interference risks. Examples of stochastic factors and the need to quantify them are:

- Measurement and test uncertainties. (E.g., probe antenna on vehicle has pattern perturbations that contribute to variability in clutter loss measurements)
- Analysis tool uncertainty: variability built into the tools
- Phenomenology of physics and physical parameters– Naturally occurring variations in physical layer properties. (e.g., propagation anomalies from atmospheric perturbations, location/time uncertainty)
- Variations in equipment characteristics – both inadvertent and by design (e.g., aging equipment, loose cables; adaptive features; dynamic and adaptable transmitter power and receiver hardware such as equipment emission or selectivity characteristics introducing variability in adjacent channel rejection)

Equation (1) represents (in its simplest form) the calculation of interfering power (***I***) based on four dominant contributing factors listed on the right-hand side of the equation. Those familiar with signal link budget analysis or interfering power calculations recognize that this expression includes the first-order factors that affect the calculation of interfering power. Each of these factors are themselves comprised of and dependent on other random variables; for example, propagation loss (Lp) can be expressed as a basic transmission loss plus an additive clutter loss, as is done in the AWS-3 analysis approach.

$$\boldsymbol{I} = Pt - Lp + Gr - FDR \qquad (1)$$

I = predicted interfering signal level at the DoD receiver input from an interfering source, dBm

Pt = interfering transmitter effective isotropic radiated power (EIRP), dBm

Lp = interference path propagation loss (including effects of clutter) between a modeled UE and a DoD receiver, dB

Gr = victim receiver antenna gain (expressed as a value in the direction of the interferer transmitter), dBi

FDR = Frequency Dependent Rejection (applied to quantify the effect of off-tuned interference, such as adjacent channel rejection), dB

Each term is a factor that has some variability… some more, some less. The end goal of the RMF approach to coexistence analytics is to express each of these factors as a random variable, and enable the expression of them as PDFs and CDFs.

Each term may also be comprised of quantifiable random sub-factors. Figure 3 depicts a tree structure of random variables that comprise and contribute to an overall metric of system performance, such as interference power at a receiver (as represented in Equation 1). Each factor can be comprised of multiple contributing sub-factors, each with its own statistical characteristics. There may be covariance among some variables; they may not be independent. The figure illustrates this concept by depicting the adjacent channel rejection performance as a function of separate transmitter and receiver bandwidth distributions, each of which are essential ingredients for calculating FDR, which in turn is the parameter that determines the value of adjacent channel rejection for any one specific set of bandwidth conditions. Each of these sub-factors can have its own PDF based on the adaptive or dynamic signal processor behaviors exhibited by the interfering transmitter and the victim receiver.

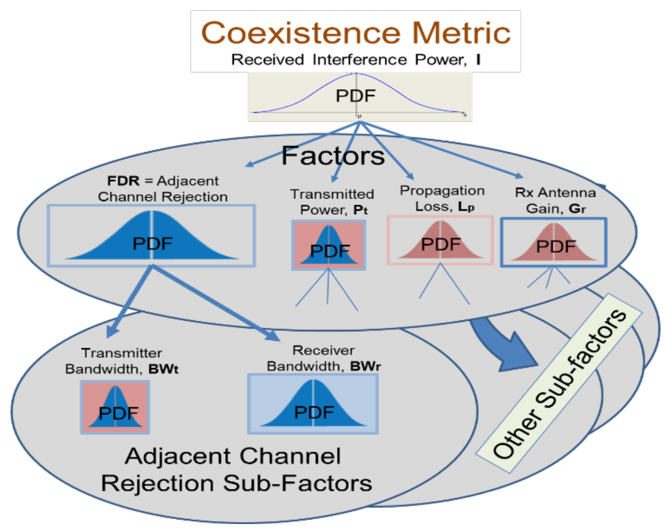


Fig. 3. Notional tree structure of statistical factors and sub-factors (shown as PDFs) comprising and contributing to the overall PDF depicting the interference power at a receiver.

If the distributions are known to the sub-factor level, we can bundle and unbundle them to express the factors and sub-factors as random variables thus increasing the fidelity of the RMF-based analysis. For example, we can apply the math of convolution and de-convolution to isolate and quantify the contribution of each to the overall risk, and solve for unknown distributions by knowing the composite effect (such as that derived from measured data). [See figure 4]

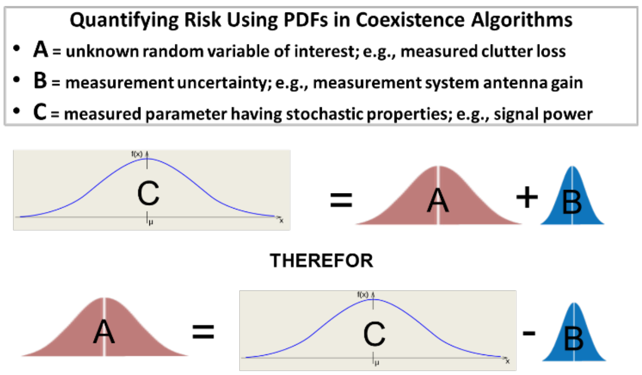


Fig. 4. Analyzing risk through the use of random variables and PDFs allows a mathematically tractable approach to isolating and quantifying the effect of contributing factors to overall risk

When this approach is applied to defining a PDF representing the probability of meeting a performance criterion of the coexisting system, this mathematical technique can allow an in-depth understanding of what features and factors are contributing most meaningfully to the statistical expression of overall system performance. For example, if the contributions from clutter variability indicate the widest distribution (largest variance) of all the contributing factors, then we know that it is the physical environment uncertainty that dominates the variability in performance. On the other hand, if the transmitter power variance is larger for a system incorporating dynamic, adaptive power control, then we know that it is a system hardware feature that contributes most to the uncertainty. One of those (clutter) we cannot easily control; the other we can. Such results provide insight to the ability to manage risk.

V. RMF Approach Applied in the AWS-3 Spectrum Transition Program

The DSO approach applied in the AWS-3 spectrum transition program is a real-world example of applying the RMF-based coexistence analytics. AWS-3 transition team developed and used tools and methods to analyze, measure, and assess operations that enable spectrum sharing between DoD and commercial wireless operations in the recently auctioned 1755 to 1780 MHz band. Deterministic tools are used to address factors that are predictable and do not substantially contribute to the uncertainty and variability of the outcome. Stochastic tools are applied for the wandering factors; i.e., those that have inherently variable behaviors due to dynamics or sheer numbers of players. For practical reasons, the number of variables that are represented as random variables is limited.

The AWS-3 spectrum sharing program has served as an incubator for development of the foundation for the RMF-based approach, and also offered us an opportunity to apply and exercise the principles on a real-world problem. The program has been unique and has inspired creative development for many reasons, some of which are:

- AWS-3 presents a technical challenge involving the issues and interactions that are most amenable to RMF-based coexistence analytics; in essence, the need to address aggregate effects, dynamics and variability in multiple domains (spatial, frequency, time, and logical)
- The program has well-organized and well-resourced tasks that advance the science of spectrum coexistence at a time when new approaches are most needed
- FCC AWS-3 rulings provide a regulatory underpinning that clearly and unambiguously articulates the need to share spectrum and resolve the unavoidable pressure to transform contention into cooperation
- The program enjoys exceptional cooperative teamwork across DoD organizations, NTIA organizations, contractor participants and commercial licensees, vendors & carriers

Details of the analytical and measurement approaches are provided in separate papers and will not be repeated here. What is worth mentioning is the summary of the outcome. The initial instantiation of a risk analytics approach in the AWS-3 context has led to some noteworthy accomplishments:

- Supported the electromagnetic spectrum sharing rules of engagement with quantifiable risk analyses
- Has established credibility with the sharing community of interest; reluctance transformed to acceptance, and then was followed by active participation and contributions to make it work
- Launched a retooling effort consistent with trends in regulatory and standards bodies
- AWS-3 has exposed and illuminated the value and need to extend statistical treatment of parameters to a comprehensive set, as described in preceding sections
- Establishes coexistence framework consistent with DoD-mandated RMF approach to systems acquisition policy and realistic mission impact assessment

VI. Modeling & Simulation Results

A prototype model of aggregate interference was developed by the DSO. The model was applied to a hypothetical scenario in order to exercise and demonstrate the methods of RMF based spectrum analysis and illustrate the value in terms of spectrum resource utilization efficiency. The model relates the variability in system equation parameters to the risk of exceeding a given IPC. The analysis presented here has been based on work performed on AWS-3 allocation of commercial LTE tower locations in the 1755 to 1780 MHz bands sharing spectrum with a DoD airborne asset, designated as the System Analysis Record (SAR). In this analysis, the hypothetical DoD airborne incumbent operates at a specific point within an operational area and is co-channel with hypothetical commercial LTE deployments which are licensed based on Bureau of Economic Analysis (BEA) areas. Figures 5 and 6 illustrate the hypothetical scenario wherein the UEs surrounding the SAR location would introduce some level of aggregate interference to the SAR receiver.

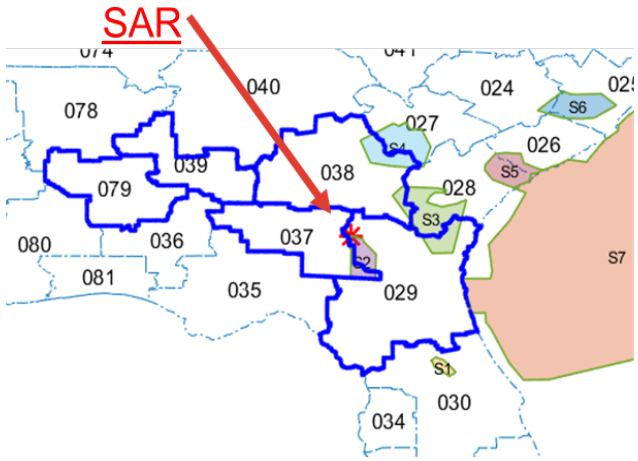


Fig. 5. Scenario depicting BEAs surrounding a DoD airborne communications asset System Analysis Record (SAR) operating cohannel with the LTE UEs. Blue outline depicts the boundary of each BEA, and the red asterisk depicts hypothetical location of the SAR.

In this analysis, the DoD is presumed to define a possible set of IPCs expressed as a SINR required for each of a set of possible operating modes. The desired signal (S) is expressed as a random variable, and the value of aggregate interference (I) is calculated as random variable. The stochastic factors contributing to aggregate interference are the clutter loss component of propagation, and the UE Effective Isotropic Radiated Power (EIRP). PDFs were generated for each of these random variables to enable the application of a Monte-Carlo analysis tool. The aggregate co-channel interference is a function of the UE's transmit power minus the various propagation & clutter losses, FDR and antenna gain. (See equation (1)).

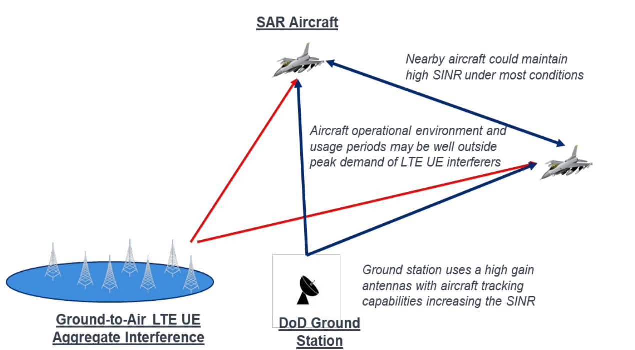


Fig. 6. Scenario depicting SINR calculations. Blue lines are desired signal paths, and red lines are aggregate interference paths.

The Monte-Carlo simulation is used to quantify the aggregate interference between all UEs in each BEA and the DoD SAR located in a protected operational region. A fixed number of hypothetical LTE sectors and their locations were used for analysis along with an assumed fixed number of 6 UEs per sector, with three sectors per tower. For this paper, the results are depicted for each BEA of interest. Variability was introduced in each Monte-Carlo trial by drawing UE transmit EIRP values from two PDFs, each representing transmitters located in either rural or urban areas (corresponding to the serving tower location). Increased variability was introduced by drawing the clutter loss value from a PDF of values for either urban or rural areas. The simulation computes the values of signal and aggregate interference as random variables (expressed as a PDF or CDF) from all sectors within the BEA to determine if it falls below the chosen DoD IPC threshold.

Some sample results are shown in Figures 7 and 8. In Figure 7, the set of graphs show the results the potential effect of truncating the maximum allowable transmit power of the UE transmitters by as much as 10 dB in each BEA assuming required value of 90% confidence in achieving a given IPC (in this case, a SINR). The hypothetical DoD receiver has multiple operating modes and can operate at a SINR as low as ~6 dB by using lower-order modulation and robust error correction, thus trading throughput for resilience. Under these conditions, some BEAs can meet the 90% confidence level without any truncation, one can meet the SINR requirement by truncating at 15 dBm, and two of the BEAs can only meet the SINR by resorting to other measures, such as removing some of the sectors associated with the towers closest to the SAR or truncating below 13 dBm, or a combination thereof.

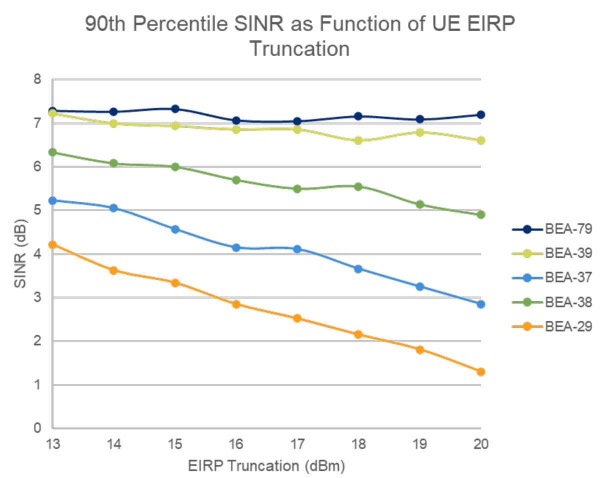
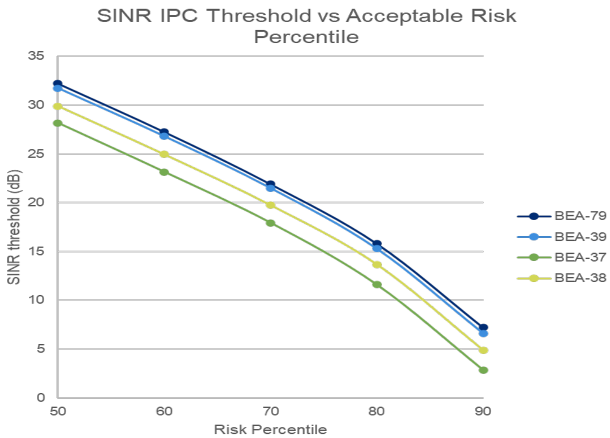


Fig. 7. SINR calculations to illustratee the effect of truncatiing allowabkle UE transmitter power for each BEA assuming a required value of 90% confidence for achieving a given SINR at a DoD SAR location.

In Figure 8 the script is flipped. The trade-space being addressed is the effect of a choice of a required confidence level on the ability to employ higher order modulation (e.g., 256 QAM) along with minimal error correction). The DoD system can achieve maximum throughput, but at the cost of much higher SINR requirements to achieve the acceptable bit-error-rate (BER), and a correspondingly lower confidence to achieve that SINR IPC.



$$P(SINR > SINR_{threshold}[dB]) = [50, 60, 70, 80, and\ 90]\%$$

Fig. 8. SINR calculations to illustrate the effect of varying acceptable confidence to achieve a given SINR at a DoD SAR location.

In the AWS-3 use case, the modeling and simulation first computes the aggregate interference from all tower sectors to determine if it falls below the chosen DoD IPC threshold. If it does not, sectors associated with towers posing the worst interference threat are removed one by one until the total aggregate interference falls below the IPC threshold. Such results yield sectors that are allowed to remain in the BEA region to meet regulatory compliance under specific conditions. Thus, the percentage of active sectors can be used as a proxy for sharing effectiveness and efficiency. By requiring zero risk and setting parameters to worst-case conditions the percentage of towers that must be removed is large resulting in inefficient use of auctioned spectrum. This analysis is unrealistic. Instead, the ability to quantify the risk associated with varying multiple parameters (not just removing sectors) can be applied to explore a larger landscape of the overall trade-space for managing coexistence. For example, in one of the hypothetical excursions applied in the DSO prototype model, the number of sectors removed was reduced over 50% by truncating UE EIRP at 15 dBm while maintaining a 90% confidence level.

VII. Application of the Principles to Operational Settings; Technical Philosophy & Strategy

The AWS-3 approach to establishing the rules for co-existence in a spectrum sharing environment is largely governed by regulatory provisions and methods developed collaboratively by the DSO, the NTIA, the Service spectrum management community and the commercial carriers. As such, it has been a successful application of science and technology to enable a specific exemplary spectrum sharing experience in the AWS-3 spectrum. But the methods developed in this effort have also pointed the spectrum community in the direction of a generalized set of principles and methods to address the spectrum coexistence by applying stochastic analytics to quantify risk.

Tools that can quantify risk as a function of technical parameters expressed as random variables can be applied in multiple ways. Two obvious application scenarios are:

- Use of the tools to work backward from a required reliability level to identify the critical set of parameters and conditions/settings to achieve a confidence level. This is what is being done in the AWS-3 analyses.
- Use of tools to quantify the risk (probability of failure or success) to support operational decisions among alternative CoAs. For example, whether to jam a target or intercept the target's transmissions. One of those CoAs may have a higher probability of success, and that would be good to know.

The current climate within the spectrum policy and regulatory community is conducive to investment in new approaches. Developing the next generation of tools to be able to quantify the attendant risks in EMS interactions can empower the spectrum community to answer questions posed by proponents of Joint Electromagnetic Spectrum Operations (JEMSO) concepts and architectures [11]. Translating dBs into expressions of mission risk and effectiveness has appeal and value. Coexistence issues include cooperative sharing, and non-cooperative events (EW; offensive/defensive cyber ops).

Nowhere does the idea of risk management ring more true than in active military operations. In the battlefield, it is rare when everything goes as planned; perfectly and without disruption. The future battles will be characterized by a frightening mix of cyber measures, countermeasures and information-rich systems combined with more conventional battlefield weaponry. Decisions play out within that trade-space to determine whether to launch missiles, fire mortars, or send a squad to destroy an adversary, or perhaps jam an adversary's spectrum. Knowing the risks and probabilities of success in making those decisions is advantageous.

VIII. Conclusions

DoD RMF-based coexistence analytics capabilities will support EMS sharing. RMF-based coexistence analytics can:

- Support the electromagnetic spectrum sharing rules of engagement with quantifiable risk analyses
- Quantify risk to benefit planning & operations in contested/congested DoD spectrum environments
- Establish credibility with the sharing community by applying coexistence tools consistent with DoD RMF approach to systems management, regulations & standards, and realistic mission impact assessment
- Increase spectrum utilization efficiency and reduced risk in EMS sharing scenarios

References

[1] DoD, "DoD Electrommagnetic Spectrum Strategy: A Call to Action," DoD, 2013.

[2] FCC, "FCC Technological Advisory Council - Report--spectrum & receivers working group," FCC, 2015.

[3] IEEE, "P1900.2 - IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence Between Radio Systems," IEEE , New York, 2008.

[4] NTIA, "“Commerce Spectrum Management Advisory Committee (CSMAC) Working Group 3 (WG 3) Report on 1755-1850 MHz

Satellite Control and Electronic Warefare”," [Online]. Available: https://www.ntia.doc.gov/publications ..

[5] DoD, DoD Instruction (DoDI) 8510.01, DoD, 2017.

[6] NIST, NIST Special Publication 800-37-Guide for Applying the Risk Management Framework to Federal IT Systems, NIST, 2012.

[7] FCC, "Report and Order - Rules with Regard to Commercial Operations in the 1695-1710 MHz, 1755-1780 MHz, and 2155-2180 MHz Bands," FCC, Washington, DC, 2014.

[8] FCC, "Report and Order and Second Further Notice of Proposed Rulemaking - Citizens Broadband Radio Service for shared wireless broadband use of the 3550-3700 MHz band," FCC, Washington, DC, 2015.

[9] J. P. De Vries, "Risk-Informed Interference Assessment: A Quantitative Basis for Spectrum Allocation Decisions. Forthcoming, Telecommunications Policy," SSRN, 2017.

[10] WinnForum, "Wireless Innovation Forum - https://www.wirelessinnovation.org/," 2019. [Online]. Available: https://www.wirelessinnovation.org/.

[11] DoD, "Joint Doctrine Note 3-16, Joint Electromagnetic Spectrum Operations," DoD, 2016.