SPaRC

Secure Pathways for Resilient Communications

7-8 GHz Point-to-Point Testing: Summary

October 2024

7-8 GHz Point-to-Point Testing: Summary
October 2024

This work was conducted by the Idaho National Laboratory (INL) for the Department of Energy (DOE) Office of Electricity (OE) Secure Pathways for Resilient Communications (SPaRC) program.

OE Project Sponsor:	David Wells
INL Project Lead:	Robert Comstock
INL Project Co-Lead:	David Wallis
INL Technical Advisor:	Nicholas Kaminski
INL Lead Engineer:	Azim Muqtadir
INL Relationship Manager:	Brad Nelson

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC.

Key Takeaways

- Under the scenarios we tested, we found interference to our microwave link that would be detrimental to grid operations. For example, Wi-Fi signals with power levels approximately 100 times lower than the microwave signals at the receiver cause the microwave link to be inoperable.
- Traditional methods of analysis that focus on simulation miss important aspects of interference. Over-the-air testing shows that simulation can be an order of magnitude off when estimating the interference levels that impact microwave links. Efficient spectrum policy needs to validate simulation with over-the-air testing.
- Relying on reports from the field of interference for spectrum management generate a false sense of success. Current equipment metrics do not provide enough clarity for when or how much interference impacts operations. In our testing, the bit error rate metric resets to show zero errors once the link has failed.
- Spectrum sharing is feasible when based on a disciplined, scientific and data driven methodology.

Project Motivation

Microwave technology is vital to the reliability, resilience and security of the nation's electric power and other critical infrastructure. Disruptive interference to microwave systems used for critical infrastructure poses a significant risk to our nation's security.

Microwave technology has played a significant role in the electric utility industry, particularly in the context of electric grid control and communication since the 1950s. From the 1950s through the 1990s, microwave communications evolved to become an integral part of electric grid management, supporting SCADA and teleprotection systems which rapidly isolate faults to protect grid infrastructure. In the 1990s, the rise of smart grid technologies increased the demand for robust communications systems supporting advanced applications. Due to this demand, microwave usage increased to support continuous grid operations between remote grid components and central control centers. Over the last two decades, real-time data analytics further emphasized the importance of reliable microwave communications channels, especially for remote or rugged area where physical cabling is impractical.

Prior to the 2020s, electric utilities and other critical infrastructure providers relied on dedicated (licensed) spectrum in the 5.925-7.125 GHz band to protect against potential interference. In 2020, the Federal Communications Commission (FCC) repurposed the 5.925-7.125 GHz spectrum for unlicensed users allowing for Wi-Fi and other users to utilize this band applying modeling and simulation for evaluating potential interference. To our knowledge, limited scientific, empirical, over-the-air field testing was conducted prior to the implementation of the repurposing. This FCC repurposing has increased the risk of interference to the critical infrastructure provider.

The NTIA is now studying 3.5-24 GHz but specifically the 7.125-8.400 GHz band to expand its usability. To provide more scientific, empirical data for this evaluation, the Department of Energy, Office of Electricity (DOE-OE) requested INL to conduct a transparent modeling, simulation, and over-the-air interference evaluation of a representative electric utility system utilizing long distance microwave communications. With the given representative system, DOE-OE requested INL to evaluate interference thresholds for Wi-Fi and cellular (i.e., 5G) devices.

Overview

Wireless spectrum is a limiting resource for continued economic growth in the United States. As discussed in the recent National Spectrum Strategy (NSS), wireless spectrum underpins several aspects of the U.S. economy and the demand for additional spectrum is driving the need for realizing spectrum sharing to enable continued development. At the same time, wireless spectrum is an essential foundation of critical energy infrastructure, including electric, oil, and natural gas resources. In particular, wireless point-to-point (P2P) links (a.k.a microwave links) are the backbone of vast infrastructure networks that enable the flow of sensor and control information needed to manage critical energy sector infrastructure in the United States. These links will only become more important as the energy sector incorporates more diverse sensing and more efficient control mechanisms, which increases system complexity and data volume requiring more resilient communications. Therefore, the continued economic development of the U.S. depends on determining novel approaches to spectrum management that balance both broad access for advanced wireless technologies and resilience for critical infrastructure.

Here, we support balancing the competing needs outlined above by providing scientifically grounded data on potential interference to critical energy sector P2P links in a co-mingled sharing scenario. We focus on over-the-air testing of commercial off-the-shelf transmitting equipment to ensure that our project captures the large variety of factors that influence the impact of interference in real-world settings. First and foremost, our efforts demonstrate that co-mingled spectrum sharing generates interference that renders critical P2P links inoperable when the approach to sharing prioritizes broad access to spectrum. Secondly, we note that simulation based examinations of interference are prone to errors leading to either under estimation or over estimation of interference impacts. Thus, simulation centric approaches are limited in their ability to balance protection of critical links against utilization of potential spectrum. Finally, our results show that effective management of spectrum sharing must extend beyond reported interference events. The identification and attribution of interference is impractical for two major reasons: (1) the large variety of environmental, geographical, and electromagnetic factors that influence communications performance and (2) limitations of metrics in commercially available equipment to monitor links. This study examines commercial off-the-shelf P2P equipment to identify potential issues in co-mingled spectrum sharing that goes beyond limitations in simulation and improves the identification of interference.

This project is an exploratory examination of co-mingled spectrum sharing in the 7 GHz band (7125 - 8400 MHz) and the potentially associated interference. This work is largely inspired by the recent opening of the 6 GHz band (5925 - 7125 MHz) to unlicensed, co-mingled sharing. In the case of the 6 GHz band, the FCC primarily considers simulation centric approaches to understand potential interference which generally minimize the concerns of the critical infrastructure community. [1] [2] We believe that an approach that validates simulation with over-the-air testing provides a holistic picture of the nuances of spectrum sharing. This builds a solids foundation for policy makers to represent the needs of all spectrum stakeholders. Therefore, we focus on open-range, over-the-air testing as the central component of our data collection. This allows us to characterize the conditions necessary for representative interferers to impact critical energy sector P2P links. We transparently describe our approach, our results including data, and the conclusions that we draw in our main report. Together, this work is intended as a foundation to facilitate policy makers taking a data driven approach to designing spectrum sharing strategies in the 7 GHz band that extracts maximum utility from the spectrum while continuing to support the resilient operation of critical energy sector infrastructure.

Approach

Our testing is designed to collect defensible, empirical, objective, quality data from a representative deployment of a P2P link in the presence of representative interference signals. We accomplish this primarily through the open-range, over-the-air testing of commercially available equipment in forward leaning representative spectrum sharing scenarios. [3] Our approach considers four potential interferers: (1) 5G, (2) Wi-Fi, (3) additive white Gaussian noise (AWGN), and (4) continuous wave (CW). We generated the 5G and Wi-Fi interferers using commercial off-the-shelf equipment up-converted to the 7 GHz band. [4] We examine these against a test P2P link deployed on our range with a link length typical of operational P2Ps links in the 7 GHz band. We consider three main use cases for a P2P link: (1) maximum data rate regardless of latency, (2) low data rate with low latency, and (3) medium data rate with medium latency. [5]

We conduct simulation studies in support of our over-the-air testing. We use these studies to select

[1] *FCC 20-51: Report and Order and Further Notice of Proposed Rulemaking.* Tech. rep. Federal Communication Commission, 2020.

[2] *FCC CIRC2310-04: Second Report and Order, Second Further Notice of Proposed Rulemaking, and Memorandum Opinion and Order on Remand.* Tech. rep. Federal Communication Commission, 2023.

[3] Section 6 of the main report provides details about of our open-range testing.

[4] See Section 2.2.3 in the main report for details about our approach to interference generation.

[5] Section 2 of the main report discusses the equipment used to realize the components of our testing in detail.

locations and parameter settings intended to explore impacts to the P2P link from various locations. We begin location selection by ensuring that we can deploy a P2P link that uses commercial equipment and operating at a typical link length without terrain obstructions. We then select interferer sites that provide clear line-of-sight to our P2P endpoints into a variety of P2P varying locations for location diversity. [6] We then calculate how much signal we will loose between the selected locations. This allows us identify how much power the interferers will need to disrupt the P2P link. We call this the interference to signal ratio (ISR) in our report. This ratio gives us critical values that indicate how much power we need to generate from the interferer to noticeably impact the P2P link. [7] Table 1 displays these predicted receive ISR threshold.

Table 1: Predicted Threshold Received ISR for each P2P paradigm

Operational Paradigm	**Critical Ratio**
Low-Rate	-1.5 dB
Mid-Rate	-15.5 dB
High-Rate	-35.0 dB

Detrimental Interference

Our results demonstrate that co-mingled spectrum sharing generates interference that renders critical P2P links inoperable for a range of situations. In particular, we see the interference signals that cause the most disruption also the most difficult to regulate. If this band is opened up to unlicensed usage and the equipment is deployed and maintained by the general public the enforcement of regulatory policies is costly and limited. This places the regulation burden on the incumbent energy sector users forcing them to identify when interference is occurring and request enforcement. Importantly, only a small amount of interference power is required to render critical P2P links inoperable relative to the level of the P2P signal. Figure 1 shows that P2P links operating within the mid-rate paradigm can no longer transfer any packets when the received interference power reaches a level approximately 100 times lower than the received level of the intended signal (i.e., when the received ISR is -20 dB). Figure 2 shows that high-rate P2P links are inoperable with received interference powers more than 31,500 times lower than the intended signal (i.e., received ISR of -45 dB). These levels are readily achieved by commercially available equipment. [8]

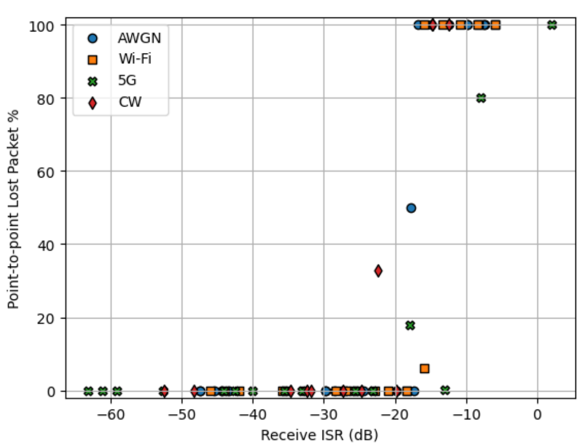

Figure 1: Average Lost Packet Percentages in Mid-Rate Link for all Test Sets

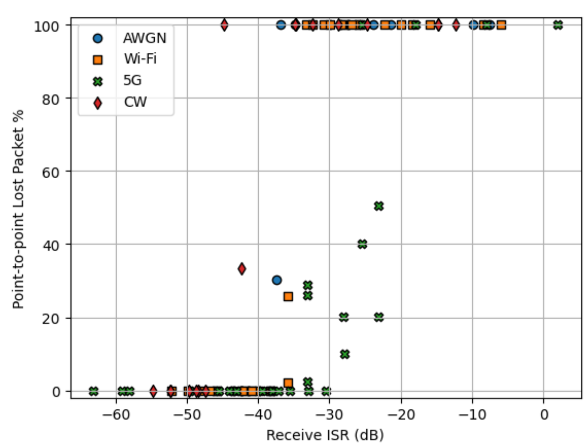

Figure 2: Average Lost Packet Percentages in High-Rate Link for all Test Sets

[6] See Section 3 of the main report for details about our site selection approach.
[7] Section 4 of the main report discusses the loss simulation and link budget analysis in detail.
[8] Section 6.3.2 provides additional discussion of the interference demonstrated in our testing

Limitations of Simulation

This project demonstrates that simulation centric investigation of interference is prone to errors that lead to miss-characterization of interference. This is shown by comparing the interference impacts predicted by standard simulation approaches verses the impact observed in over-the-air testing. Table 1 provides predicted levels for impactful interference and Table 2 displays the measured ISR values where we begin to see impact from each interferer type on each P2P paradigm. [9] In some cases simulation significantly under predicts the impact of interference. For example, the CW interferer impacts the high-rate paradigm at power levels an order of magnitude lower than predicted (i.e., the predicted receive ISR threshold is 9.8 dB higher than the observed receive ISR threshold in this case). In other cases simulation significantly over predicts the impact of interference. For example, the 5G interferer only impacts the high-rate paradigm at power levels an order of magnitude higher than predicted (i.e., the predicted ISR threshold is 9.5 dB lower than the observed ISR threshold). These results highlight the importance of particular sensitivities and factors that are often overlooked or difficult to represent in simulation.

Table 2: Observed Threshold Received ISR for each Interferer Type

P2P Paradigm	P2P Link Modulation	Interferer Type	Threshold Rx ISR
Low-Rate	QPSK	5G	-2.5 dB
Mid-Rate	64 QAM	5G	-8.0 dB
Mid-Rate	64 QAM	AWGN	-16.8 dB
Mid-Rate	64 QAM	CW	-14.8 dB
Mid-Rate	64 QAM	Wi-Fi	-15.9 dB
High-Rate	4096 QAM	5G	-25.5 dB
High-Rate	4096 QAM	AWGN	-36.8 dB
High-Rate	4096 QAM	CW	-44.8 dB
High-Rate	4096 QAM	Wi-Fi	-33.3 dB

Interference Identification

Our results show that effective management of spectrum sharing can not only rely on reported interference events. This results from the impracticality of identifying or attributing interference during the ongoing operation of critical P2P links. [10] We identify two underlying reasons for this impracticality in our work: (1) a large variety of factors that influence communications performance (such as weather and other atmospheric conditions) and (2) limitations of interference focused metrics in equipment.

This work highlights that P2P links are part of a broader, complex communication system whose performance depends on the interaction of several components. Communication performance depends in part on the interaction of several system components. [11] Additionally, the link performance itself is influenced by a variety of factors from regular atmospheric fluctuations to nuances in equipment implementation. [12]

The metrics provided by commercially available P2P equipment are limited in their ability to identify interference. This stems in part from confusing P2P metric behavior such as metrics that reset to show no degradation after a certain threshold of harm. [13] While the metrics are useful for establishing the P2P link initially, they are less helpful when being reviewed to determine how much interference is being received.

Figure 3 displays the bit error rate (BER) return to zero behavior for a mid-rate P2P case. Figure 4 shows the average packet lost percentage for the same case. Considering the impact of the Wi-Fi interferer, show by the square in the figures, we see that the reported BER resets to zero after an ISR of -14 dB but the average lost packet percentage continues to rise. Further, the narrow transition between a completely

[9] Section 6.3.2 of the main report discusses these results in detail.

[10] Section 8.3 of the main report shows that identifying interference is non-trivial in practice.

[11] Section 6.2.4 of the main report discusses errors that can arise from the interaction between applications and the P2P link supporting them.

[12] Section 6.3.4.2 of the main report highlights significant variability in link performance that is independent from interference.

[13] Section 6.3.4.1 of the main report discusses a specific example of this resetting behavior.

unaffected link and a completely inoperable one limits the time available to observe interference. [14] In many cases, interference invisibly pushes the P2P link closer to the threshold of significant degradation.

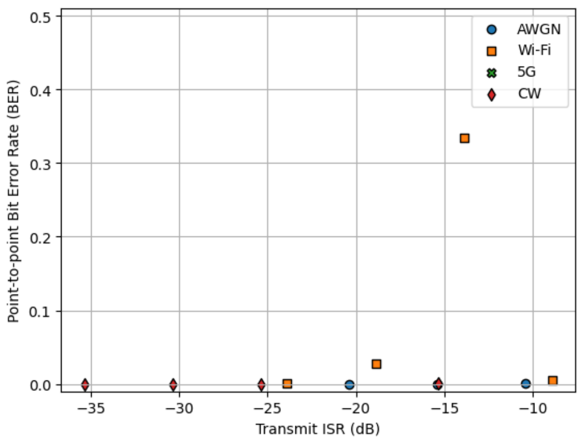

Figure 3: Average BER Mid-Rate Case

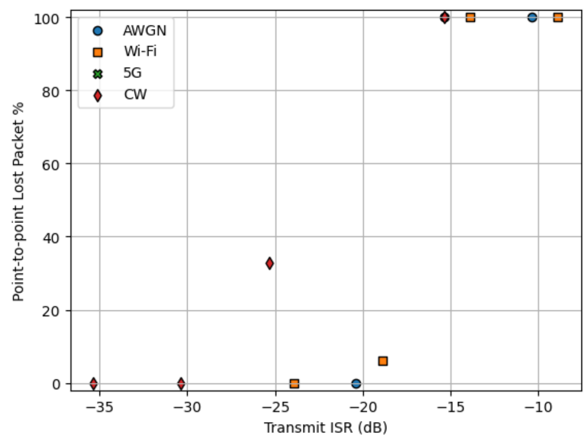

Figure 4: Average Packet Loss % Mid-Rate Case

Part of the limitation in identifying interference results from the lack of information about the operation of the error correction mechanism of the P2P receiver. [15] We note that exposing metrics that provide near real-time information about the error correcting mechanism would improve the visibility of signal degradations. Monitoring signal degradation with this expanded visibility would better support the identification of potentially bursty interference events.

A Path Toward Sharing

Given our intention to provide a foundation to data-driven spectrum policy making, we also extend our over-the-air results to support geographic based policies. We apply simulation to predict the geographic regions where interferers are likely to meet or exceed the threshold interference power to impact P2P links. The simulation demonstrates an approach to applying over-the-air testing results to expanded planning uses. In particular, we show the impact regions implied by the open-range test results, per interferer type and P2P paradigm combination. These regions highlight the variable impact of interferers on different P2P paradigms. Further, theses maps account for both antenna patterns and terrain effects to illustrate the geographic regions of concern for P2P protection. Figure 5 shows an example impact region for a 5G interferer at 30 ft. [16]

[14] Section 8.4 of the main report discusses the transition from unaffected to inoperable.
[15] Section 9.3 discusses the lack of visibility into the error correction mechanism.
[16] Section 7 of the main report discusses the determination of geographic impact regions in detail.

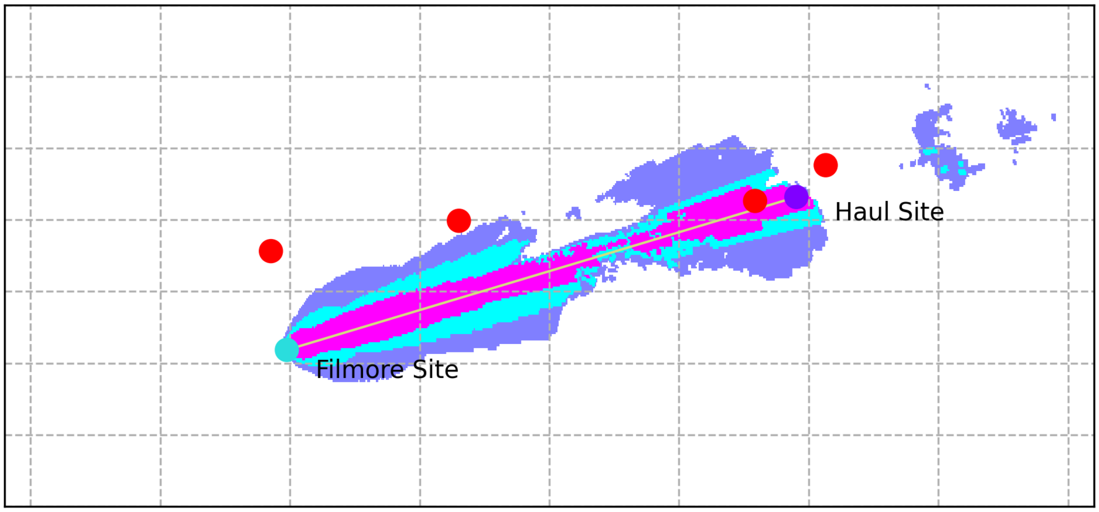

Figure 5: Sensitivity of Low-Rate Link Received at Filmore to 5G at 30 ft

This project takes a forward leaning approach to inform emerging spectrum policy with empirical data about the impact of interference on critical energy sector links. Ensuring that spectrum policy considers this impact is increasingly important as energy sector P2P links must provide increasing levels of performance and resilience at the same time that spectrum policy is increasingly turning toward spectrum sharing to meet growing spectrum demand.