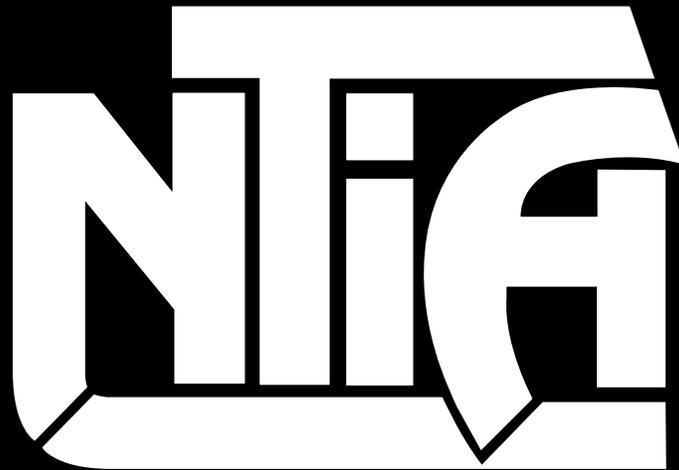


Emission Measurements of a Contraband Wireless Device Jammer at a State Prison

Frank H. Sanders
Geoffrey A. Sanders
John E. Carroll



report series

Emission Measurements of a Contraband Wireless Device Jammer at a State Prison

**Frank H. Sanders
Geoffrey A. Sanders
John E. Carroll**



U.S. DEPARTMENT OF COMMERCE

September 2019

DISCLAIMER

Some technical information regarding the wireless device jammer that NTIA measured may be considered intellectual property by the manufacturer of the device. Jammer device description, operational parameters, and measured emissions are provided to document the spectrum impact of the device that was measured. The device that is described herein has not been FCC-certified, nor does a certification standard for such a device exist.

Some test and measurement equipment are identified in this report for the purpose of comprehensively describing the methodology and results of the work that NTIA performed. Such identification does not imply endorsement by the Department of Commerce of the equipment so identified, nor does such identification imply that the equipment was the only possible choice for adequate performance of such work.

ACKNOWLEDGMENTS

The authors thank the Department of Justice's Bureau of Prisons, and especially Mr. Todd Craig, for coordinating the use of the Broad River Correctional Institution at Columbia, South Carolina, where the measurements described in this report were performed. Mr. Brian Sterling, the head of the South Carolina Department of Corrections, is likewise thanked for his assistance and support in making that facility available for this work.

CONTENTS

	Page
Acknowledgments.....	v
Figures.....	viii
Tables.....	xi
Abbreviations/Acronyms.....	xii
Executive Summary.....	xiii
1. Introduction.....	1
1.1 Objective.....	2
1.2 Considerations of Jammer Effectiveness Against Contraband Wireless Devices and Potential for Harmful Interference to Licensed Radio Services.....	2
1.3 Approach.....	4
2. Jammer Description and Installation.....	6
2.1 Jammer Electrical Characteristics.....	6
2.2 Measured Jammer Power as a Function of Measurement Bandwidth.....	8
2.3 Targeted Jamming Space.....	8
2.4 Jammer Installation and Effective Isotropic Radiated Power (EIRP).....	9
3. Measurement Description.....	10
3.1 Measurement System Hardware and Software.....	10
3.2 Measurement System Parameters.....	11
3.2.1 Measurement Frequency Bands.....	11
3.2.2 Measurement Bandwidths.....	11
3.2.3 Peak Detection Mode.....	12
3.3 Spectrum Analyzer Preamplifier and Thermal Noise Limit.....	13
3.4 Measurement Procedure.....	13
4. Measurement Results.....	15
5. Data Analysis.....	28
5.1 Jammer Signal Relative to CMRS Signals.....	28
5.2 Emissions in Defined Jammer Operational Bands.....	28
5.3 Peak Detected Jammer Power as a Function of Receiver Bandwidth (Peak Detected Bandwidth Progression Rate).....	28
6. Summary.....	30
7. Conclusions.....	31
8. References.....	33
Appendix A . Jammer Emissions Measured in 1 MHz Bandwidth.....	35

FIGURES

	Page
Figure 1. Jammer LFM behavior. The complete chirp sequence, across all bands, was repeated every 40 microseconds. Frequencies are plotted to a non-fixed scale.	7
Figure 2. The Broad River jammer installation top view, approximately scaled. Seven jammers were spaced every other cell, in utility shafts, on each of two floors. Only one jammer on the ground floor was operated for the measurements.	9
Figure 3. Block diagram schematic of the jammer emission measurement system used at Broad River Correctional Institution.	10
Figure 4. M4 statistics, jammer on, 723-763 MHz, inside targeted prison housing block.	16
Figure 5. M4 statistics, jammer off, 723-763 MHz, inside targeted prison housing block.	16
Figure 6. M4 statistics, jammer on, 860-900 MHz, inside targeted prison housing block.	17
Figure 7. M4 statistics, jammer off, 860-900 MHz, inside targeted prison housing block.	17
Figure 8. M4 statistics, jammer on, 1920-2000 MHz, inside targeted prison housing block.	18
Figure 9. M4 statistics, jammer off, 1920-2000 MHz, inside targeted prison housing block.	18
Figure 10. M4 statistics, jammer on, 2090-2170 MHz, inside targeted prison housing block.	19
Figure 11. M4 statistics, jammer off, 2090-2170 MHz, inside targeted prison housing block.	19
Figure 12. M4 statistics, jammer on, 723-763 MHz, outdoor location O-1.	20
Figure 13. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.	20
Figure 14. M4 statistics, jammer on, 860-900 MHz, outdoor location O-1.	21
Figure 15. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.	21
Figure 16. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-1.	22

Figure 17. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.....	22
Figure 18. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-1.	23
Figure 19. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.....	23
Figure 20. M4 statistics, jammer on, 723-763 MHz, outdoor location O-2.	24
Figure 21. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.....	24
Figure 22. M4 statistics, jammer on, 860-900 MHz, outdoor location O-2.	25
Figure 23. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.....	25
Figure 24. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-2.	26
Figure 25. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.....	26
Figure 26. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-2.	27
Figure 27. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.....	27
Figure A-1. M4 statistics, jammer on, 723-763 MHz, inside targeted housing unit.	35
Figure A-2. M4 statistics, jammer off, 723-763 MHz, inside targeted housing unit.....	35
Figure A-3. M4 statistics, jammer on, 860-900 MHz, inside targeted housing unit.	36
Figure A-4. M4 statistics, jammer off, 860-900 MHz, inside targeted housing unit.....	36
Figure A-5. M4 statistics, jammer on, 1920-2000 MHz, inside targeted housing unit.	37
Figure A-6. M4 statistics, jammer off, 1920-2000 MHz, inside targeted housing unit.	37
Figure A-7. M4 statistics, jammer on, 2090-2170 MHz, inside targeted housing unit.	38
Figure A-8. M4 statistics, jammer off, 2090-2170 MHz, inside targeted housing unit.	38
Figure A-9. M4 statistics, jammer on, 723-763 MHz, outdoor location O-1.	39
Figure A-10. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.....	39

Figure A-11. M4 statistics, jammer on, 860-900 MHz, outdoor location O-1.	40
Figure A-12. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.....	40
Figure A-13. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-1.	41
Figure A-14. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.....	41
Figure A-15. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-1.	42
Figure A-16. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.....	42
Figure A-17. M4 statistics, jammer on, 723-763 MHz, outdoor location O-2.	43
Figure A-18. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.....	43
Figure A-19. M4 statistics, jammer on, 860-900 MHz, outdoor location O-2.	44
Figure A-20. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.....	44
Figure A-21. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-2.	45
Figure A-22. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.....	45
Figure A-23. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-2.	46
Figure A-24. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.....	46

TABLES

Table 1. Jammer Transmitter Signal Characteristics	6
Table 2. Jammer Transmitter Linear Frequency Modulation (LFM, Chirping) Details	7
Table 3. Measurement Parameters	11
Table 4. Preamp States and Data Files for Broad River, April 11, 2019.....	13
Table 5. Key for Data Figures in this Report.....	15
Table 6. Jammer Power Levels Relative to CMRS Signals, Mean Peak Statistics, 100 kHz Bandwidth	28
Table 7. Differences Between Mean Peak-Detected Jammer Emission Spectra for 100 kHz and 1 MHz Bandwidths (from Indoors Data).....	29

ABBREVIATIONS/ACRONYMS

B_c	chirped-transmitter jammer bandwidth
B_{meas}	measurement (or any receiver) bandwidth
BOP	Federal Bureau of Prisons
CMRS	commercial mobile radio service
DOJ	Department of Justice
dBμV/m	decibels relative to a microvolt per meter
EIRP	effective isotropic radiated power
EMC	electromagnetic compatibility
FM	frequency modulation or modulated
IF	intermediate frequency (stage of a radio receiver)
ITS	Institute for Telecommunication Sciences
LMR	land mobile radio
LNA	low noise amplifier
LOS	line-of-sight
LTE	Long Term Evolution
M4	maximum, minimum, median, and mean (signal statistics)
μsec	microsecond
NTIA	National Telecommunications and Information Administration
OoB	out of band
OSM	Office of Spectrum Management, NTIA
PC	personal computer
preamp	preamplifier
RSMS-5G	Radio Spectrum Measurement System 5 th Generation
RB	resource block
RF	radiofrequency
RMS	root mean square (average) radio power detection
SC DOC	South Carolina Department of Corrections
RSMS	Radio Spectrum Measurement System
STA	Special Temporary Authorization
τ	chirp interval of a jammer device
W	watts

EXECUTIVE SUMMARY

This report describes National Telecommunications and Information Administration (NTIA) emission spectrum measurements of a jammer transmitter in a state prison facility. The measurements were intended to demonstrate the operation of the jammer in four commercial mobile radio services (CMRS) bands between 730 MHz and 2.155 GHz. The demonstration of the jammer's performance occurred at a South Carolina Department of Corrections (SC DOC) Broad River Correctional Institution maximum security housing block at Columbia, South Carolina. NTIA did not participate in the jammer's design, installation or operation. The jammer was operated under a federal government special temporary authority (STA) to radiate, under the control of the Department of Justice (DOJ) Bureau of Prisons (BOP) personnel. Measurements of jammer radiated power were taken both inside and outside the prison.

The demonstration jammer installation consisted of 14 pairs of transmitters and receivers. Seven of the receiver-transmitter pairs were located on the ground floor of the housing unit and the other half were on the floor above. Each pair was installed in a poured-concrete utility shaft, the shafts being located between pairs of prison cells. In ordinary operation, a single jammer transmitter (i.e., only one of the 14 that were installed) would operate only when a paired receiver was triggered by a radio signal interpreted as having originated from a nearby contraband wireless device. This on-demand transmitter action would be fully automated; jammer transmissions would start automatically in response to any given paired receiver having been triggered, and such transmissions would run for a pre-set time interval (a minute or two) before automatically terminating. This receive-then-jam sequence would occur any time that a receiver detected a contraband-CMRS wireless device signal. Jammer transmissions would only ordinarily run in a given band, or even on a given channel, where a paired receiver had detected nearby contraband activity. The central idea behind this system design was to limit aggregates of jammer transmitter signals, with the intention of running only one jammer or so within the system on any given frequency at any instant of time.

This system design could not be scientifically evaluated in a prison environment when operated in its normal on-demand mode. To do so would have required a more complex measurement system and approach than could be brought into, and operated within, any prison location. For the prison environment the measurement was simplified to a single jammer transmitter running continuously, without the transmit-on-demand feature. The jammer transmitter was set to run, sequentially and repetitively, across the four targeted CMRS bands while emission data were collected at selected indoor and outdoor locations.

The targeted jamming zone was half of the housing unit's cell block. The jammer's emissions were measured at a location near the main entrance to the cell block and at two locations outdoors, beyond the exterior wall of the targeted prison cells. Ambient CMRS signals were measured with the jammer turned off. This approach provided data that clearly show the jammer emission levels versus the ambient CMRS signal levels at each measurement location.

At the indoor measurement location, measured differences in incident power between when the jammer was on versus off showed that jammer power levels were 35 to 40 dB higher than the ambient CMRS power levels. At outdoor locations where jamming was not intended, the jammer's power was 0 to 10 dB higher than the ambient CMRS signals.

Because the jammer signal was much stronger than the CMRS signal received inside the prison it would be likely to deny service to other wireless devices within some indoor zone. It is unclear whether it was unnecessarily powerful to the detriment of licensed CMRS wireless devices outside the targeted prison area. Further analysis is not possible without accepted technical criteria for harmful interference thresholds for CMRS wireless devices. The data in this report can be compared to such criteria, if (or when) those criteria are eventually developed.

The measurement results of this study are idiosyncratic to this particular jammer installation at this particular facility. Variations in jammer designs and emission characteristics, structural and attenuation characteristics of buildings, and site-dependent propagation factors would be expected to produce different results for different jammer installations at the Broad River Correctional Institution or at other facilities.

The measured jammer was part of a system designed to limit aggregate jamming emissions via on-demand jammer operation, as described above. Analysis of the extent to which this system or others like it actually limit aggregate emissions was beyond the scope of this measurement effort.

Product demonstrations performed within prison environments, such as the one described in this report, are inherently limited in what they can tell us about the impact of these jammers on other wireless devices operated inside such facilities. Nor do such demonstrations tell us the extent to which external, non-targeted wireless receivers (non-targeted phones) might be affected by stray emissions from the jammers. In order to understand the impact of jammers on other wireless devices, whether inside or outside the facility, it is necessary to know:

- *At what power level will an interfering signal prevent service to CMRS wireless devices inside a particular building?*
- *At what power level will an interfering signal prevent service to CMRS wireless receivers operating outside a building where interfering signals exist?*

These questions can only be answered by theoretical analysis, simulation and modeling, plus selected measurements in controlled laboratory environments. A carefully engineered analysis of the impact of interfering signals of various levels on CMRS wireless devices would require a complex setup that would allow a large number of combinations of simulated device stimulus signals in multiple CMRS bands to be methodically transmitted with time-coordinated and frequency-coordinated measurements of jammer responses running in the instantaneously targeted channels and bands. In this way, the impact of interfering transmissions on CMRS wireless devices could be objectively quantified. Laboratory and *in situ* work should go hand-in-hand, since only *in situ* work can describe:

- CMRS-band signal strength inside a particular building
- CMRS-band signal strength outside a particular building, beyond which harmful interference to non-targeted receivers is not to be tolerated
- Radio propagation factors inside a particular building

EMISSION MEASUREMENTS OF A CONTRABAND WIRELESS DEVICE JAMMER AT A STATE PRISON

Frank H. Sanders, Geoffrey A. Sanders and John E. Carroll¹

This report describes emission spectrum measurements of a wireless jammer device operated temporarily inside a South Carolina state prison maximum security housing block. The measurements were intended to demonstrate the operation of the jammer in four commercial mobile radio service (CMRS) bands between 730 MHz to 2.155 GHz. Spectrum measurements of the jammer emissions were performed indoors and outdoors with two measurement bandwidths. Measurements at each location were performed with the jammer on versus off, so as to show the relative power levels of the jamming and ambient CMRS signals at each location. This report's data can be applied in future electromagnetic compatibility (EMC) analyses. However, the data provide no information as to whether a CMRS wireless device can or cannot perform its intended communications function in the presence of a competing signal of specified strength. Only thorough theoretical analysis, well-engineered simulation and modeling, plus selected measurements in controlled (laboratory) environments can objectively quantify the impact of interfering transmissions on CMRS wireless devices.

Key words: cellular jamming; commercial mobile radio service (CMRS) jamming; denial-of-service jamming; electromagnetic compatibility (EMC); harmful interference; communications jamming; micro-jammer; radio jamming; wireless device jamming

1. INTRODUCTION

This report describes measurements that National Telecommunications and Information Administration (NTIA) Institute for Telecommunication Sciences (ITS) laboratory engineers performed on radiated emissions produced by a micro-jammer² [1], [2] transmitter at a Broad River Correctional Institution maximum security housing unit operated by the state of South Carolina's Department of Corrections (SC DOC) at Columbia, South Carolina. The work was done in coordination with, and under the control of, Department of Justice (DOJ) Bureau of Prisons (BOP) personnel.

¹ The authors are with the Institute for Telecommunication Sciences (ITS), National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, Boulder, Colorado.

² "Micro jammer" is a generic term used by the federal government to describe relatively low-powered jammers that are designed to be deployed in networks to cover entire prison facilities. See [1] and [2] for examples of this terminology as used by DOJ and BOP.

The jammer transmitter radiated intentional interference emissions in the following commercial mobile radio service (CMRS) frequency ranges:

- 729–757 MHz
- 869–894 MHz
- 1930–1990 MHz
- 2110–2155 MHz

Details of the jammer’s transmitter characteristics are provided in Section 2 of this report.

1.1 Objective

The objective of this study was to perform emission spectrum measurements on micro-jammer signals inside and outside a targeted jamming zone at an operational prison facility. The micro-jammer prototype device was designed to operate at a relatively low power level so as to effectively disrupt wireless communications in a small targeted zone indoors while not affecting other CMRS operations outdoors, outside the zone of intentional jamming.

Specific tasks included:

- 1) Determination of the radiated power levels that the micro-jammer transmitter produced inside and outside the zone of intentional jamming. The measurement locations were to be:
 - a) indoors, near an entrance to the housing unit;
 - b) outdoors, 20 m (66 ft) outside the building and adjacent to the housing unit’s outer wall;
 - c) outdoors, 40 m (132 ft) outside the building and adjacent to the housing unit’s outer wall.
- 2) Determination of the power levels of the ambient CMRS signals in the four identified frequency bands, at the same places where the jammer’s signals were measured.
- 3) Comparison of the jammer signal power levels to the ambient CMRS signal power levels at each measurement location.
- 4) The rate at which jammer power varies with the bandwidth of receivers, which would be needed for future electromagnetic compatibility (EMC) studies.

1.2 Considerations of Jammer Effectiveness Against Contraband Wireless Devices and Potential for Harmful Interference to Licensed Radio Services

A desirable technical objective for *in situ* radiation of jamming signals at a prison facility, such as is described in this report, would be:

- Technical assessment of the jammer’s effectiveness against contraband wireless devices within the targeted jamming zone
- Technical assessment of the jammer’s potential for harmful interference to licensed radio service receivers outside the targeted jamming zone

Such assessments are currently hindered by a lack of accepted technical criteria for jamming-signal effectiveness against targeted receivers and potential for harmful interference to non-targeted receivers.

Consider first the question of jammer effectiveness. In order to be more than anecdotal (e.g., “when we turned on the jammer, we couldn’t complete a phone call”), jammer effectiveness needs to be quantified in terms of a ratio such as available CMRS signal power, S , to jammer power, J . A mathematical expression is needed in terms of S/J or something similar. Studies to determine such ratios have been performed, for example, for LTE-type receiver performance in the presence of radar pulses ([3], [4]). We are not aware of similar open-literature studies for the effects of intentional jamming against CMRS receivers in any way similar to, e.g., [5] and [6]. Jamming-effects engineering studies need to be performed against CMRS-type receivers if definitive criteria are to be developed for jammer effectiveness. Such criteria would allow engineers to assess the levels at which jamming power would be effective without being excessive.

A second, similar problem exists for assessment of harmful-interference thresholds for CMRS-type receivers. Similarly to some sort of S/J criterion for jamming effectiveness, a criterion for harmful interference effects would likely be written in terms of desired signal power, S , compared to jamming interference power, I , (that is, as an S/I ratio). One distinction between S/J and S/I criteria would be that harmful interference effects would be expected to occur at lower I power levels than effective J power levels.

Again, studies of harmful radio interference-effects thresholds on radio receivers can be performed and in fact have been performed for radar receivers in the presence of interference from communication signals (e.g., [7], [8]). But we are not aware of any generally accepted S/I criteria for harmful interference thresholds for CMRS-type receivers. Until such studies are performed and S/I criteria have been accepted for such receivers, we are unable to quantitatively assess the harmful interference potential for measured levels of jamming power against CMRS-type receivers. Non-engineering sorts of assessments (e.g., “we placed phone calls from location X when jammer Y was running nearby”) are anecdotal. They lack the statistical engineering strength that would be obtained from controlled studies. They also do not indicate the extent, if any, to which CMRS communications might be operating in a possibly degraded manner even though some phone calls were successfully connected.

To put it even more simply, two engineering numbers would be needed in order to understand the impact of jammers on other wireless devices:

- *At what power level will an interfering signal prevent service to CMRS wireless devices inside a particular building?*
- *At what power level will an interfering signal prevent service to CMRS wireless receivers operating outside a building where interfering signals exist?*

Then, the data collected in this study could be compared to power levels required for 1) effective jammer operations within the targeted jamming zone; and 2) assessment of potentially harmful interference to CMRS receivers outside the jamming zone. Since such accepted technical criteria do not currently exist, we cannot perform these assessments at this time.

Engineering studies combining theoretical modeling and analysis with controlled laboratory observations are the only ways to develop such criteria. Lacking such criteria at this time, we can only report the measured relative power levels of jammer signal strength and ambient CMRS signals, and point out that such comparative levels may eventually be assessed on an engineering basis when the appropriate technical criteria described above become available.

1.3 Approach

The study approach was as follows:

- 1) On behalf of the BOP and SC DOC, DOJ requested and obtained from NTIA an experimental Special Temporary Authorization (STA) to use the jamming device for purposes of demonstrating a micro-jamming approach in an SC DOC prison facility.³ Some SC DOC personnel were temporarily federally deputized for this STA operation.
- 2) A private sector company, with cooperation and supervision of BOP and SC DOC, temporarily installed a jamming system inside a Broad River Correctional Institution maximum security housing unit at Columbia, South Carolina. The jamming system consisted of 14 pairs of CMRS-band receivers and jammer transmitters. Seven of the receiver-transmitter pairs were on a ground floor of the housing unit and the other half were on the floor above. Each pair was installed inside a concrete utility shaft (14 shafts being put into use, altogether). The shafts were located between pairs of prison cells.
- 3) This jammer-transmitter system design could not be scientifically evaluated in a prison environment when operated in its normal on-demand transmitter mode. To do so would have required a more complex measurement system and approach than could be brought into, and operated within, any prison location. Therefore the jammer was operated in a simplified mode. Only a single jammer transmitter was operated, without transmit-on-demand. The

³ NTIA, in consultation with the Frequency Assignment Subcommittee of the Interdepartment Radio Advisory Committee provides short-term, temporary authorizations to Federal agencies under Section 8.3.31 of the Manual of Regulations and Procedures for Federal Radio Frequency Management (Sept. 2017 revision of the May 2013 Edition). As a condition of the STA, DOJ coordinated in advance with commercial wireless carriers in the Columbia, South Carolina, area.

jammer transmitter was set to run, continuously, across the four targeted CMRS bands while emission data were collected at selected indoor and outdoor locations.

- 4) The targeted jamming zone was half of the cell block. The jammer's emissions were measured at a location near the main entrance to the cell block and at two locations outdoors, outside the exterior wall of the targeted prison cells. The outdoor locations had clear line-of-sight (LOS) (e.g., no obstructions) propagation to the building. The distances were 20 m (66 ft) and 40 m (132 ft) from the outside building wall. Every measurement was repeated twice at each location, once with the jammer turned on and once with the jammer turned off. This approach provided data that show the jammer emission levels versus the ambient CMRS signal levels at each measurement location.
- 5) NTIA engineers used an ITS-designed portable, battery-powered measurement system to measure the emission levels of the jammer. Under BOP supervision, the jammer was turned on and off for each measurement at each location, so as to allow ambient CMRS signal levels to be measured and observed separately from the jammer emissions.
- 6) NTIA engineers reduced the raw measurement data to graphical plots, which are provided in this report (main body and Appendix A) and conducted pertinent data analysis. The plots show received power at the measurement antenna terminals in units of decibels relative to a milliwatt (dBm) per unit bandwidth (100 kHz and 1 MHz).⁴

⁴ Although we do not do it in this report, these data can be converted into incident field strength in space at the measurement antenna, via application of the measurement antenna's gain.

2. JAMMER DESCRIPTION AND INSTALLATION

2.1 Jammer Electrical Characteristics

Table 1 provides the basic electro-technical characteristics of the micro-jammer transmitter as culled from data in DOJ's STA. Table 2 shows details of the signal parameters. The jammer signal used a linear frequency modulation (LFM), commonly called 'chirped' modulation, that repetitively tuned a carrier wave up across each targeted CMRS band. The frequency-tuning behavior is a ramp when plotted as a function of time, as shown in Figure 1.

Table 1. Jammer Transmitter Signal Characteristics⁵

Jammer Technical Characteristic	Parameter Value
Band 1	729-757 MHz
Band 2	869-894 MHz
Band 3	1930-1990 MHz
Band 4	2110-2155 MHz
Transmitter Power	2 watt (+33 dBm) per band ⁶
Antenna Gain	+0.5 dBi, omnidirectional
Antenna Polarization	Not specified
Modulation	N0N = linear frequency modulation (LFM)
Chirp On Time	10 μ s
Chirp Off Time	30 μ s
Chirp Sequence	Band 1, Band 2, Band 3, Band 4, then repeat
Emission Line Spacing	25 kHz (each band re-visited every 40 μ s)

⁵ The jammer transmitter operated sequentially in time through the four jamming bands. The interval for each band was stated by the installer to be 10 microseconds. So, each band was jammed for 10 microseconds, followed by 30 microseconds of non-jamming while the other three bands were jammed. After 30 microseconds of non-transmit in each band, the jammer transmitter returned to any given band and jammed that band for another 10 microseconds. See Figure 1.

⁶ The STA called for a maximum transmitter power of +33 dBm (2 watts) per band. The transmitter power output could not be verified by the authors under the conditions of the prison environment.

Table 2. Jammer Transmitter Linear Frequency Modulation (LFM, Chirping) Details

Low Freq. (MHz)	High Freq. (MHz)	Sweep Rate (MHz per μ s)	On Time (μ s)	Peak Detected Measurement Bandwidth ⁷ (MHz)	Average Detected Measurement Bandwidth ⁸ (MHz)
729	757	28/10 = 2.8	10	≈ 1.67	≈ 31
869	894	25/10 = 2.5	10	≈ 1.58	≈ 28
1930	1990	60/10 = 6	10	≈ 2.45	≈ 66
2110	2155	45/10 = 4.5	10	≈ 2.12	≈ 50

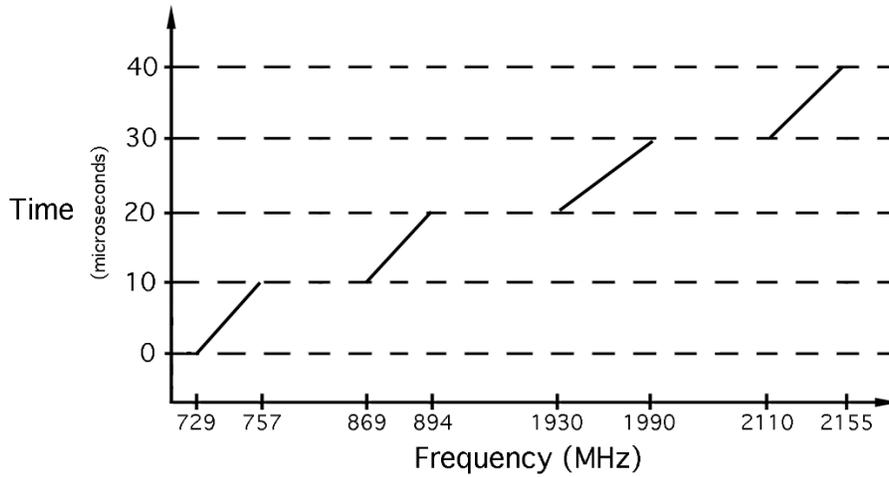


Figure 1. Jammer LFM behavior. The complete chirp sequence, across all bands, was repeated every 40 microseconds. Frequencies are plotted to a non-fixed scale.

In this system’s ordinary operation, any single jammer transmitter (i.e., only one of the multiple installed units) would only operate when its paired⁸ receiver was triggered by a radio signal interpreted as having originated from a nearby contraband wireless device. This on-demand transmitter action would be fully automated; jammer transmissions would start automatically in response to any given paired receiver having been triggered, and such transmissions would run for a pre-set time interval (a minute or two) before automatically terminating. This receive-then-jam sequence would occur any time that a receiver detected a contraband-device signal. Jammer

⁷ See Appendix B of [10] for further description and discussion of peak and average detector responses to LFM signals.

⁸ The pairing function did the following: Following reception of an *uplink* signal from a contraband mobile unit to a local carrier’s base station by a surveillance receiver, a jammer system controller would use an internal, pre-programmed look-up table to identify the paired *downlink* signal that would be *expected* to be transmitted from the base station to the contraband mobile unit. The jammer would then activate against that *expected downlink* signal frequency in order to jam the contraband receiver’s operation.

transmissions would only ordinarily run in a given band, or even on a given channel, where a paired receiver had detected nearby contraband activity. The central idea behind this system design was to limit aggregates of jammer transmitter signals, with the intention of running only one jammer or so in the system on any given frequency at any instant of time.

2.2 Measured Jammer Power as a Function of Measurement Bandwidth

Jammer power can be measured in two different ways. One method uses a root mean square (RMS) averaging detector in a measurement bandwidth, B_{meas} , slightly wider (by about ten or eleven percent) than the LFM chirped emission bandwidth, B_c . While this method includes all the jammer power it does require a wide measurement bandwidth (equal to the chirp bandwidth, B_c) to obtain the full power of the transmitter.

The second method uses a positive peak detector in the measurement bandwidth. Full power can be measured in a narrower bandwidth than that required for RMS detection. This full-power peak-detection measurement bandwidth, B_{meas} , is, from (6b) in [9]:

$$B_{meas} = (B_c/\tau)^{1/2},$$

where τ is the LFM (chirp) on-time in microseconds and B_{meas} and B_c are both in units of megahertz.

The full-power measurement bandwidths of these methods are shown in the last two columns of Table 2. For the Broad River measurements, all measurements were peak detected. B_{meas} was less than the values shown in Table 2. Therefore the measured power measured was always less than the jammer's total power and varied with B_{meas} . As noted in Section 3 of this report and as discussed further in Appendix B of [10], measurements performed in multiple bandwidths less than B_{meas} at Broad River allowed us to observe the *rate* at which peak-detected power in *any* receiver will vary with bandwidth for this jammer. This allows scaling of the received power from the jammer in *any* receiver and detection mode, so long as the receiver's own bandwidth and detection mode are known.

2.3 Targeted Jamming Space

Figure 2 shows the jammer installation in utility spaces within the Broad River Correctional Institution maximum security housing unit. Seven jammers were located on each of two floors (14 jammers total), the jammers being placed between alternating pairs of prison cells. The housing unit construction was of poured steel-reinforced concrete. Utility space dimensions, internal piping arrangements, concrete thicknesses and composition, and reinforcement details are unspecified. The targeted area where indoors measurements were performed was in the housing unit's ground floor.

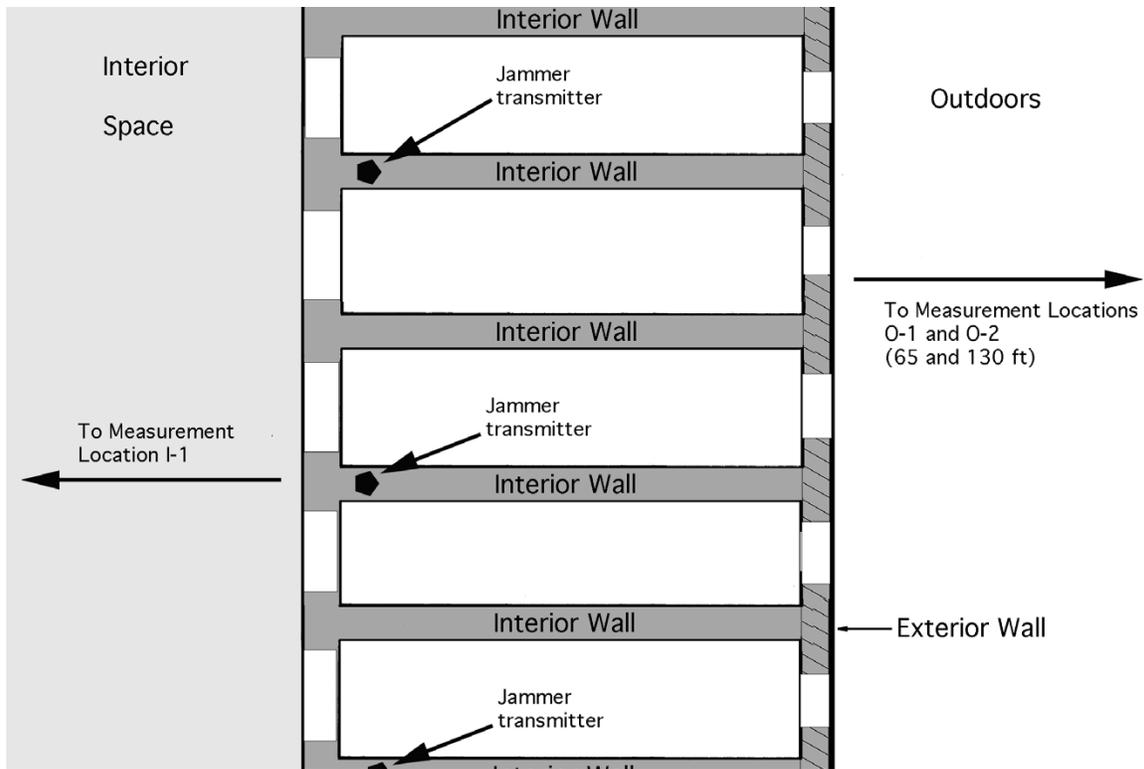


Figure 2. The Broad River jammer installation top view, approximately scaled. Seven jammers were spaced every other cell, in utility shafts, on each of two floors. Only one jammer on the ground floor was operated for the measurements.

The prison cell interior dimensions were approximately 4 m (13 ft) long by 2.4 m (8 ft) wide by 3 m (10 ft) high. Fixed interior infrastructure in each cell included a toilet, sink, and bunk bed. Doors were made of steel. Cells had small single exterior windows. Electrically, the targeted spaces could be considered to be empty six-sided steel-and-concrete rectangular boxes of these dimensions, with a limited number of small exterior apertures.

2.4 Jammer Installation and Effective Isotropic Radiated Power (EIRP)

The jammer was a single transmitter. To jam multiple CMRS bands, this one jammer operated sequentially through them (Figure 1). The jammer transmitter box was installed inside a utility shaft, as shown in Figure 2, with an omnidirectional jammer antenna mounted inside the shaft as well. As shown in Table 1 (based on STA data), each antenna was supposed to have had +0.5 dBi gain. Polarization was not specified.

For the Broad River installation, the EIRP in each band was the decibel sum of transmitter power and antenna gain, or $(+33 \text{ dBm} + 0.5 \text{ dBi}) = +33.5 \text{ dBm}$ within the utility shaft installation. Radio propagation conditions within the shaft and across the rest of the housing unit were not characterized.

3. MEASUREMENT DESCRIPTION

3.1 Measurement System Hardware and Software

The measurement system is shown schematically in Figure 3.

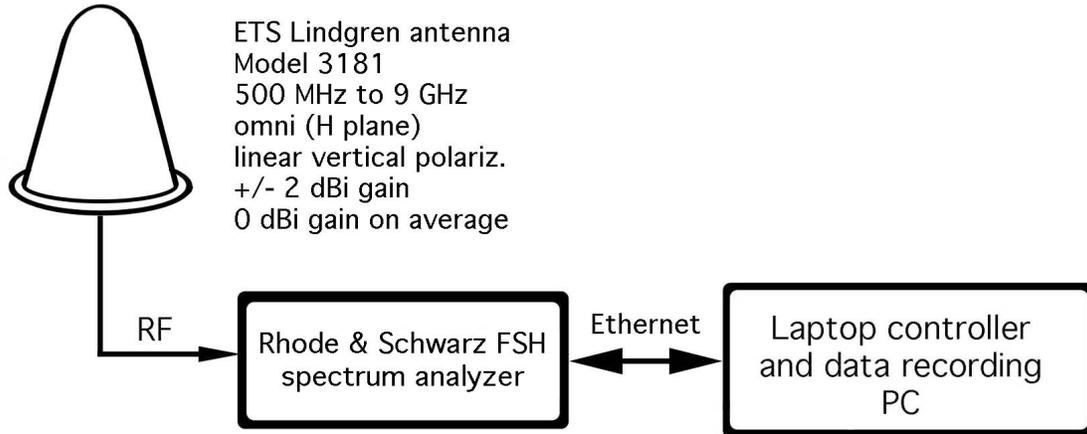


Figure 3. Block diagram schematic of the jammer emission measurement system used at Broad River Correctional Institution.

The measurement system used an ETS Lindgren Model 3181 biconical, azimuthally omnidirectional, linearly vertically polarized antenna with a calibrated frequency response range of 500 MHz to 9 GHz. Its azimuthal gain varied by ± 2 dBi, depending on exact frequency.⁹ The antenna was connected via a short length of low-loss radiofrequency (RF) coaxial line to the input of a Rhode & Schwarz FSH battery-powered portable spectrum analyzer. The analyzer was controlled via ITS-written software (called Radio Spectrum Measurement System 5th Generation, or RSMS-5G) installed on an ITS laptop personal computer (PC).

Using an intermediary ethernet connection (Figure 3), the laptop PC sent commands to the spectrum analyzer to run a pre-programmed set of emission measurements at each measurement location. The parameters for these pre-programmed measurements are shown in Table 3. The software ran each of the measurements listed in that table twice at each measurement location: once with the jammer on and once with the jammer off, so that the jammer emissions could be compared to the ambient CMRS signal-power levels in the jammed bands.

The data from all of these measurements were sent from the spectrum analyzer to the controller PC, where they were recorded on the PC's hard drive as MATLAB® format files. Subsequent to the measurement series on April 11, 2019, all of the data were backed up on additional platforms.

⁹ For analysis purposes, a typical antenna gain of 0 dBi should be used as an overall best fit.

3.2 Measurement System Parameters

The measurement parameters are shown in Table 3.

Table 3. Measurement Parameters

Freq. Range (MHz) ¹⁰	Measurement (Resolution) Bandwidth (kHz)	Video Bandwidth (kHz)	Detector	Sweep Time (sec)	Freq Bin Size (kHz)	Dwell per Bin (μsec)	Total Jammer Sweeps per Bin
723–763	100	300	Peak, 50 sweeps	0.28	63	444	44
723–763	1000	3000	Peak, 50 sweeps	0.28	63	444	44
860–900	100	300	Peak, 50 sweeps	0.14	63	222	22
860–900	1000	3000	Peak, 50 sweeps	0.14	63	222	22
1920–2000	100	300	Peak, 50 sweeps	0.28	126	444	44
1920–2000	1000	3000	Peak, 50 sweeps	0.28	126	444	44
2090–2170	100	300	Peak, 50 sweeps	0.14	126	222	22
2090–2170	1000	3000	Peak, 50 sweeps	0.14	126	222	22

The number of jammer frequency sweeps per bin was a trade-off between the need to gather a statistically significant number of jammer pulse events and the time available to complete the measurements. This number in turn drove the other values for the dwell interval per bin and the total frequency sweep time for each CMRS band. The size of each bin, in kilohertz, was driven by the width of each band divided by the 631 bins available on the spectrum analyzer screen display.

3.2.1 Measurement Frequency Bands

As shown in Table 3, detailed measurements were performed in each of the four intentionally jammed CMRS bands, including a few extra megahertz on the lower side and upper side of each band. The margins were added to show the out-of-band (OoB) roll-off of the jammer emissions in adjacent spectrum.

3.2.2 Measurement Bandwidths

In the CMRS bands, peak-detected data were acquired in a 100 kHz measurement (also called resolution, or intermediate frequency (IF)) bandwidth and in a 1 MHz resolution bandwidth.¹¹ The use of two bandwidths that differ from each other by a factor of 10 allows for easy scaling of the power measured for the jammer signal in any intermediate bandwidth of interest for possible

¹⁰ The measurement band edges were set somewhat wider than the CMRS band edges so that adjacent-band roll-off of the jammer emissions could be observed in the measurement data.

¹¹ The spectrum analyzer's baseband, lowpass filter, called a video filter, was set to be wider than the resolution bandwidth so as to not affect the overall measurement result for any given resolution bandwidth setting.

future EMC analysis studies that might involve receivers having any given bandwidth. (See further discussion in Appendix B of [10].)

For example, if the jammer's measured power were to change by a factor of 10 between measurements made in a 100 kHz and 1 MHz bandwidth (called a 10-log progression of power with bandwidth), then that would mean that the jammer's measured power is directly proportional to any receiver's bandwidth. In that case, the power that would be seen (measured) in the 180 kHz bandwidth of a typical Long Term Evolution (LTE) receiver's resource block (RB) relative to the power measured in 100 kHz would be the power measured (in decibel units) in 100 kHz *plus* $10 \times \log(180/100) = 2.5$ dB more power than in 100 kHz.

For general EMC studies, it cannot be assumed that any and all CMRS receiver bandwidths will have any particular value. The 180 kHz LTE RB bandwidth, although currently common in CMRS radios, may not remain constant or common in the future; other existing and future communication systems may use different bandwidths from 180 kHz. By taking data in a *pair* of bandwidths, however, we obtain the variation in jammer power (and of existing CMRS communication-signal power) *as a function of bandwidth*. Our data can then be applied to existing or future systems which may use any receiver bandwidths between 100 kHz to 1 MHz.

3.2.3 Peak Detection Mode

Peak detection mode was used to measure the jammer emissions. Peak detection shows the highest power level of the emitted waveform in the selected measurement resolution bandwidth for each measured frequency bin in each frequency sweep of the spectrum analyzer.

Peak data show the maximum power that the waveform can have at any given frequency in the selected resolution bandwidth. In peak detection mode, the spectrum analyzer's time-domain digitizer output is continuously sensed by the spectrum analyzer for the duration of each bin in each measurement sweep trace. As this within-a-bin monitoring progresses, a hardware peak-latch circuit (in analog spectrum analyzers) or a software peak-latch function (in digital analyzers such as the Rhode & Schwarz FSH) retains the highest-power value that goes through the individual bin while the bin is active. When the measurement has ceased for each bin, the highest-power latched value is displayed and retained by the analyzer's sweep trace for each respective bin.

In order to peak-detect the highest power in the waveform in the analyzer's selected measurement bandwidth, the bin sampling interval must be long enough for the waveform to reach its maximum level while the bin measurement is active. For measurements of this jammer, the LFM emission of a jammer was expected to reach maximum power on any given frequency once every 40 microseconds (Figure 1). The next-largest available analyzer interval of 44 microseconds was therefore used. With the analyzer trace being 631 bins across, the trace sweep time must be no shorter than $(631 \times 44 \text{ microseconds}) = 27.76$ milliseconds; a rounded value of 28 milliseconds was selected for the analyzer's band-sweeping interval.

3.3 Spectrum Analyzer Preamplifier and Thermal Noise Limit

The Rohde & Schwarz FSH spectrum analyzer includes a built-in low noise amplifier (LNA), also called a preamplifier or preamp. This preamp reduces the spectrum analyzer noise figure (and concomitantly increases its sensitivity) by 20 dB when it is turned on. Thus the preamp can make some weak signals visible, signals which would have otherwise been below the spectrum analyzer’s noise floor.¹²

However, the analyzer’s power-overload point is reduced (the analyzer becomes more vulnerable to being overloaded) when the preamp is activated. The preamp should only be used when the *sum total* power from all signals in its response range does not exceed its overload point (at about -30 dBm). Overload tests at the measurement site were conducted to determine when it was appropriate to use the preamp. The result was: the preamp was turned on, both indoors and outdoors, to see background CMRS signals when the jammer was off. The preamp was turned off, both indoors and outdoors, when the jammer was on, to avoid overload from the jamming signal power. See Table 4.

Table 4. Preamp States and Data Files for Broad River, April 11, 2019

Measurement Location	Jammer State	Spectrum Analyzer Preamp State	Data File Number ¹³
Indoors	On	Off	6
Indoors	Off	On	20
Outdoors (O-1)	On	Off	4
Outdoors (O-2) ¹⁴	On	Off	5
Outdoors (O-1)	Off	On	3

3.4 Measurement Procedure

All measurements were performed at the Broad River Correctional Institution on April 11, 2019. The measurement gear had been previously shipped to South Carolina from Boulder and had been preliminarily tested before being deployed at the prison. On the morning of the 11th the NTIA engineers assembled the measurement system, including the portable equipment cart, in

¹² The spectrum analyzer’s noise figure, NF , was 29 dB with preamp off and 9 dB with preamp on. Peak detection adds approximately 10 dB to noise floor. The spectrum analyzer’s noise floor in any bandwidth was therefore: $(-174 \text{ dBm} + 10 \log(B_{meas}) + NF + (10 \text{ dB for peak detection, if used}))$. For example, in 100 kHz bandwidth with the preamp on and positive peak detection in use, the analyzer’s noise floor was $-174 \text{ dBm (thermal physics)} + 50 \text{ dB (bandwidth)} + 9 \text{ dB (NF)} + 10 \text{ dB (peak detection)} = -105 \text{ dBm}$.

¹³ These are RSMS-5G data file numbers.

¹⁴ Because locations O-1 and O-2 were close together, and time was a consideration for measurement completion, only a single outdoor control/baseline jammer-off location was used: O-1. Jammer-off data were not collected at location O-2.

the prison parking lot. The system was turned on and was rolled through the facility's security checkpoint as it warmed up (all power being provided by an on-board battery power supply). The measurement system (Figure 1) was then rolled into one of the facility's ground-level maximum security housing units where the jamming system had been temporarily installed (Figure 2).

Because the active part of the measurement system consisted only of the spectrum analyzer, the analyzer's internal self-calibration routine was judged adequate for these measurements. (The loss in power through the low-loss RF line between the antenna and the analyzer is negligible.) All power measurements in this report's graphics are shown in units of dBm per unit measurement bandwidth (100 kHz or 1 MHz) in the 50 ohm circuitry at the measurement antenna terminals.¹⁵

The installer's personnel, under the supervision and control of BOP staff, operated the jammer from a remote location (in Florida) via mobile telephone calls. The single jammer transmitter that was used for our measurements was set to operate across the four radio bands shown in Figure 1, sequentially, for as long as was required to gather measurement data at the three measurement locations (one indoors and two outdoors).

Baseline data for background activity in CMRS bands was measured at a location inside the housing unit and at another location outside, 20 m (66 ft) from the unit's outside wall.¹⁶ When the jammer was activated, emission data were collected at each of those locations plus a second outside location that was 40 m (132 ft) from the outside wall. As noted above, the spectrum analyzer's preamp was turned on for all baseline data collections. It was turned off when the jammer was on.

At each measurement location, the jammer was turned on for jammer-plus-background signal data collection, and then was turned off for background-only ambient signal data collection. This was a manually-forced mode of operation; the jammer would normally only have operated in an on-demand mode in any one band, and only for about a minute at a time, on a downlink (base station-to-mobile) channel when triggered by a contraband wireless uplink (mobile-to-base station) signal detected by a paired monitoring receiver.¹⁷

The spectrum measurement data were automatically retrieved from the spectrum analyzer after every individual analyzer sweep was completed. Data were stored on the measurement PC's hard drive in MATLAB® format. Table 4 summarizes the data file collection.

¹⁵ These data can be converted to absolute field strength at the measured points in space, by applying the measurement antenna's gain factor to the power measured in 50 ohms. See [11] for the conversion formula.

¹⁶ As noted above, only a single outdoor control/baseline jammer-off location was used: O-1. Jammer-off data were not collected at location O-2. The outdoor locations were sufficiently close together, and time was sufficiently limited, to justify a single baseline outdoor location for this measurement effort.

¹⁷ As noted above, proper operation in the jammer's "normal" demand-based mode would have relied on accurate table-based mapping of downlink frequencies to the activity-sensed uplink frequencies.

4. MEASUREMENT RESULTS

Table 5 summarizes the measurement results. For the sake of easily making comparisons from one data graph to the next, all spectra are plotted with an ordinate range of -110 dBm to -10 dBm; this dynamic range accommodates all collected Broad River data. All data sets in Table 5 contain comparative jammer-on versus jammer-off pairs. Appendix A provides peak-detected measurements in 1 megahertz bandwidth as Figures A-1 through A-24. Those graphs, showing the jammer signal and ambient CMRS signals in 1 megahertz bandwidth, can be compared with the peak-detected 100 kilohertz graphs to establish the rate of change of the jammer signal as a function of bandwidth, as discussed above in Section 3.2.2 and in Appendix B of [10].

Spectra are always paired on each page, the upper graphs always being jammer-on data and the lower graphs being corresponding jammer-off data. Analysis of measurement results is provided in Section 5.

Table 5. Key for Data Figures in this Report

Figures	Location	Measurement Bandwidth
4–11	Indoors	100 kHz
12–19	O-1 (outdoors 20 m)	100 kHz
20–27	O-2 (outdoors 40 m)	100 kHz
A-1–A-8	Indoors	1 MHz
A-9–A-16	O-1 (outdoors 20 m)	1 MHz
A-17–A-24	O-2 (outdoors 40 m)	1 MHz

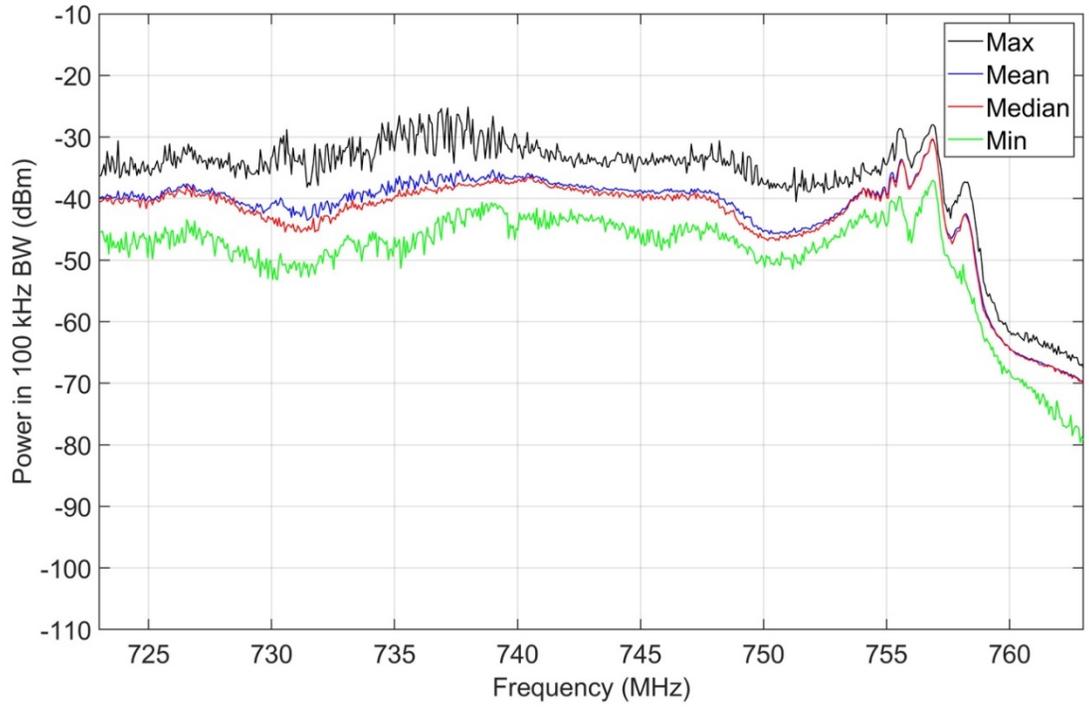


Figure 4. M4 statistics, jammer on, 723-763 MHz, inside targeted prison housing block.

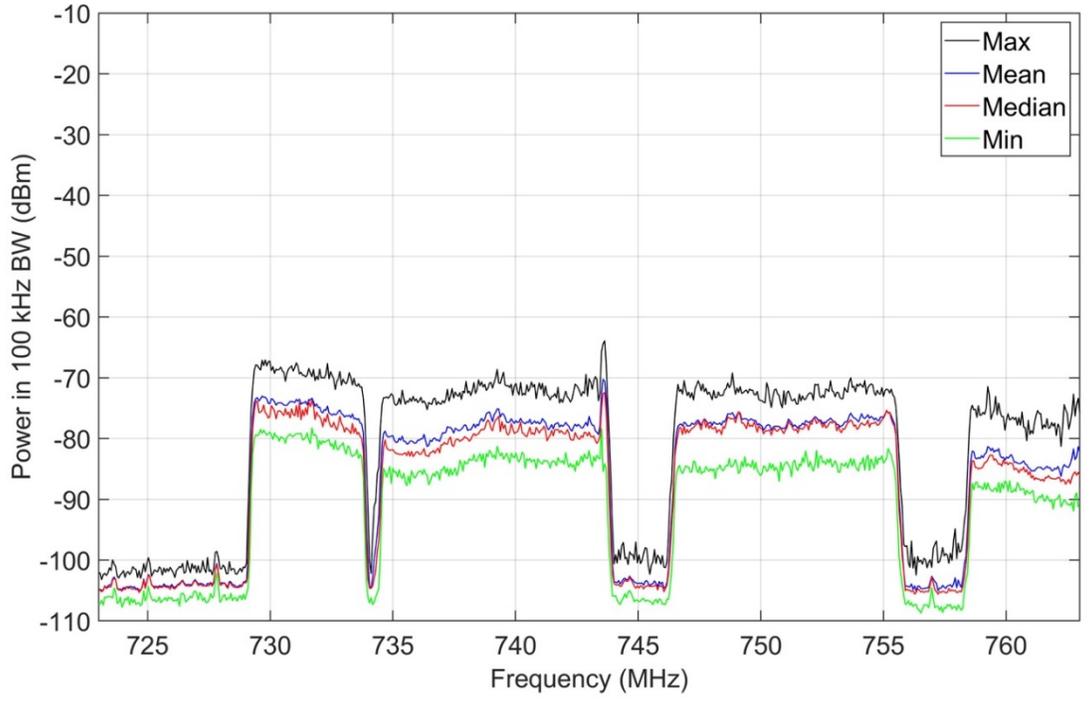


Figure 5. M4 statistics, jammer off, 723-763 MHz, inside targeted prison housing block.

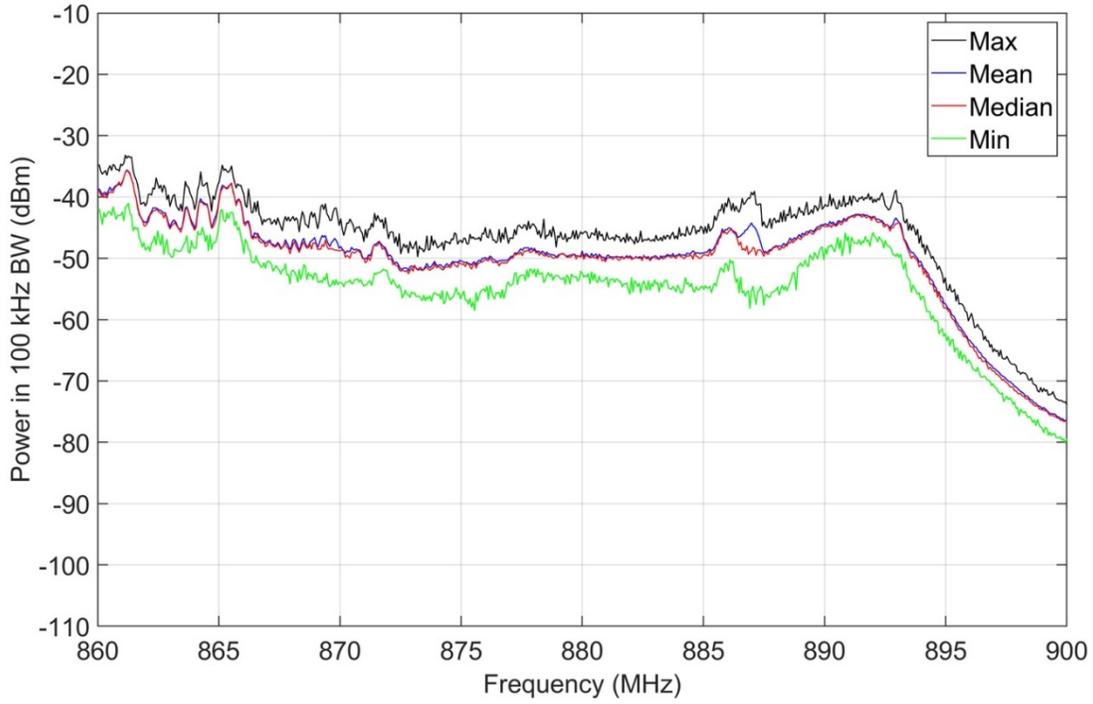


Figure 6. M4 statistics, jammer on, 860-900 MHz, inside targeted prison housing block.

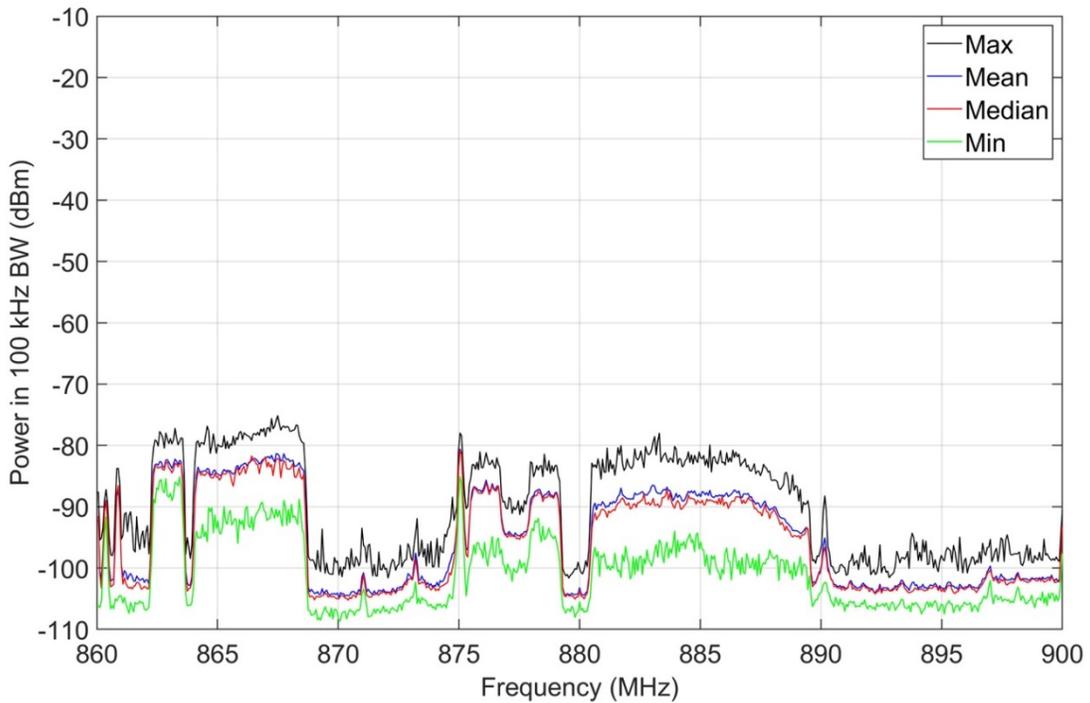


Figure 7. M4 statistics, jammer off, 860-900 MHz, inside targeted prison housing block.

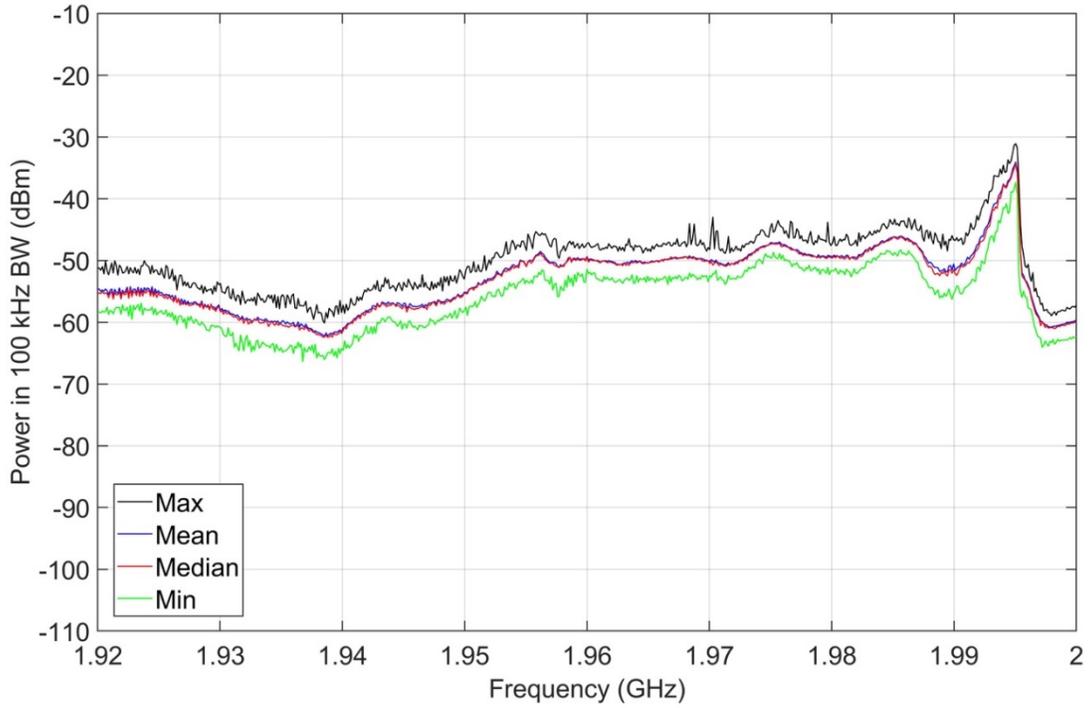


Figure 8. M4 statistics, jammer on, 1920-2000 MHz, inside targeted prison housing block.

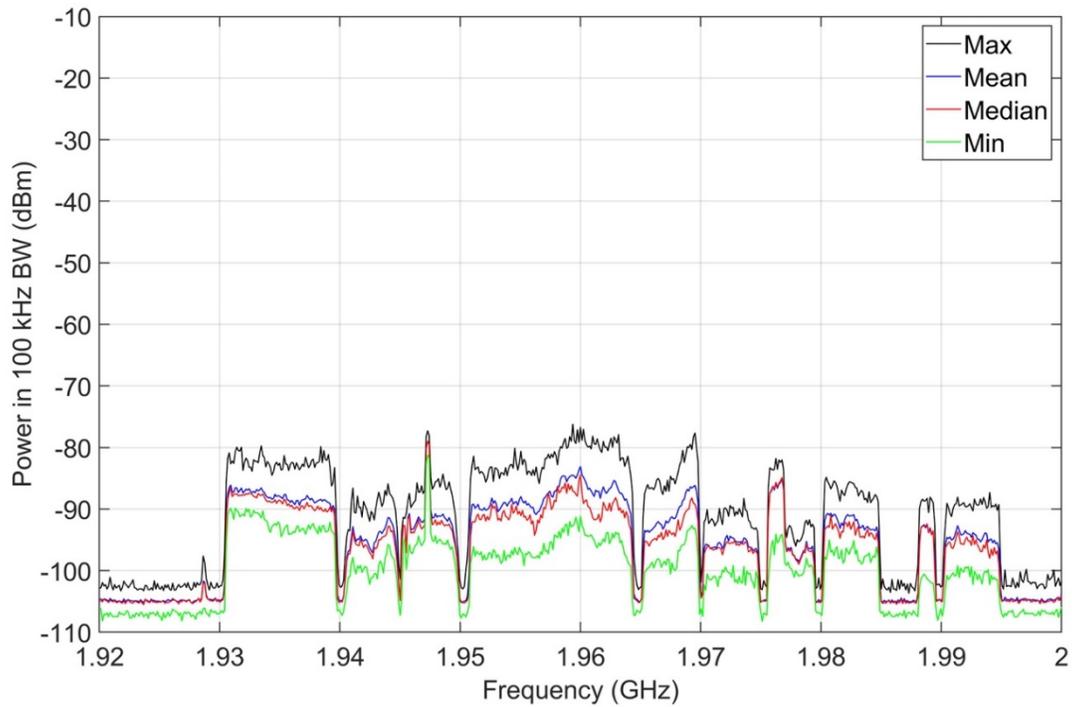


Figure 9. M4 statistics, jammer off, 1920-2000 MHz, inside targeted prison housing block.

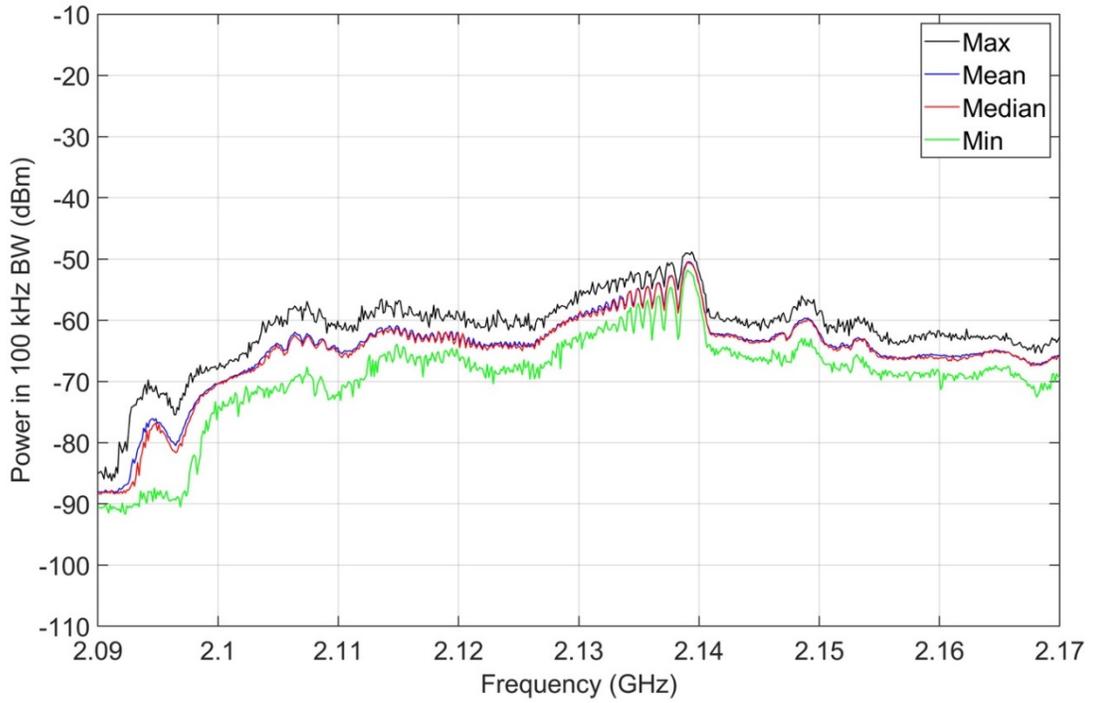


Figure 10. M4 statistics, jammer on, 2090-2170 MHz, inside targeted prison housing block.

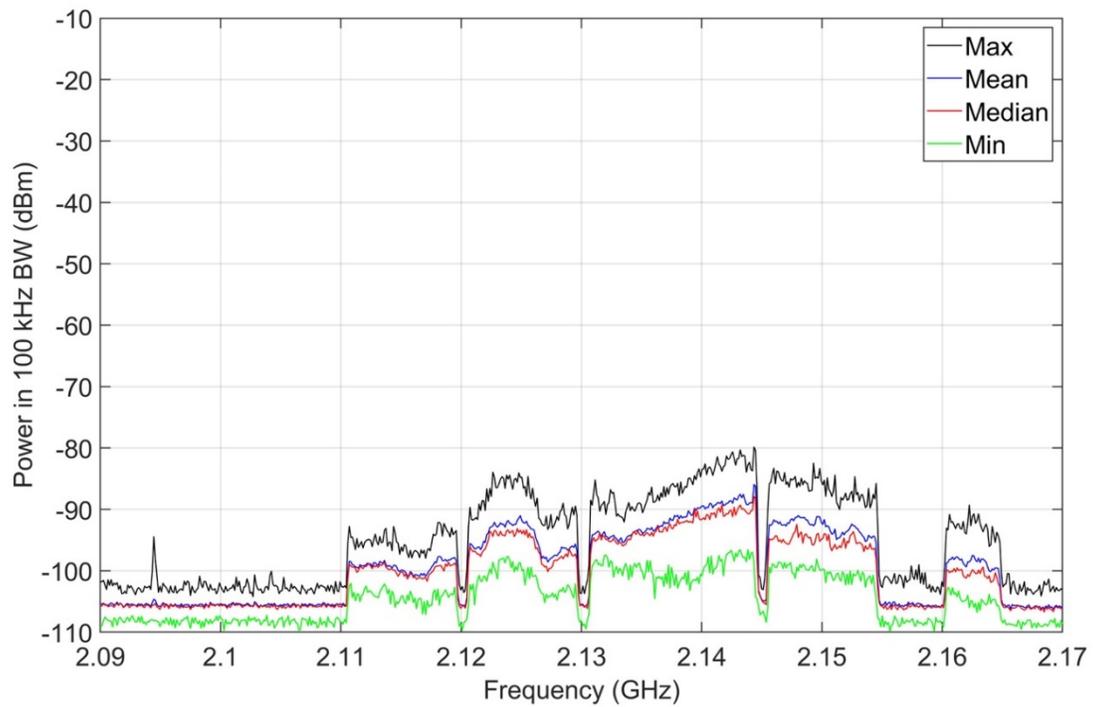


Figure 11. M4 statistics, jammer off, 2090-2170 MHz, inside targeted prison housing block.

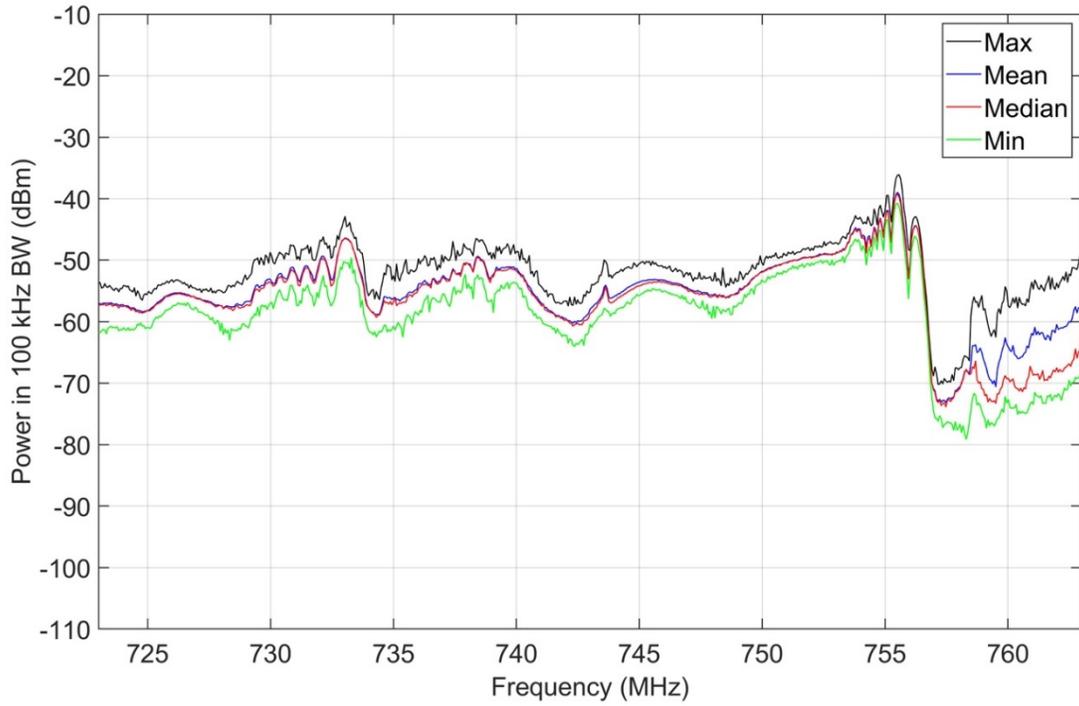


Figure 12. M4 statistics, jammer on, 723-763 MHz, outdoor location O-1.

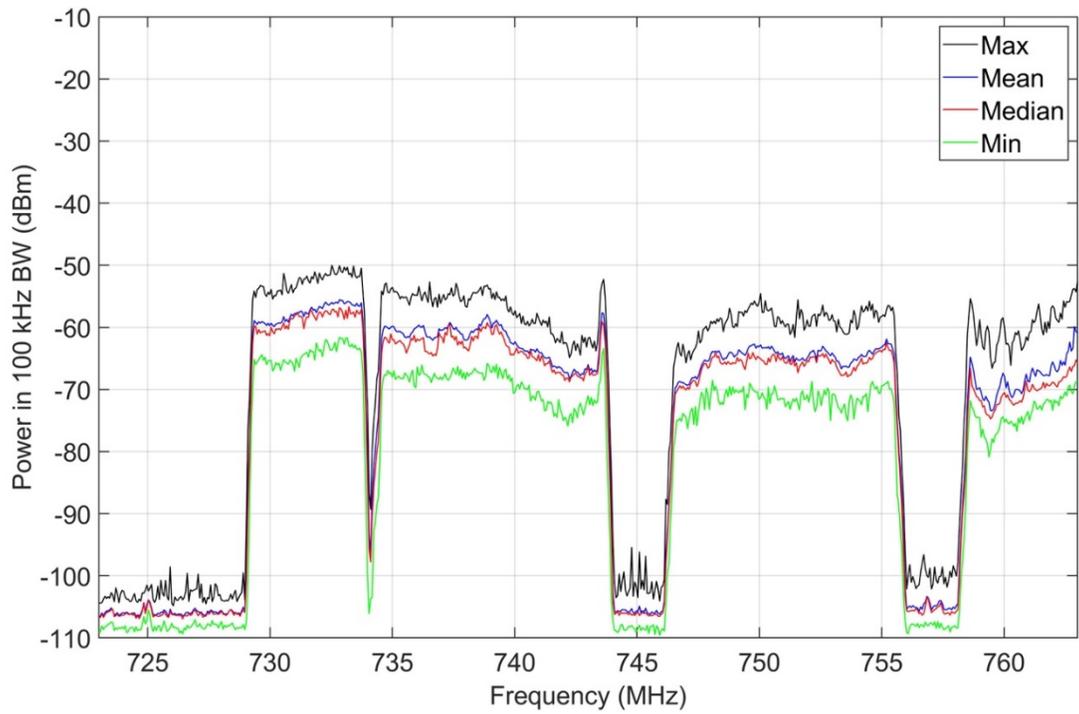


Figure 13. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.

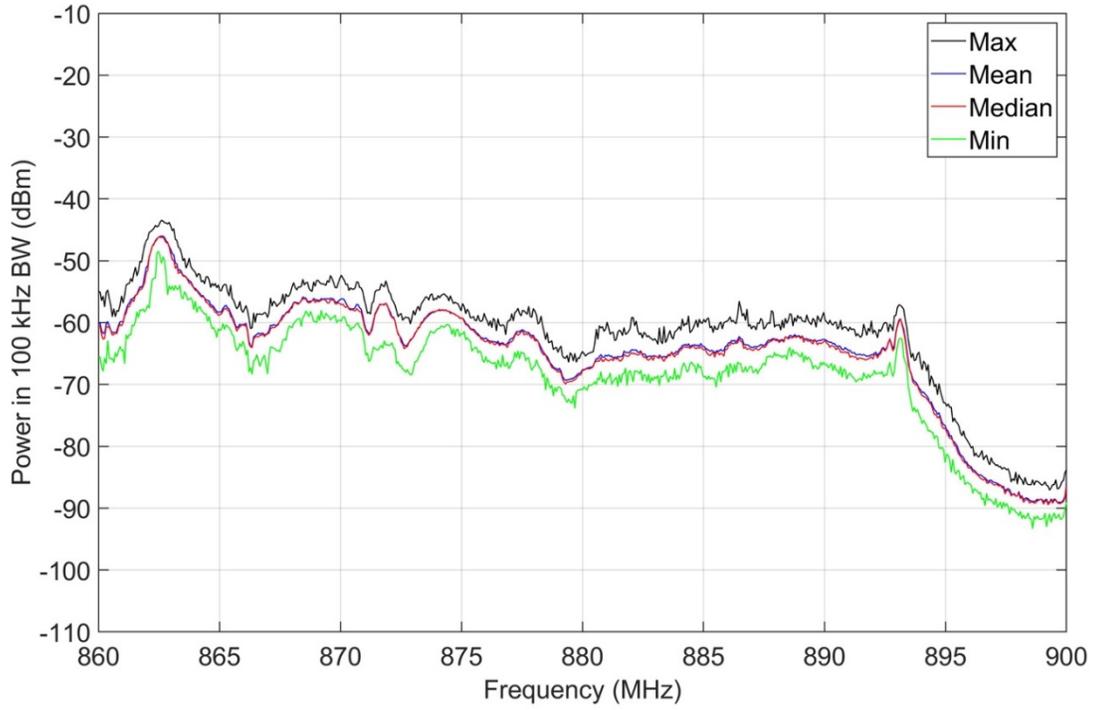


Figure 14. M4 statistics, jammer on, 860-900 MHz, outdoor location O-1.

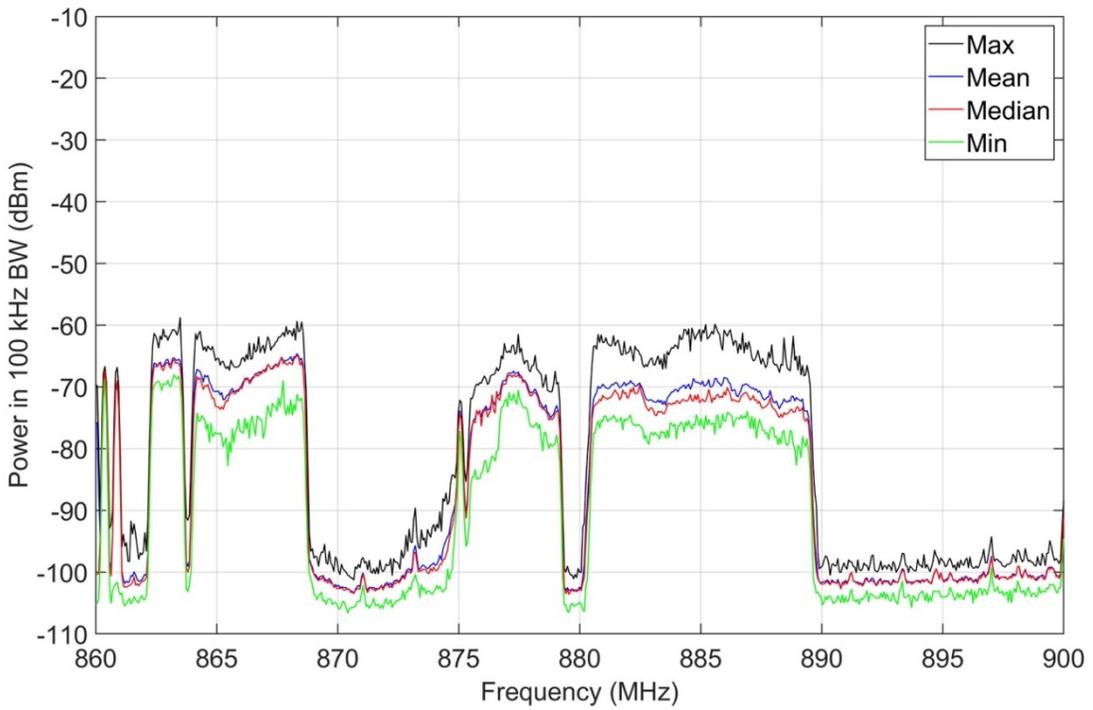


Figure 15. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.

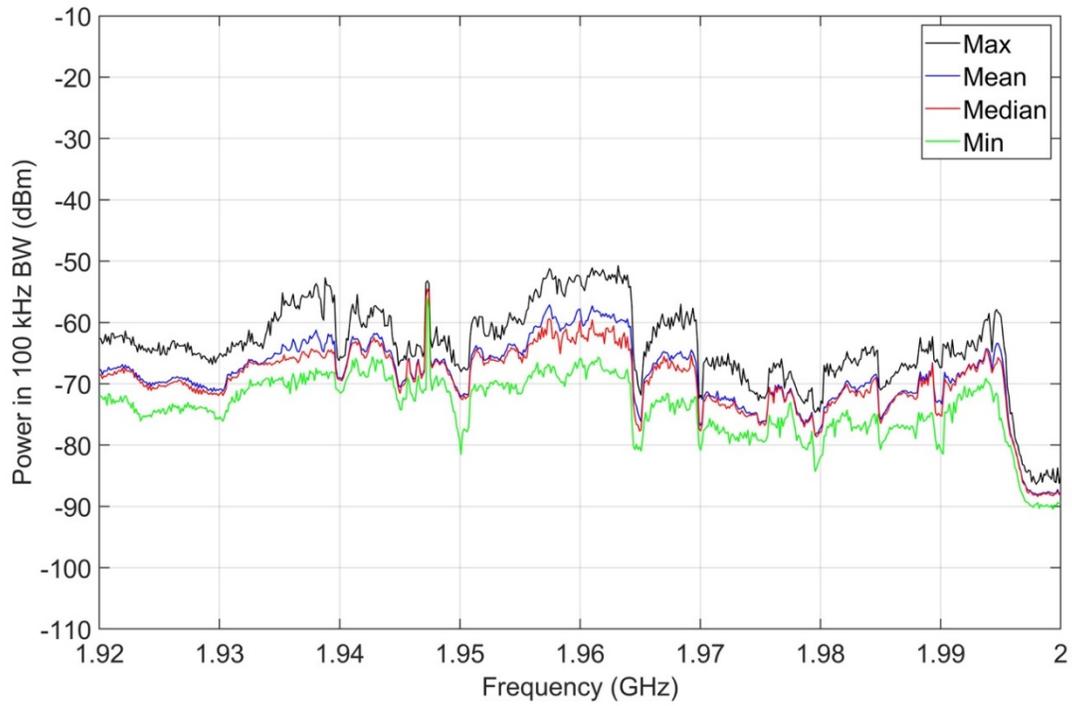


Figure 16. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-1.

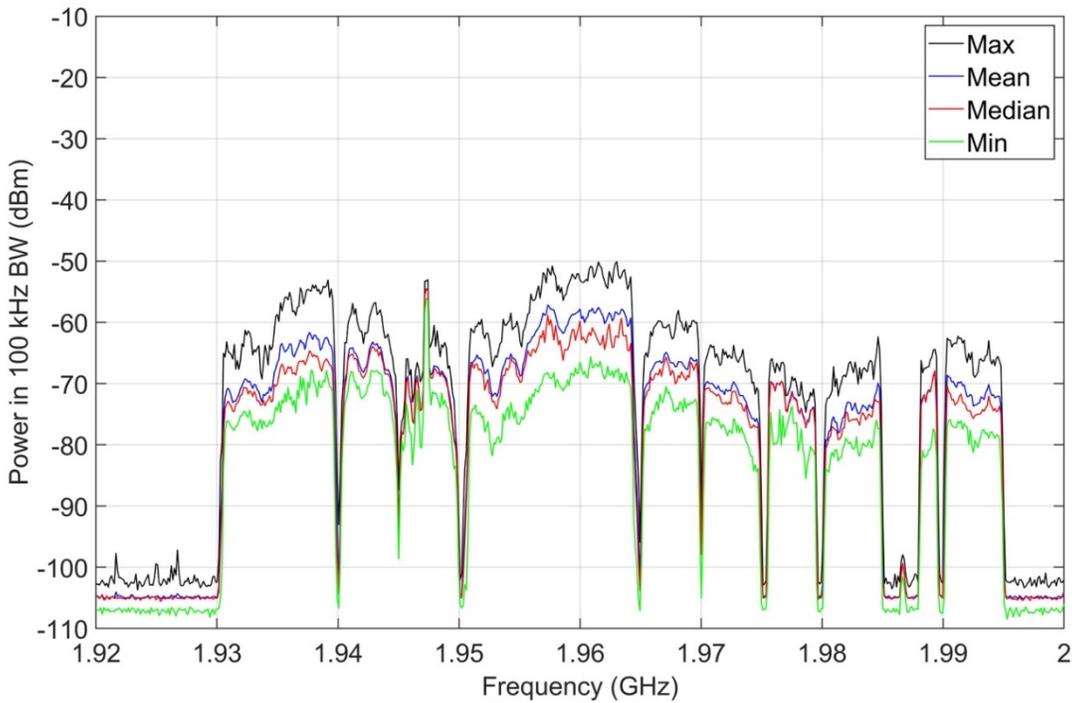


Figure 17. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.

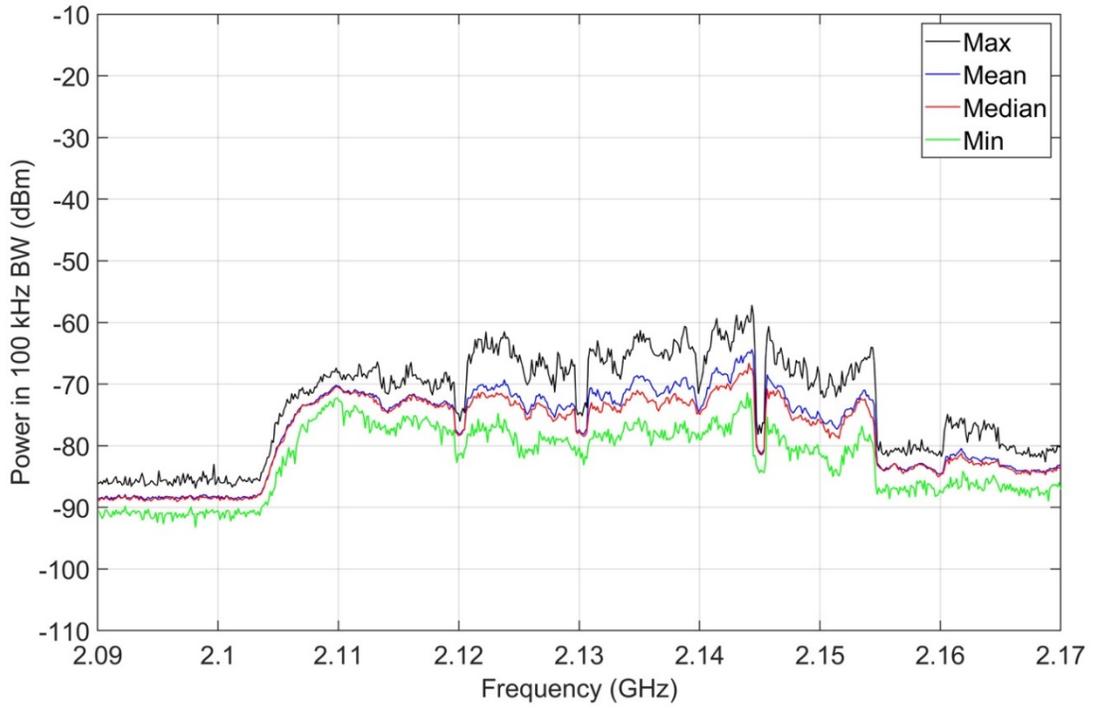


Figure 18. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-1.

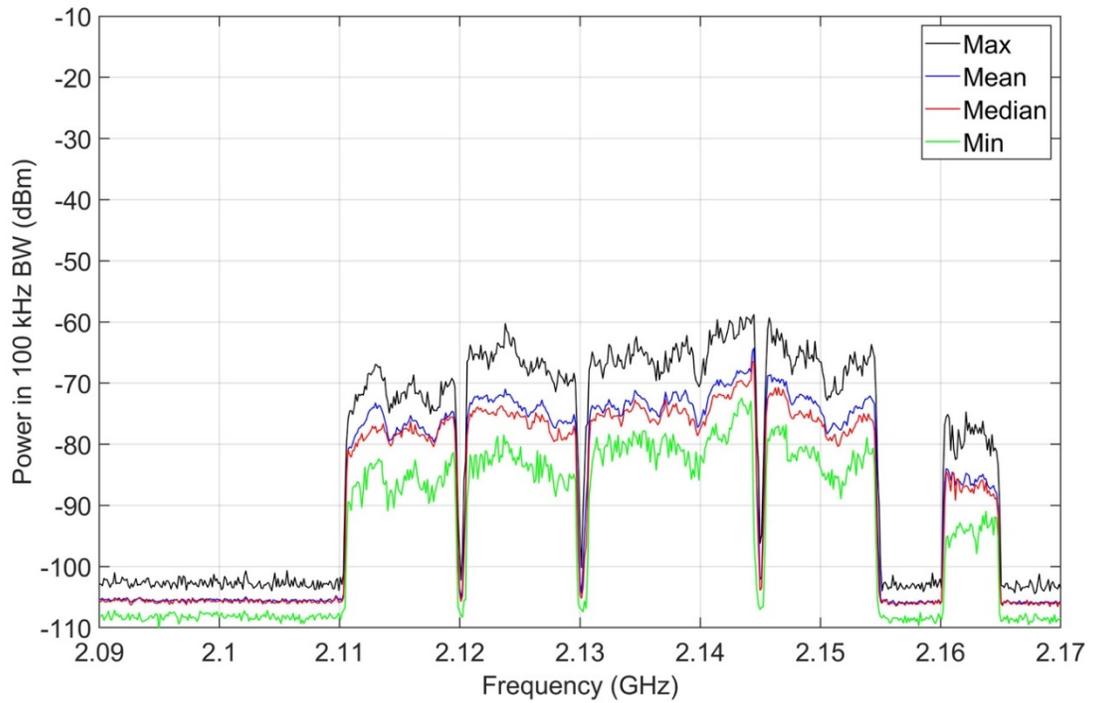


Figure 19. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.

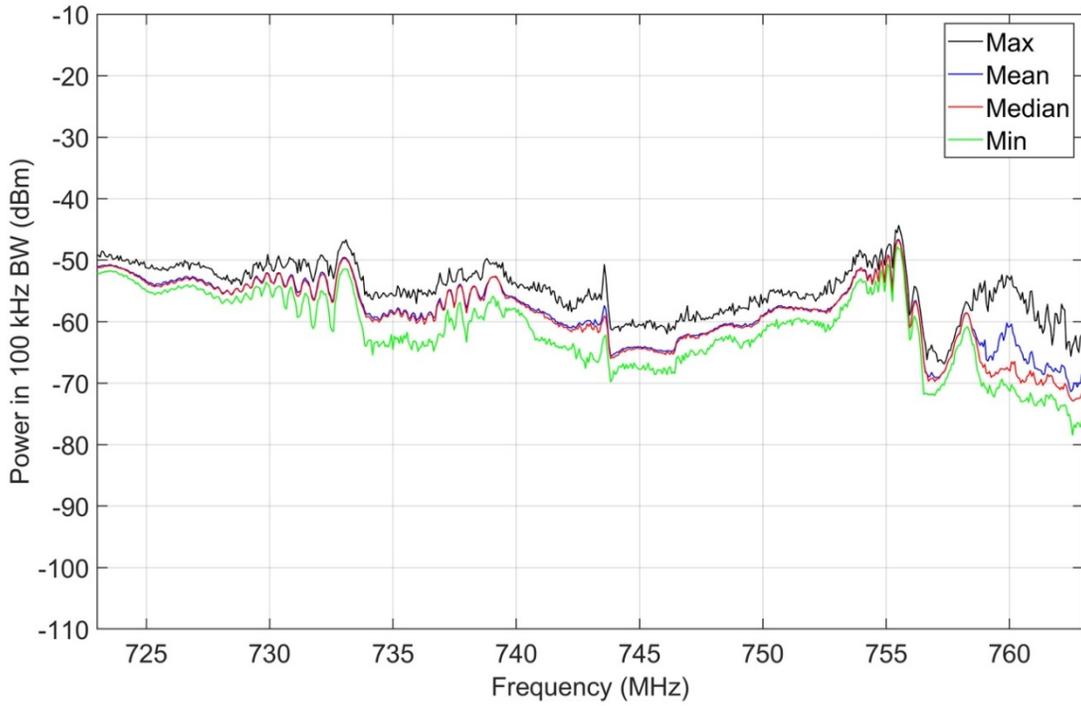


Figure 20. M4 statistics, jammer on, 723-763 MHz, outdoor location O-2.

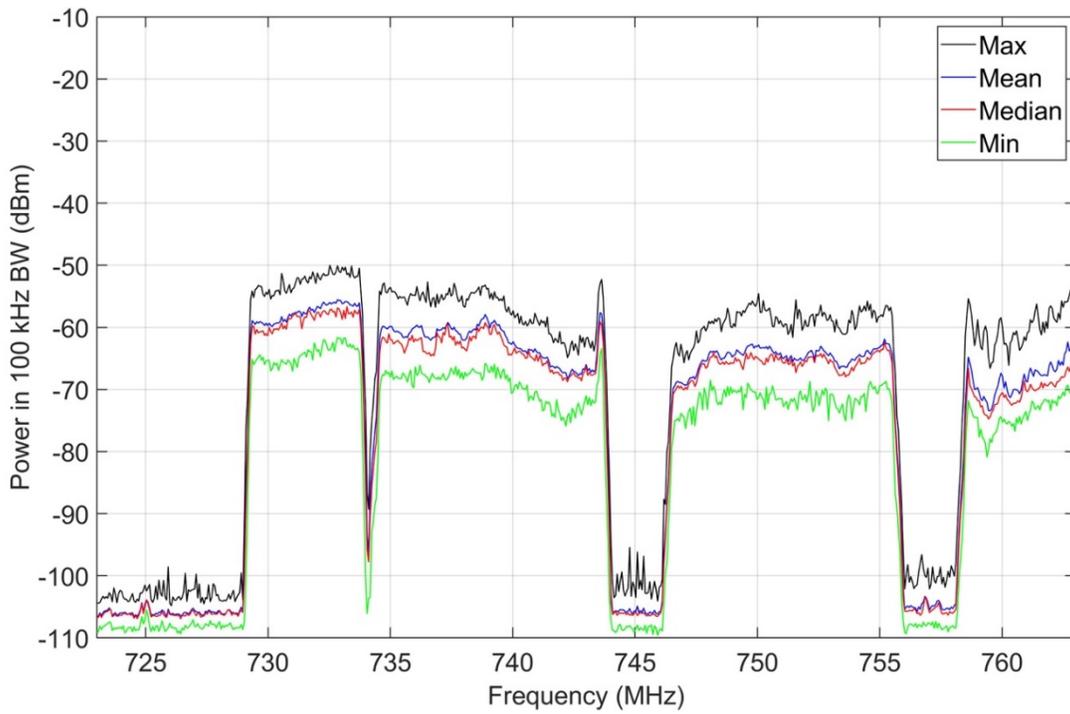


Figure 21. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.

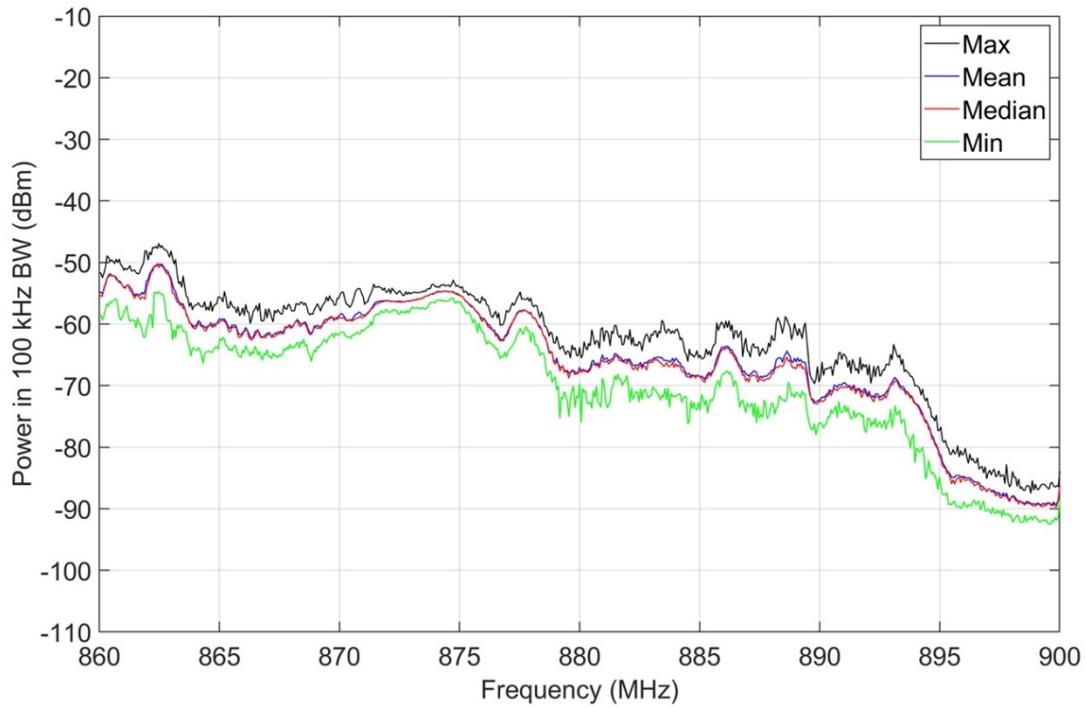


Figure 22. M4 statistics, jammer on, 860-900 MHz, outdoor location O-2.

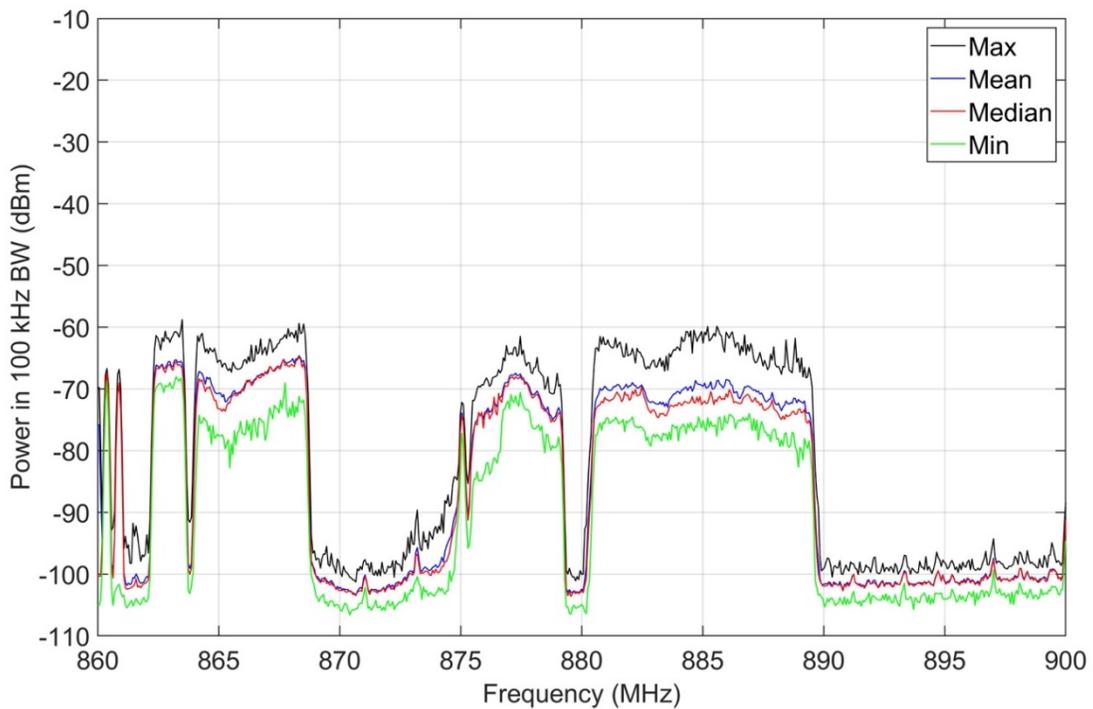


Figure 23. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.

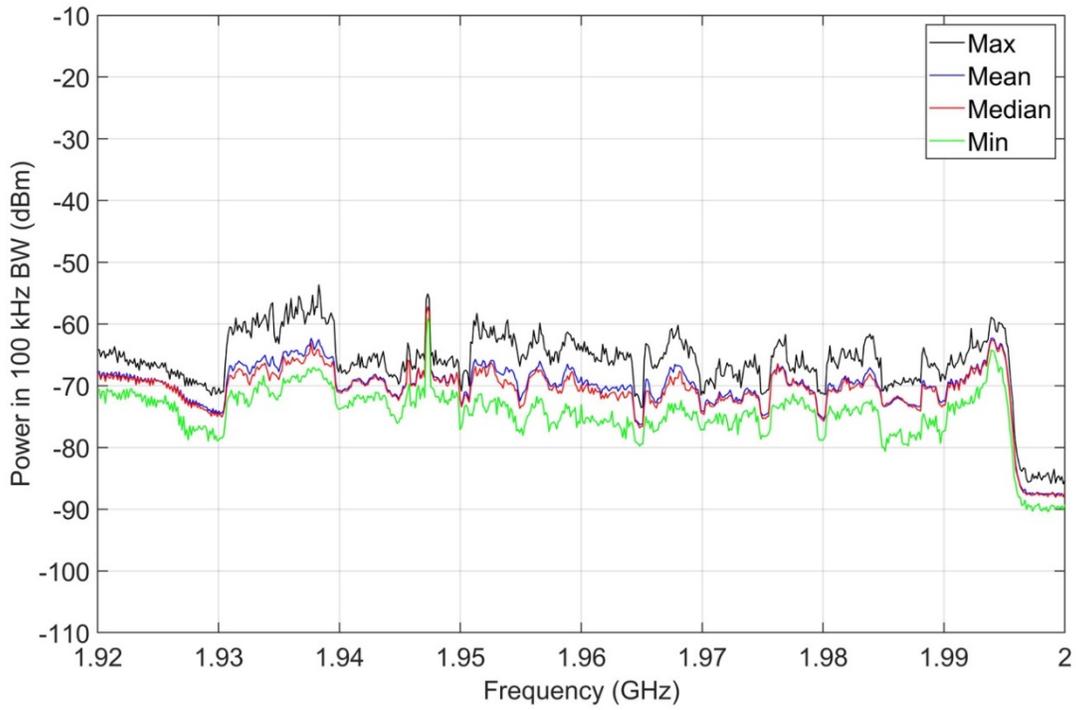


Figure 24. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-2.

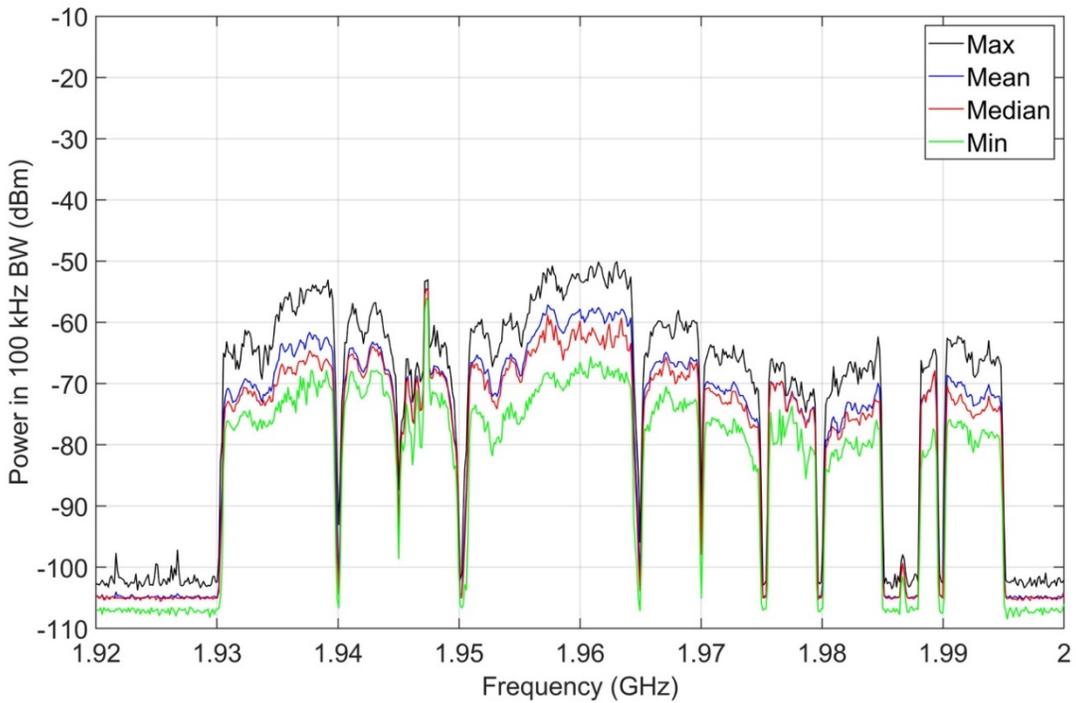


Figure 25. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.

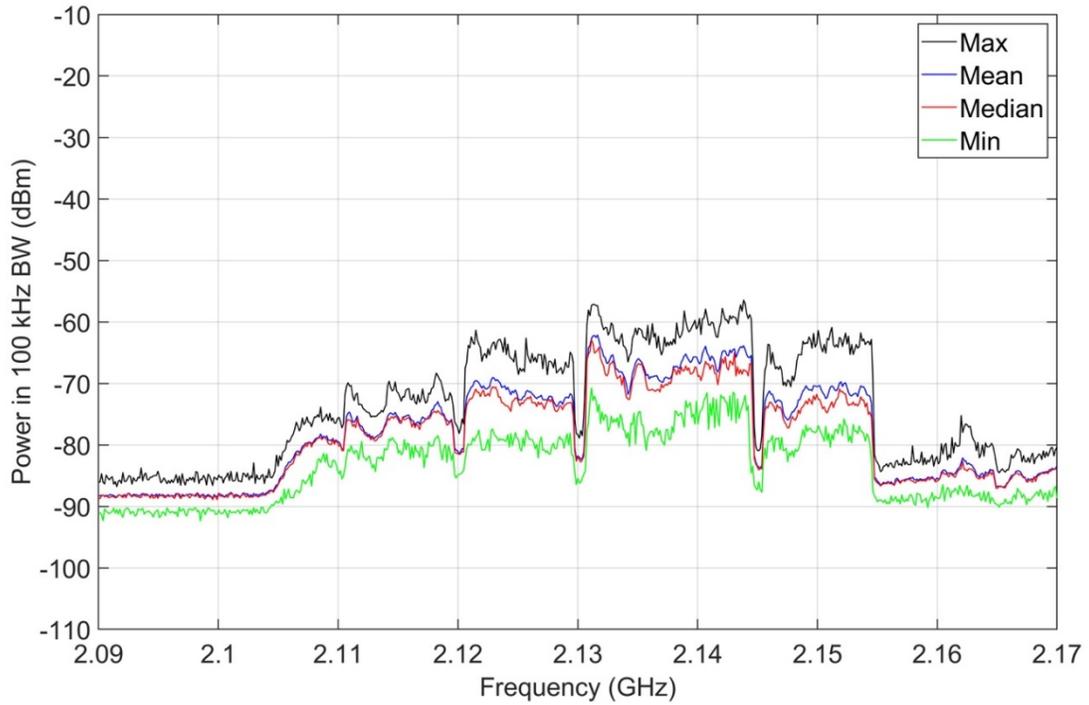


Figure 26. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-2.

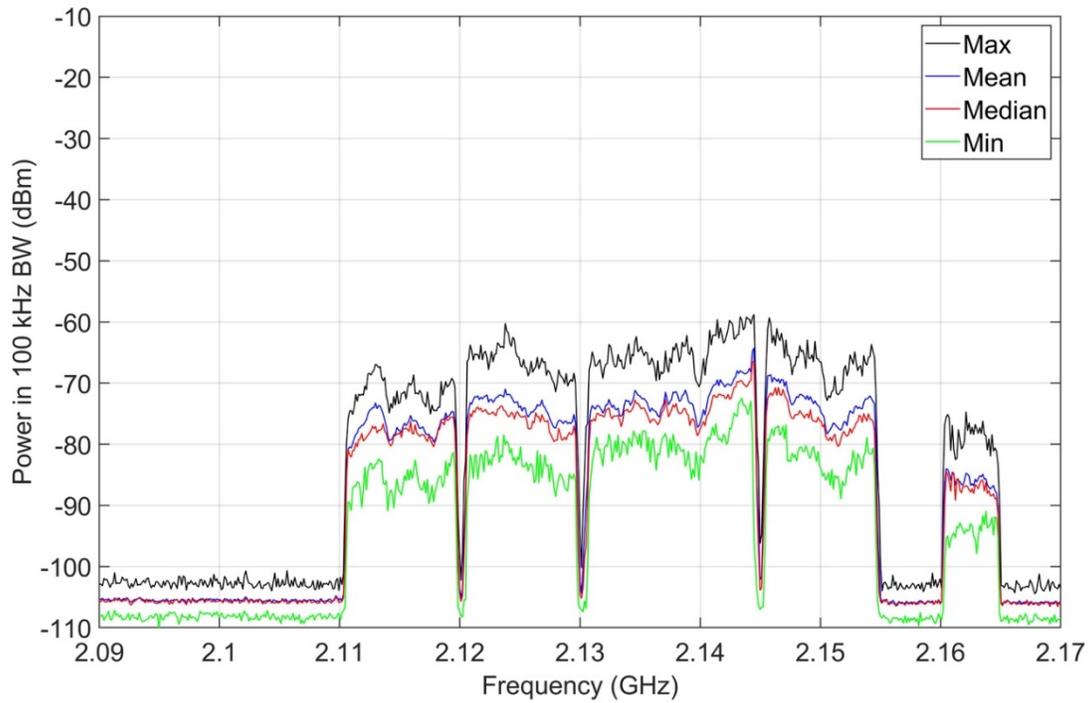


Figure 27. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.

5. DATA ANALYSIS

5.1 Jammer Signal Relative to CMRS Signals

Within the targeted housing unit, the jammer signal was substantially stronger than the ambient CMRS signals. Outdoors, the jammer signal power was reduced but was still strong compared to the ambient CMRS signals. Table 6 shows the relative peak power levels of CMRS and jammer signals at all measurement locations, based on visual examination of the data graphs.

Table 6. Jammer Power Levels Relative to CMRS Signals, Mean Peak Statistics, 100 kHz Bandwidth

CMRS Band (MHz)	Indoors		Outdoors O-1 (20 m)		Outdoors O-2 (40 m)	
	Jammer (dBm)	CMRS (dBm)	Jammer (dBm)	CMRS (dBm)	Jammer (dBm)	CMRS (dBm)
729–757	-40	-80	-55	-65	-50 to -60	-60 to -65
869–894	-50	-90	-60 to -70	-70	-55 to -65	-70
1930–1990	-55	-90	-60 to -70	-65 to -75	-70	-60 to -75
2110–2155	-60	-95	-75	-75	-70	-75

Indoors, mean peak jamming signals were 35 to 40 dB stronger than the mean peak ambient CMRS signals. Outdoors, the mean peak jamming signals exceeded the mean peak ambient CMRS signals by about 0 to 10 dB.

5.2 Emissions in Defined Jammer Operational Bands

The jammer is natively capable of operating across wide swaths of spectrum up to, we understand, 6 GHz. For the Broad River measurements, we requested that the jammer operate in the four CMRS bands listed in this report (see, for example, Table 6 above). Based on the measured emission spectra (e.g., Figures 4, 6, 8, and 10), the jammer did not appear to entirely confine its operations to the CMRS bands that had been requested. In Figures 4, 6, and 8 the jammer emissions went below the lower CMRS band edges. In Figure 10 the jammer emissions went above the upper edge of the requested CMRS band. We do not know why this occurred, as the jammer control was in an out-of-state location as noted above.

5.3 Peak Detected Jammer Power as a Function of Receiver Bandwidth (Peak Detected Bandwidth Progression Rate)

The data graphs taken in 100 kHz and 1 MHz bandwidth can be used to determine the rate at which peak-detected jammer power varies as a function of receiver bandwidth. Table 7 shows these differences between the 100 kHz and 1 MHz spectra.

Table 7. Differences Between Mean Peak-Detected Jammer Emission Spectra for 100 kHz and 1 MHz Bandwidths (from Indoors Data)

CMRS Band (MHz)	Location: Figure (100 kHz)	L, C, H Power Levels (dBm)			Location: Figure (1 MHz)	L, C, H Power Levels (dBm)			Deltas: 1 MHz minus 100 kHz (dB)		
		L	C	H		L	C	H	L	C	H
729–757	4	-40	-38	-35	A-1	-25	-25	-25	15	13	10
869–894	6	-40	-50	-45	A-3	-25	-32	-30	15	18	15
1930–1990	8	-55	-50	-40	A-5	-38	-35	-30	17	15	10
2110–2155	10	-70	-60	-65	A-7	-55	-42	-48	15	18	17

The power levels in the third and fifth columns of Table 7 are those of the mean peak curve measured at the lowest, center, and highest (L, C, and H in the table) frequencies in the CMRS band. The differences between the corresponding values in the two bandwidths are shown in the last column of the table.

The average of the decibel differences¹⁸ is 14.8 dB. The variance¹⁹ of decibels is 6.6 dB. The standard deviation²⁰ of decibels is 2.6 dB.

So the rate of change of the mean peak-detected jammer power is $14.8 \times \log(B_2/B_1) \pm 2.6 \times \log(B_2/B_1)$, where B_1 and B_2 are any two bandwidths. According to [9], the peak-detected relationship would go as $10 \times \log$ of bandwidth ratio for uniformly distributed spectrum energy (and likewise for Gaussian noise) and would go as $20 \times \log$ of bandwidth ratio for pulsed signals. The empirically determined coefficient of 14.8 for the jammer signal is consistent with the signal being somewhat, but not entirely, pulse-like in a bandwidth. This relationship is further explored in Appendix B of [10]. A similar result was obtained for another LFM jammer evaluated in a previous NTIA study [10]. In that study the coefficient of the rate of change was $16.7 \text{ dB} \pm 7 \text{ dB}$, with a standard deviation of 2.6 dB. The rate-of-change coefficient values between these two studies overlap each other, as would be expected for two jammers that both use the same (LFM) signal modulation.

Using a mean decibel rate-of-change factor of $15.8 \times \log(B_2/B_1)$ between the two studies, the expected relative offset between measured power in 100 kHz and the power that would be seen in 180 kHz (a CMRS RB bandwidth) would be $15.8 \times \log(180/100) = +4.0 \text{ dB}$. This is the correction factor that would be added to the 100 kHz power level data to find the power in an LTE RB of 180 kHz in the two studies.

¹⁸ Sum of all decibel differences = 178, divided by 12 data point values.

¹⁹ Sum of all of the squared decibel differences between each of the 12 deltas and the average of 14.8 dB, divided by 12.

²⁰ Square root of variance.

6. SUMMARY

- 1) A contraband wireless device micro-jammer operating in four CMRS bands was temporarily installed and operated under an STA for a single day inside a maximum security housing unit at the Broad River Correctional Institution near Columbia, South Carolina. Broad River is operated by SC DOC. This jammer, installed inside a utility shaft, radiated its signal through wall structures (concrete and steel, unspecified thickness) to cover a targeted indoor area comprising roughly half of one floor of the housing unit.
- 2) The jammer was a single unit containing a single transmitter and associated antenna. The transmitter produced an LFM signal that sequentially covered the CMRS bands 729-757 MHz, 869-894 MHz, 1930-1990 MHz, and 2110-2155 MHz. The jammer transmitter produced 2 W, delivered into a radiating antenna (unknown polarity) of +0.5 dBi gain.
- 3) The jammer transmitter was operated in *on* versus *off* states with emission measurements performed at three locations: one place inside the targeted indoor zone and two non-targeted places outdoors, adjacent to the targeted indoor zone. The outdoor locations were 20 m (66 ft) and 40 m (132 ft) outside the building, with clear LOS to the housing unit's exterior wall.
- 4) NTIA performed in-band (CMRS band) measurements of the jammer emissions relative to the ambient CMRS signal levels at the indoor (targeted) and outdoor (non-targeted) measurement locations. The results of those measurements are provided in this report.
- 5) Our data show that inside the targeted jamming zone (the prison housing unit), the jammer peak power signal levels substantially exceeded those of the CMRS signals, by 35 to 40 dB. At the outdoor measurement locations, the jamming signals were lower but still exceeded the ambient CMRS signals by 0 to 10 dB.
- 6) Jammer transmitter detected peak power measurements show that the measured (received) power varies as $14.8 \times \log(\text{receiver IF bandwidth})$ for receiver bandwidths between 100 kHz to 1 MHz. Combining this value with the result from an earlier NTIA study, the typical rate of variation for LFM jammers appears to be $15.8 \times \log(\text{receiver IF bandwidth})$. This rate of variation can be applied to future EMC studies examining jamming of receivers with bandwidths in the range of 100 kHz to 1 MHz.

7. CONCLUSIONS

The data scans taken indoors at Broad River show that jammer power levels exceeded the ambient indoor CMRS downlink signal levels by 35 to 40 dB (which is four orders of magnitude in linear terms). The corresponding scans taken outdoors showed jamming power levels that still substantially exceeded (on the order of 10 dB, an order of magnitude) the ambient downlink levels there. As with previous studies such as [10], the results of this study are idiosyncratic to the particular facility where the demonstration occurred, and aggregate effects were not examined.

Accepted quantitative engineering criteria for jammer effectiveness and harmful interference do not presently exist. Therefore, we do not know, and cannot currently assess, the extent to which a CMRS wireless device can or cannot perform its intended communications function in the presence of the measured jammer power levels. Likewise, we cannot assess the extent to which the jamming power that leaked outdoors did or did not have the potential to cause harmful interference to non-targeted cellular phones in the prison yard or anywhere else. The data in this report can be used for such analysis in the future, if (or when) these criteria are eventually developed.

To the best knowledge of the authors, prior to the measurements, no assessment was made of the impact of specified jamming power levels (including EIRP outputs) on the ability of a CMRS wireless device operating within the housing unit to perform its intended communications function. Nor was any *a priori* engineering assessment possible of the amount of power that would leak out of the housing unit, since propagation data were lacking. The jammer transmitter power, antenna characteristics, and antenna locations were all, to the best knowledge of the authors, simply what a manufacturer had developed for a general product line.

In the study described in this report and in previous studies ([5], [6], [10], [12]) we have gathered many numbers describing jammer signal levels inside and outside prison housing units and even in anechoic chambers. But, as existing literature in this area ([13], [14]) makes clear, the technical community lacks agreed technical criteria to interpret what these numbers mean.

Noting this gap in knowledge, we recommend that quantitative engineering criteria for jammer effectiveness against contraband wireless devices (e.g., S/J thresholds) and for harmful interference to non-targeted wireless receivers (e.g., S/I thresholds) be developed if jamming technology is to be further analyzed for application in prison environments. A more thorough and systematic approach is needed to arrive at a determination of such threshold values. Careful theoretical analysis, simulation and modeling should be used in conjunction with selected measurements in controlled laboratory environments to determine:

- *At what power level will an interfering signal prevent service to CMRS wireless devices inside a particular building?*
- *At what power level will an interfering signal prevent service to CMRS wireless receivers operating outside a building where interfering signals exist?*

Laboratory and *in situ* work should go hand-in-hand, since only *in situ* work can describe:

- CMRS-band signal strength inside a particular building
- CMRS-band signal strength outside a particular building, beyond which harmful interference to non-targeted receivers will not be allowed
- Radio propagation factors inside a particular building

These propagation measurements can be performed by minimally trained personnel using smart-phone applications that have already been developed. CMRS band occupancy measurement surveys can likewise be performed by minimally trained personnel inside prisons using pre-programmed, handheld, battery-powered measurement and recording equipment. The resulting data can be analyzed to understand the idiosyncracies of a particular building, but it provides no information as to whether a CMRS wireless device can or cannot perform its intended communications function in the presence of a competing signal of specified strength.

8. REFERENCES

- [1] Department of Justice, “Bureau of Prisons Tests Micro-Jamming Technology in Federal Prison to Prevent Contraband Cell Phones,” January 17, 2018 press release.
<https://www.justice.gov/opa/pr/bureau-prisons-tests-micro-jamming-technology-federal-prison-prevent-contraband-cell-phones>.
- [2] Bureau of Prisons, “Micro-Jamming Technology Testing: Part of ongoing effort to prevent contraband cell phone use,” January 24, 2018 press release.
https://www.bop.gov/resources/news/20180124_tech_testing.jsp.
- [3] Sanders, F. H, J. E. Carroll; G. A. Sanders and R. L. Sole, “Effects of Radar Interference on LTE Base Station Receiver Performance,” NTIA Technical Report 14-499, U.S. Dept. of Commerce, Dec. 2010. <https://www.its.bldrdoc.gov/publications/2742.aspx>.
- [4] Sanders, G. A., J. E. Carroll; F. H. Sanders and R. L. Sole, “Effects of Radar Interference on LTE (FDD) eNodeB and UE Receiver Performance in the 3.5 GHz Band,” NTIA Technical Report 14-506, U.S. Dept. of Commerce, Jul. 2014.
<https://www.its.bldrdoc.gov/publications/2759.aspx>.
- [5] Sanders, F. H., R. T. Johnk, M. A. McFarland and J. R. Hoffman, “Emission Measurement Results for a Cellular and PCS Signal-Jamming Transmitter,” NTIA Technical Report 10-465, U.S. Dept. of Commerce, Oct. 2009.
<https://www.its.bldrdoc.gov/publications/2503.aspx>.
- [6] Sanders, F. H. and R. T. Johnk, “Emission Measurements of a Cellular and PCS Jammer at a Prison Facility,” NTIA Technical Report 10-466, U.S. Dept. of Commerce, May 2010.
<https://www.its.bldrdoc.gov/publications/2504.aspx>.
- [7] Sanders, F. H., R. L. Sole, B. L. Bedford, D. Franc and T. Pawlowitz, “Effects of RF Interference on Radar Receivers,” NTIA Technical Report 06-444, U.S. Dept. of Commerce, Feb. 2006. <https://www.its.bldrdoc.gov/publications/2481.aspx>.
- [8] Sanders, F. H., J. E. Carroll, G. A. Sanders, R. L. Sole, R. J. Achatz and L. S. Cohen, “EMC Measurements for Spectrum Sharing Between LTE Signals and Radar Receivers,” NTIA Technical Report 14-507, U.S. Dept. of Commerce, Jul. 2014.
<https://www.its.bldrdoc.gov/publications/2760.aspx>.
- [9] Sanders, F. H. and R. A. Dalke, “Relationships Between Measured Power and Measurement Bandwidth for Frequency-Modulated (Chirped) Pulses,” NTIA Technical Report 12-488, U.S. Dept. of Commerce, Aug. 2012.
<https://www.its.bldrdoc.gov/publications/2680.aspx>.

- [10] Sanders F. H., R. T. Johnk and E. F. Drocella, "Emission Measurements of a Contraband Wireless Device Jammer at a Federal Prison," NTIA Technical Report TR-18-533, U.S. Dept. of Commerce, Jun. 2018. <https://www.its.bldrdoc.gov/publications/3206.aspx>.
- [11] Sanders, F. H., "Derivations of Relationships Among Field Strength, Power in Transmitter-Receiver Circuits and Radiation Hazard Limits," NTIA Technical Memorandum 10-469, U.S. Dept. of Commerce, Jun. 2010. <https://www.its.bldrdoc.gov/publications/2507.aspx>.
- [12] Drocella, E. F., "Initial Assessment of the Potential Impact from a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers," NTIA Technical Memorandum TM-10-468, U.S. Dept. of Commerce, May 2010. <https://www.its.bldrdoc.gov/publications/2506.aspx>.
- [13] Crozier, R., "NSW faces tough path to expand prison jammer rollout," IT News, July 19, 2018. <https://www.itnews.com.au/news/nsw-faces-tough-path-to-expand-prison-jammer-rollout-497449>
- [14] Howarth, M., "£1m jamming system to block use of mobiles in jails," Scottish Daily Mail, Feb. 12, 2014. <https://www.pressreader.com/uk/scottish-daily-mail/20140212/281685432739897>.

APPENDIX A. JAMMER EMISSIONS MEASURED IN 1 MHz BANDWIDTH

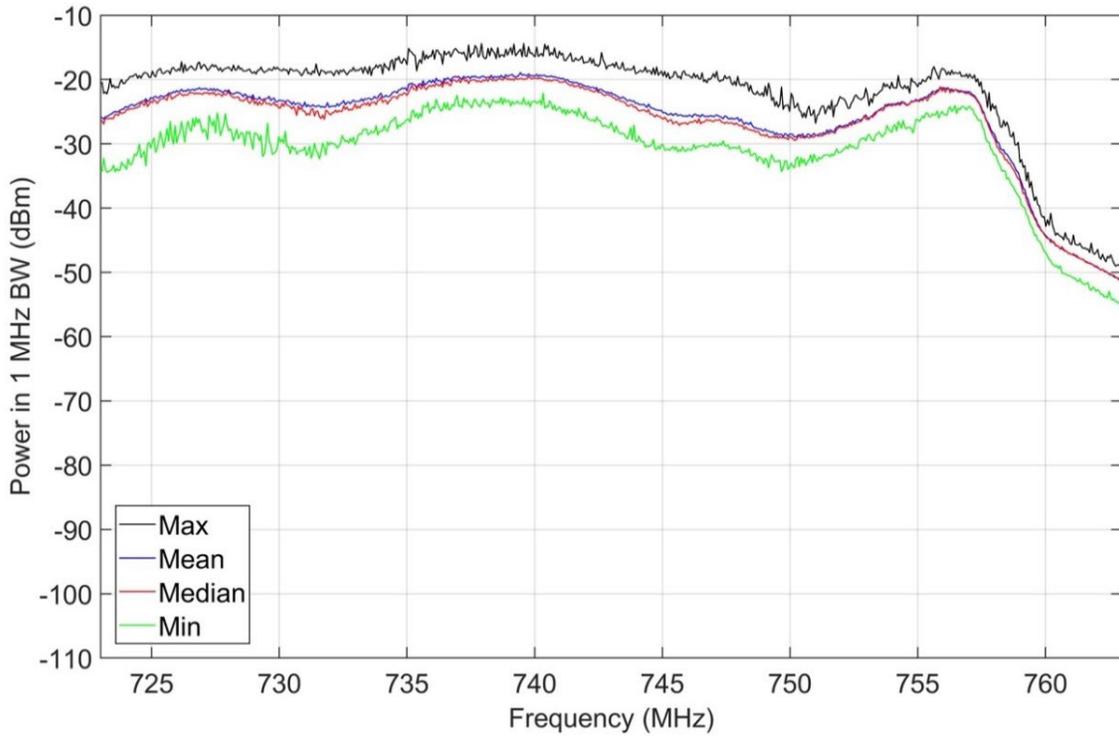


Figure A-1. M4 statistics, jammer on, 723-763 MHz, inside targeted housing unit.

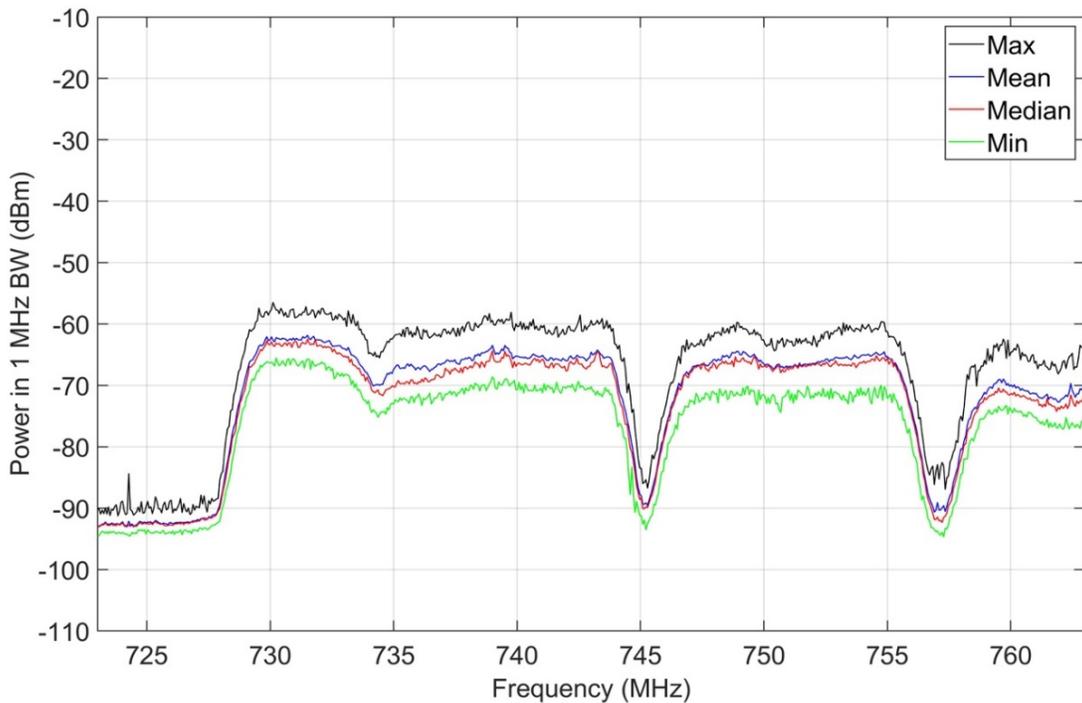


Figure A-2. M4 statistics, jammer off, 723-763 MHz, inside targeted housing unit.

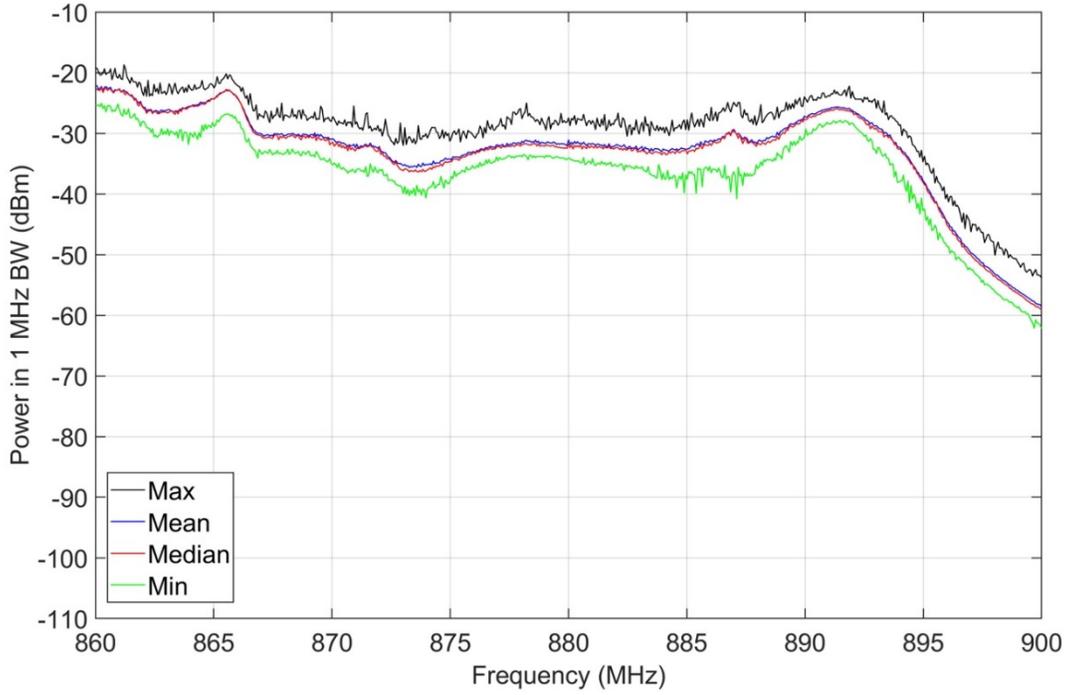


Figure A-3. M4 statistics, jammer on, 860-900 MHz, inside targeted housing unit.

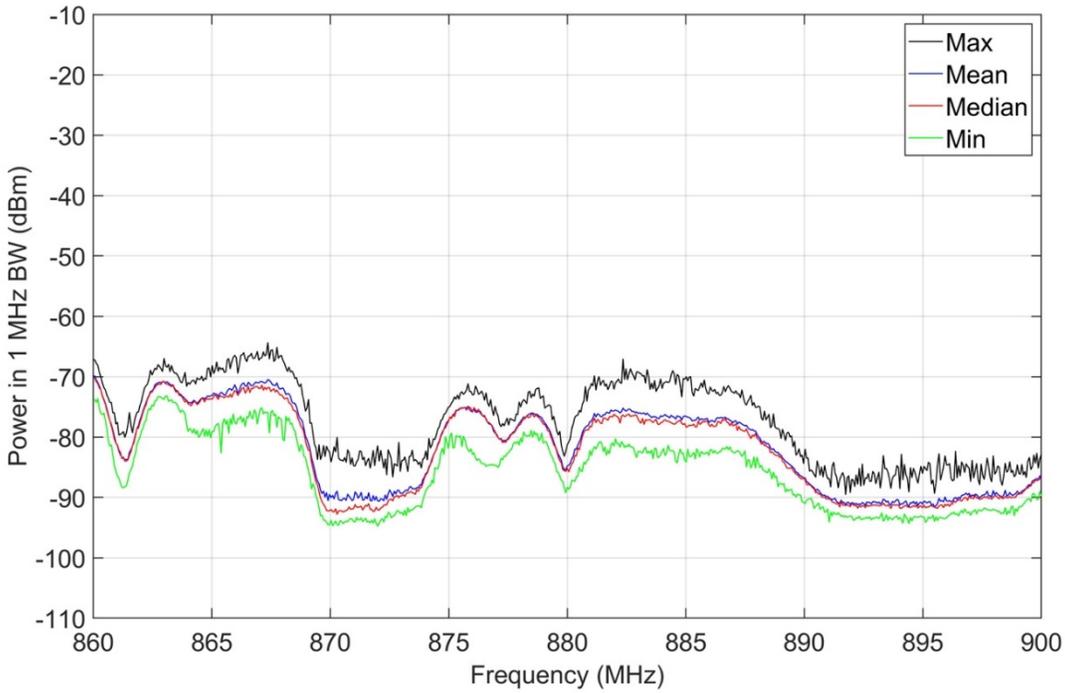


Figure A-4. M4 statistics, jammer off, 860-900 MHz, inside targeted housing unit.

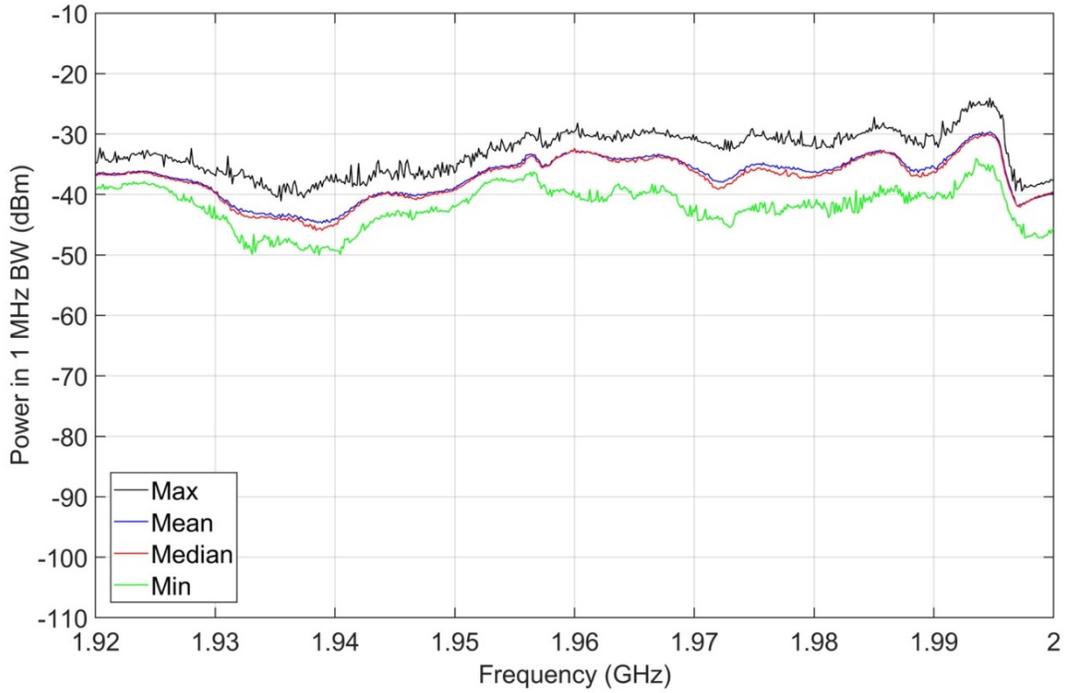


Figure A-5. M4 statistics, jammer on, 1920-2000 MHz, inside targeted housing unit.

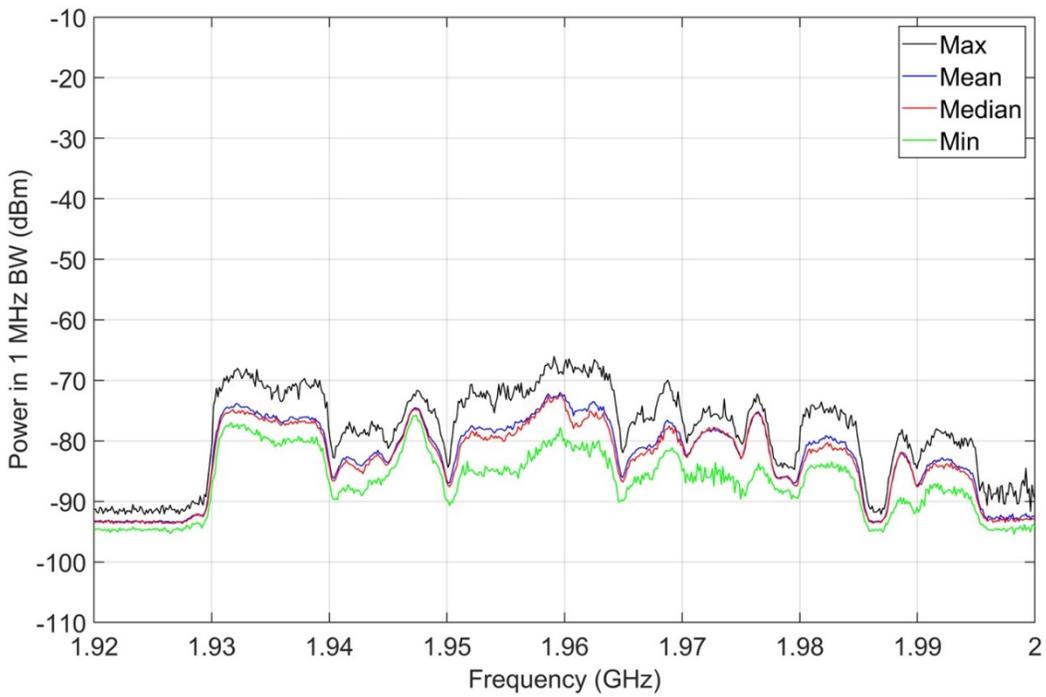


Figure A-6. M4 statistics, jammer off, 1920-2000 MHz, inside targeted housing unit.

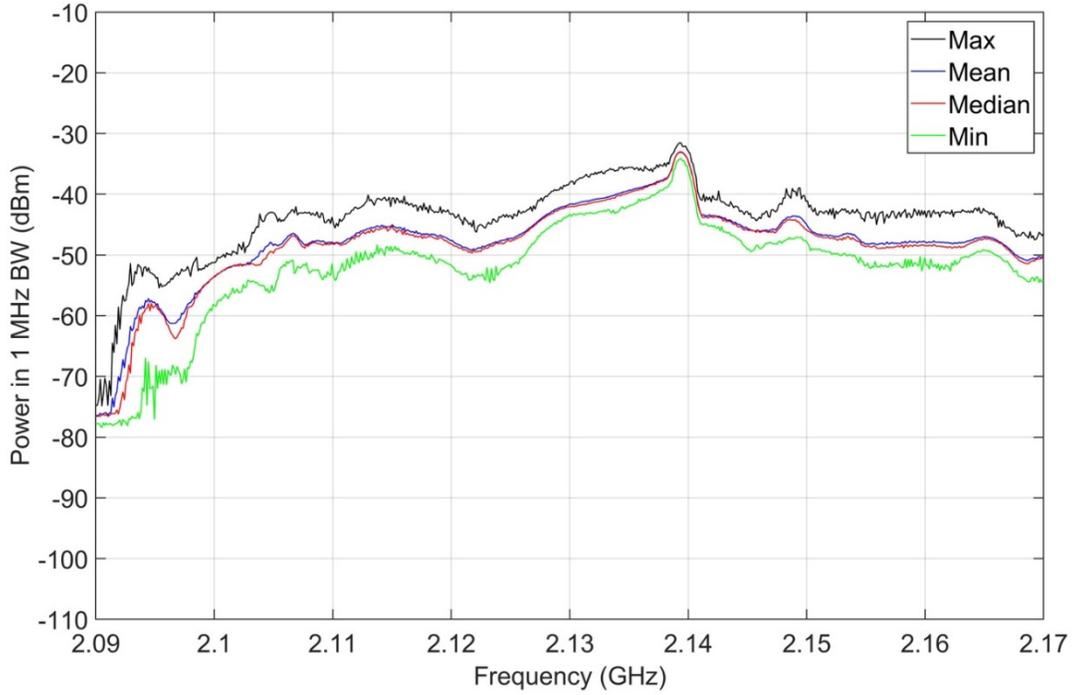


Figure A-7. M4 statistics, jammer on, 2090-2170 MHz, inside targeted housing unit.

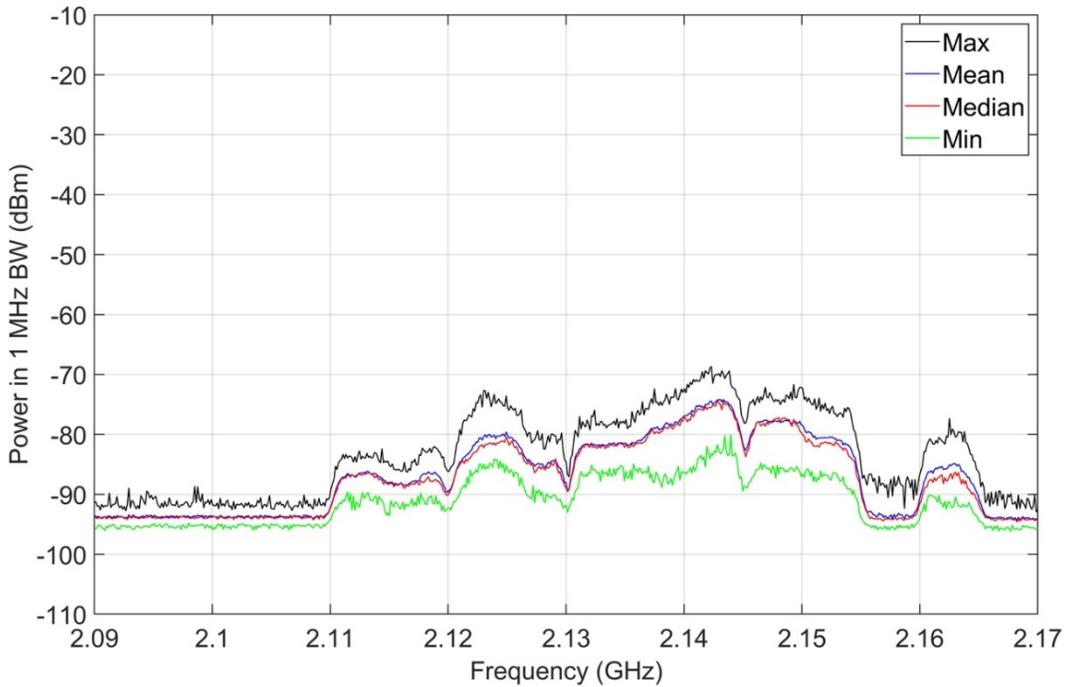


Figure A-8. M4 statistics, jammer off, 2090-2170 MHz, inside targeted housing unit.

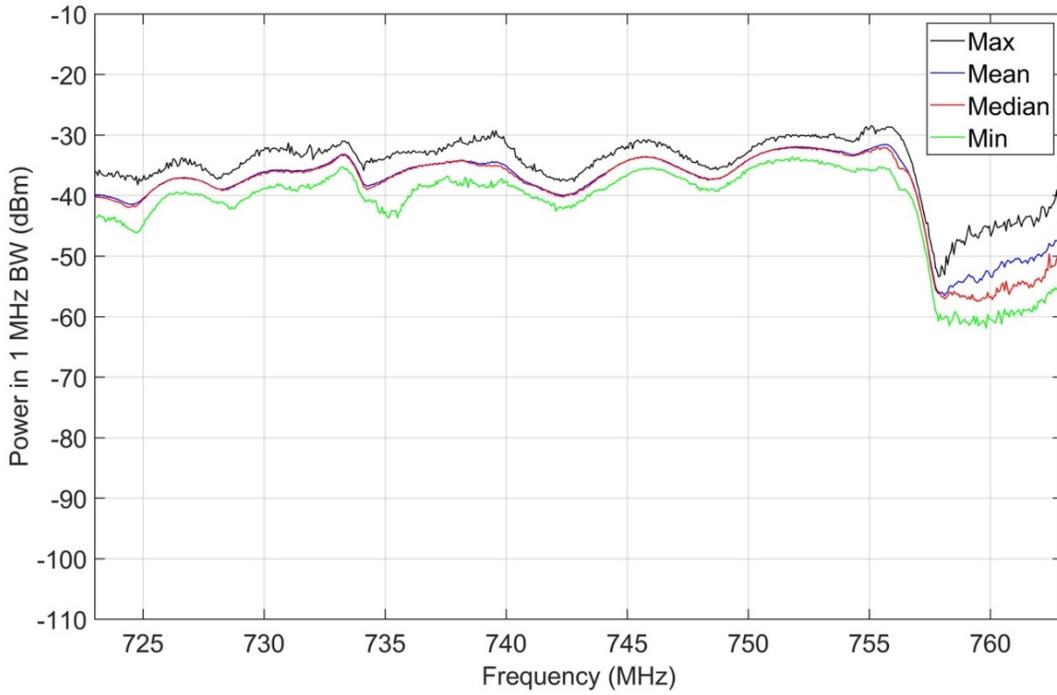


Figure A-9. M4 statistics, jammer on, 723-763 MHz, outdoor location O-1.

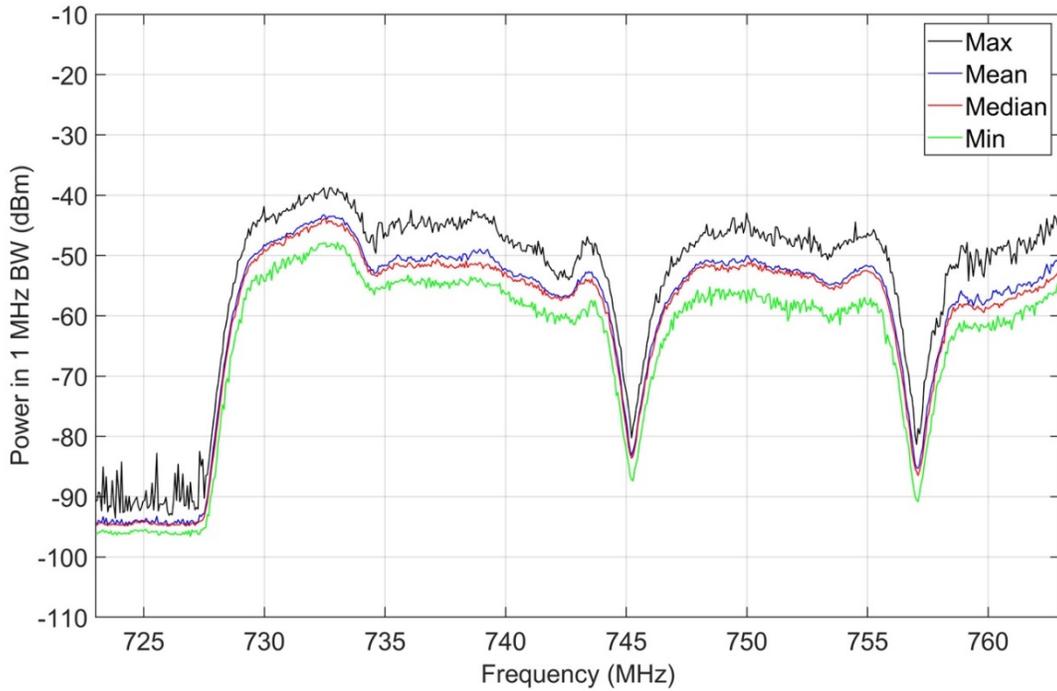


Figure A-10. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.

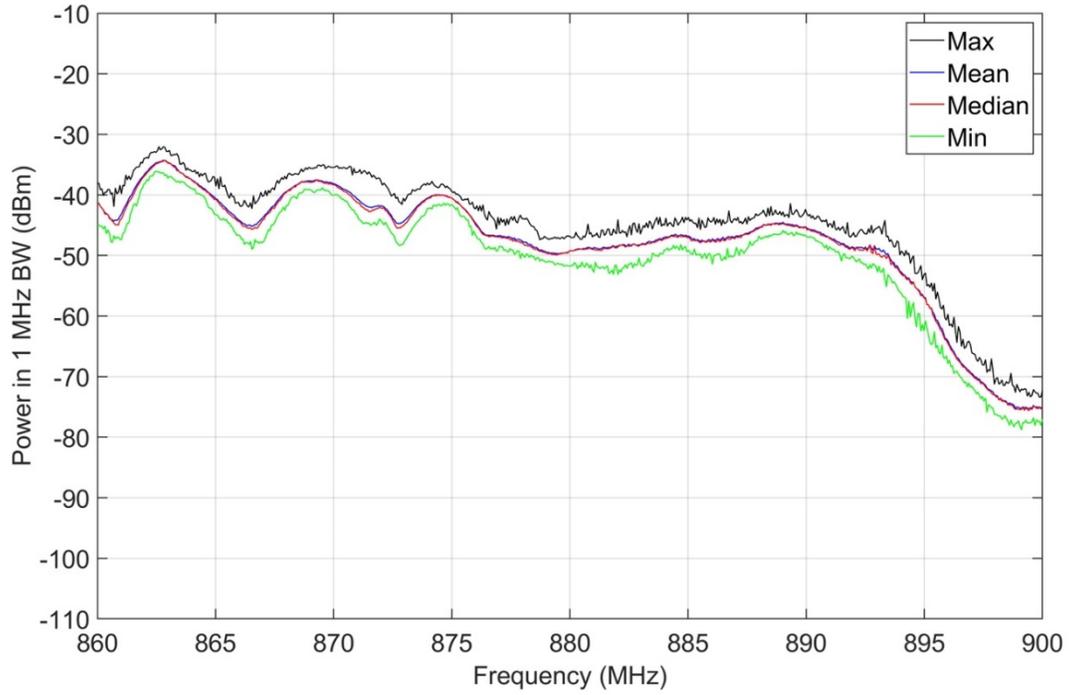


Figure A-11. M4 statistics, jammer on, 860-900 MHz, outdoor location O-1.

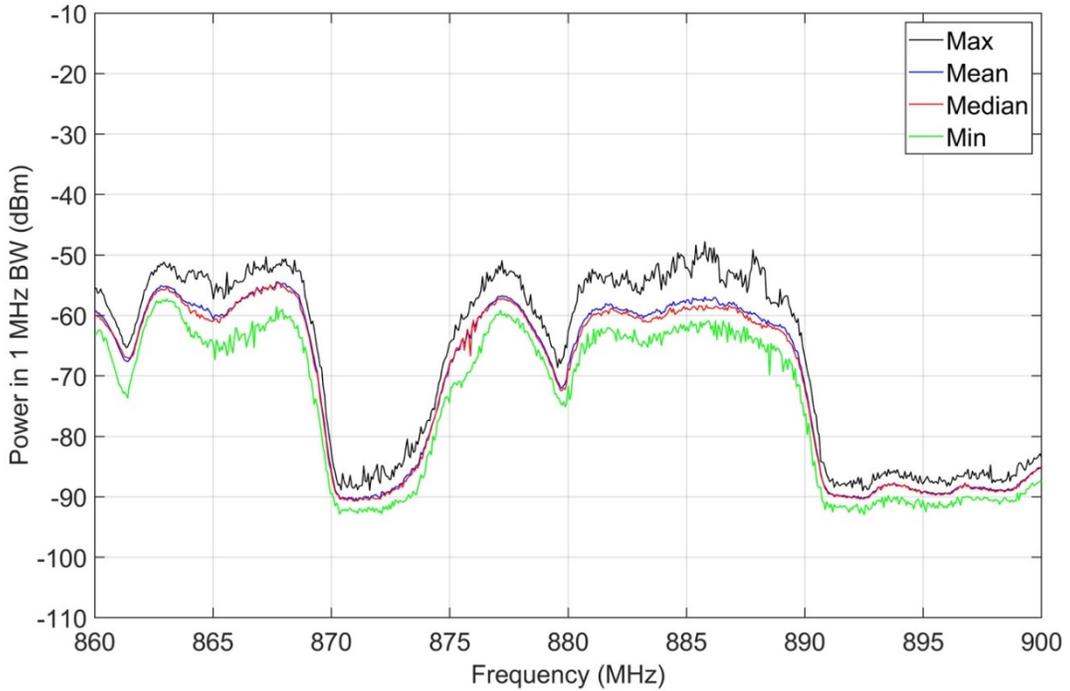


Figure A-12. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.

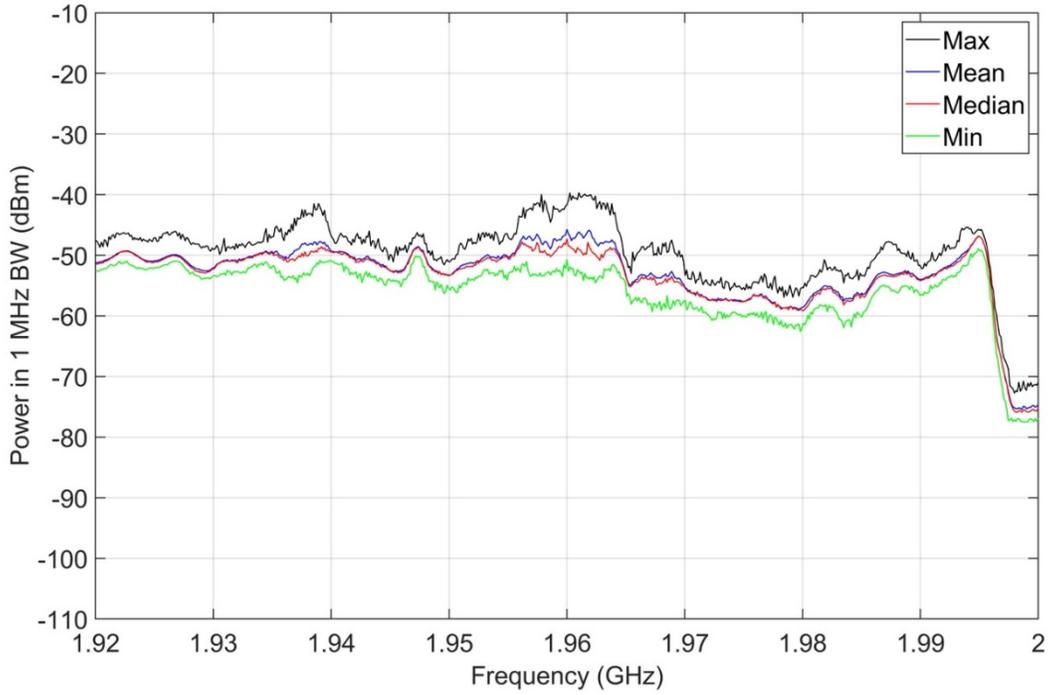


Figure A-13. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-1.

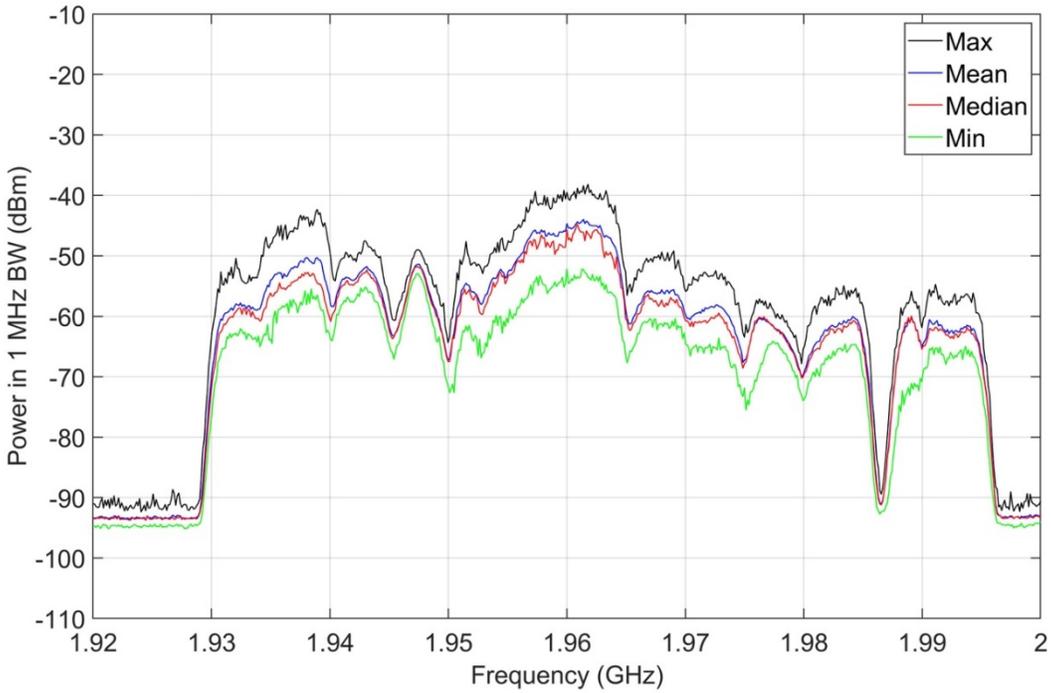


Figure A-14. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.

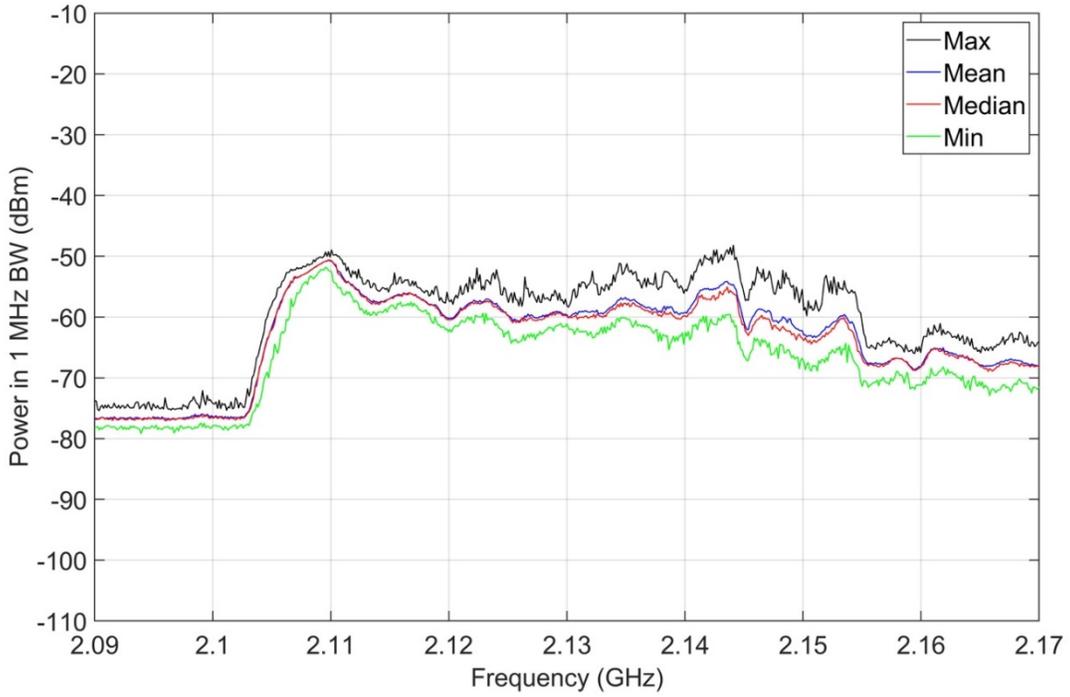


Figure A-15. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-1.

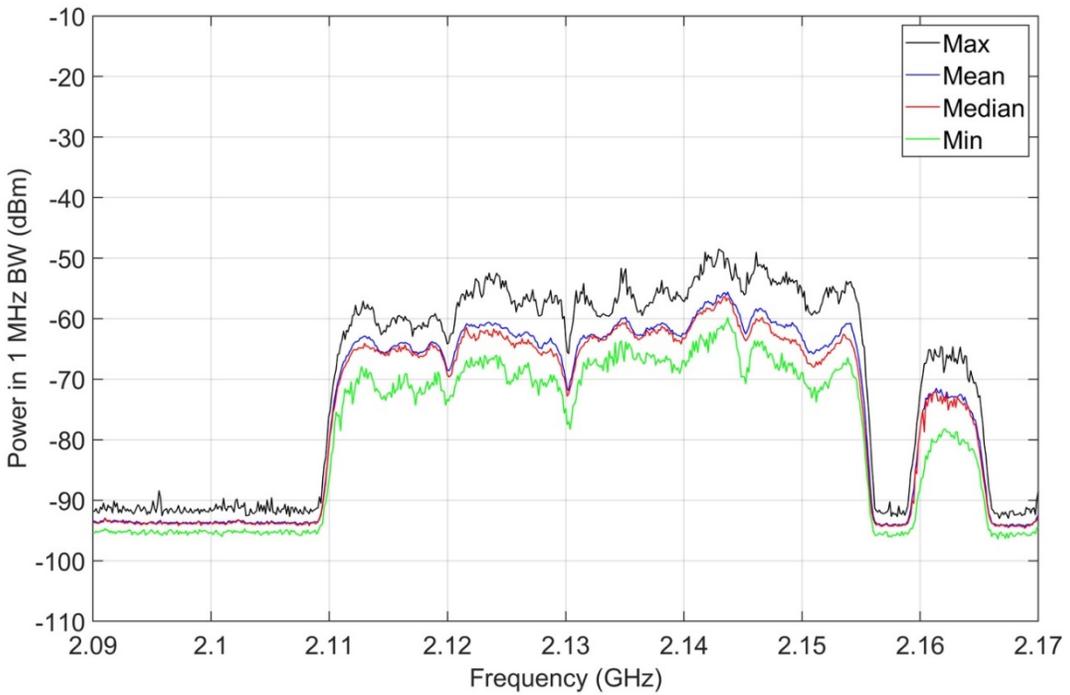


Figure A-16. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.

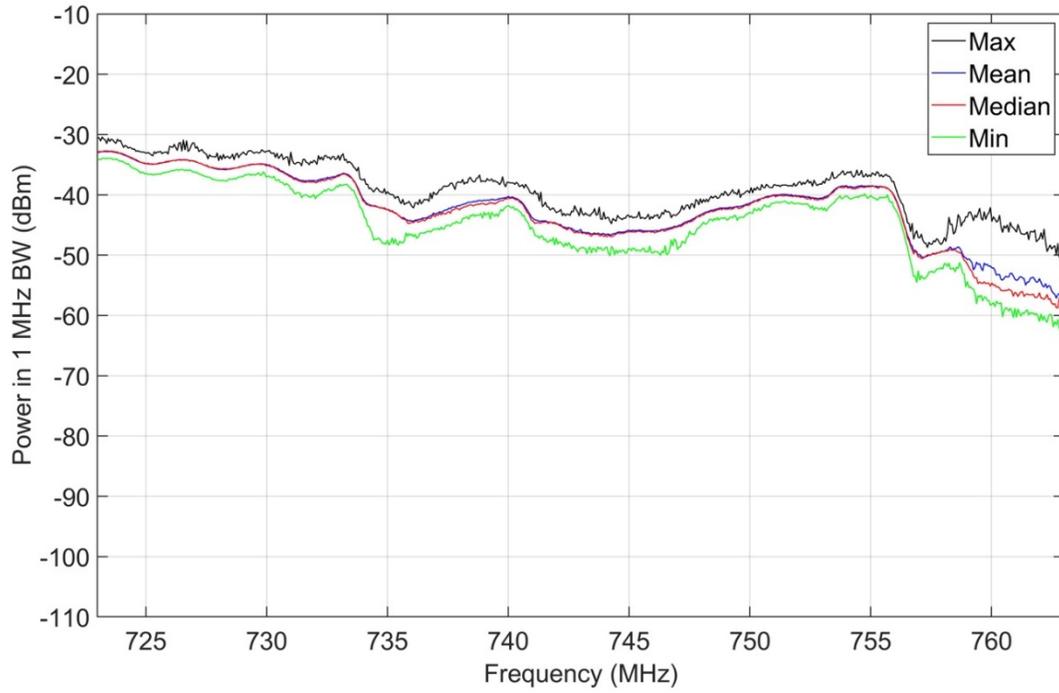


Figure A-17. M4 statistics, jammer on, 723-763 MHz, outdoor location O-2.

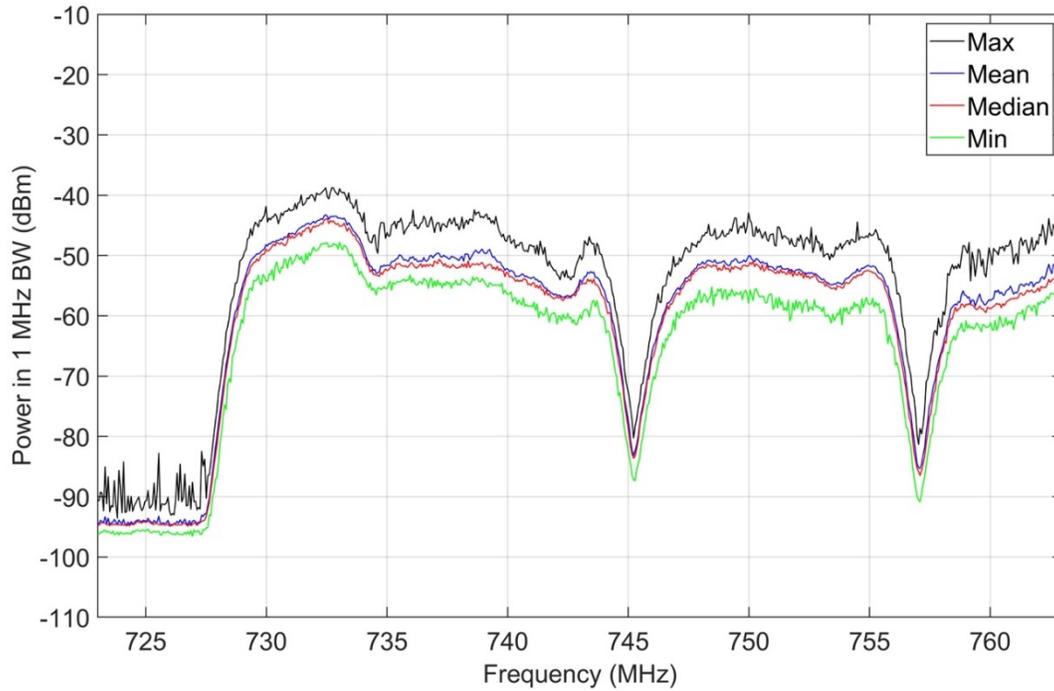


Figure A-18. M4 statistics, jammer off, 723-763 MHz, outdoor location O-1.

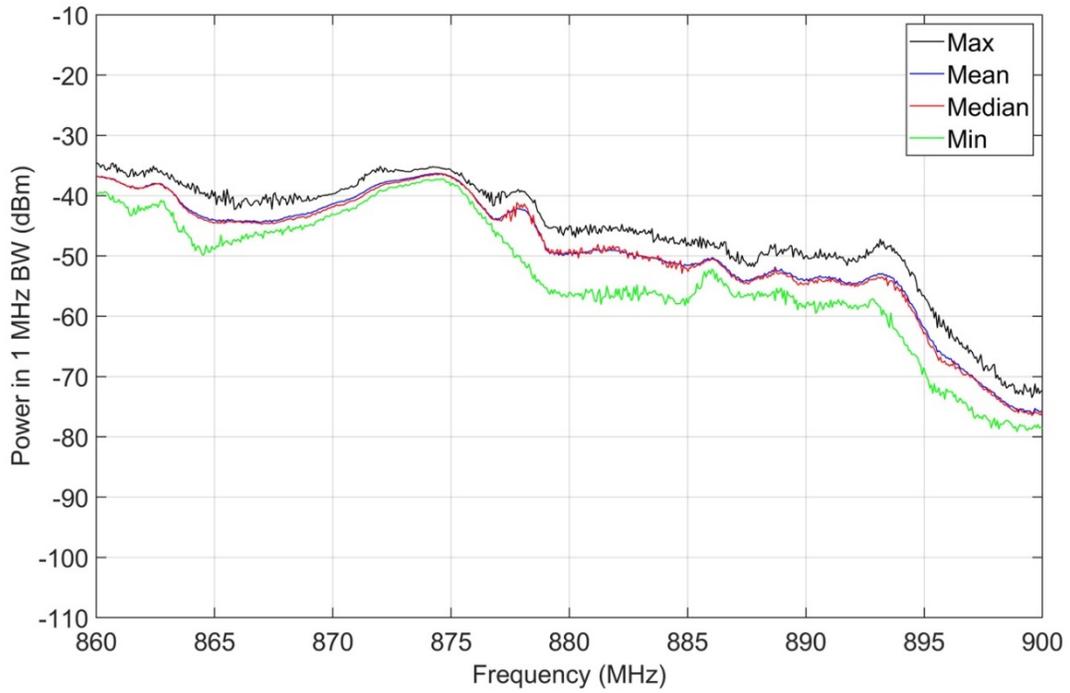


Figure A-19. M4 statistics, jammer on, 860-900 MHz, outdoor location O-2.

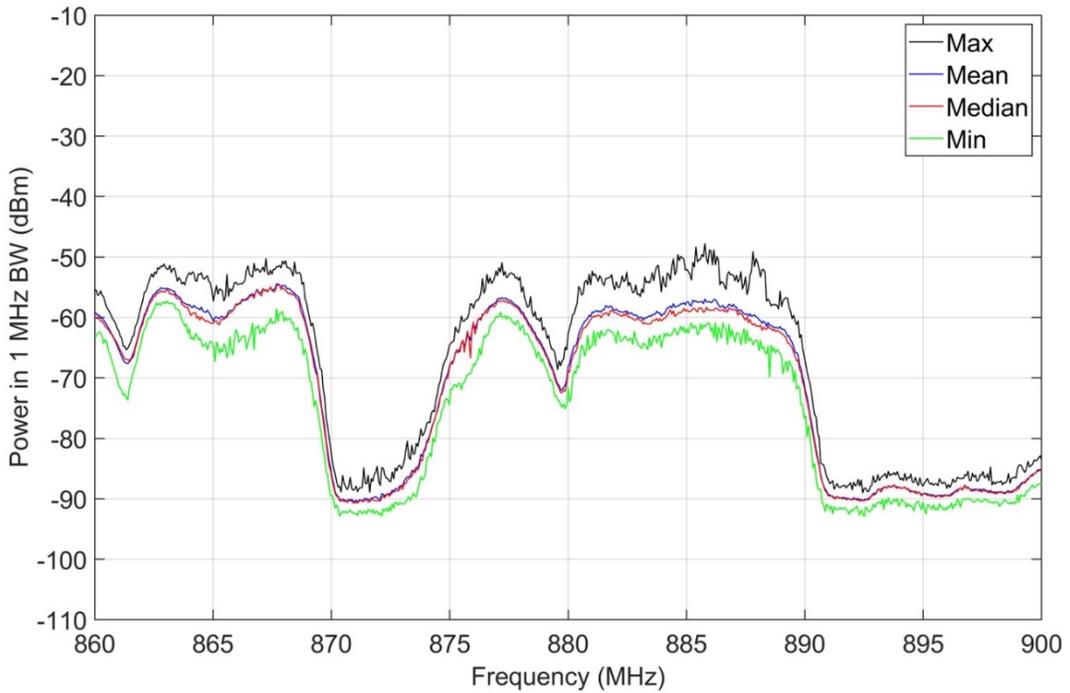


Figure A-20. M4 statistics, jammer off, 860-900 MHz, outdoor location O-1.

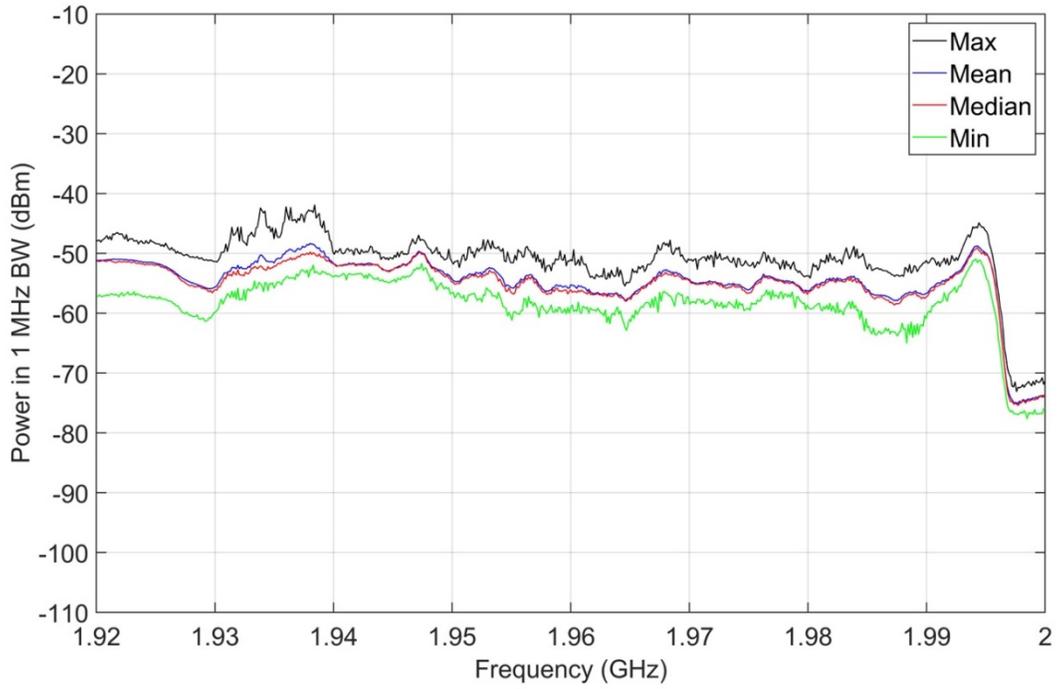


Figure A-21. M4 statistics, jammer on, 1920-2000 MHz, outdoor location O-2.

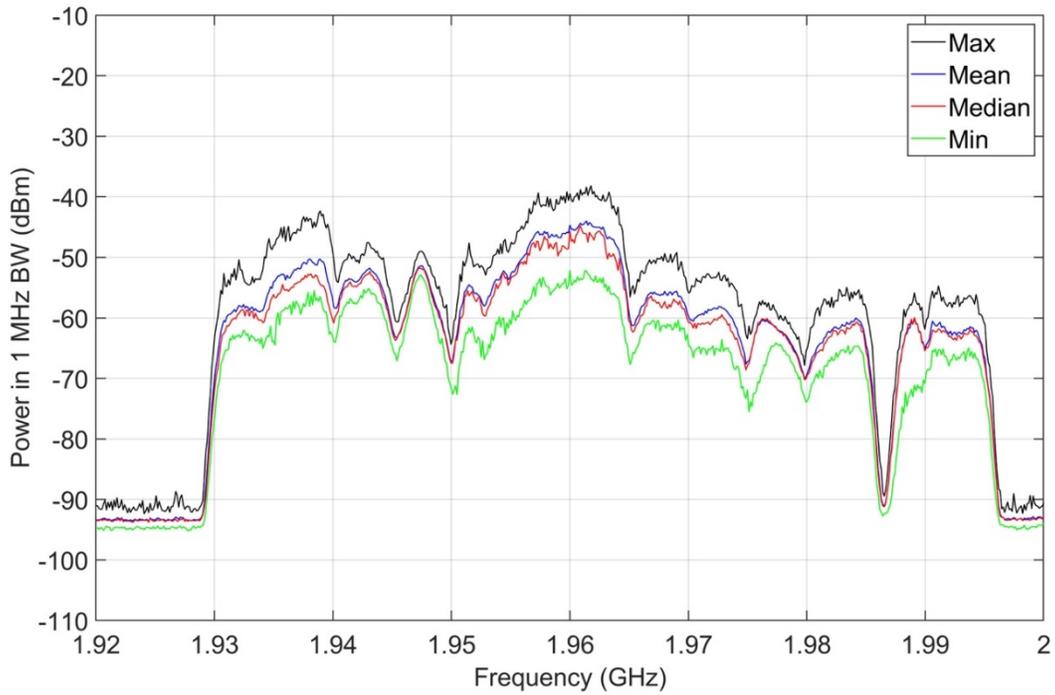


Figure A-22. M4 statistics, jammer off, 1920-2000 MHz, outdoor location O-1.

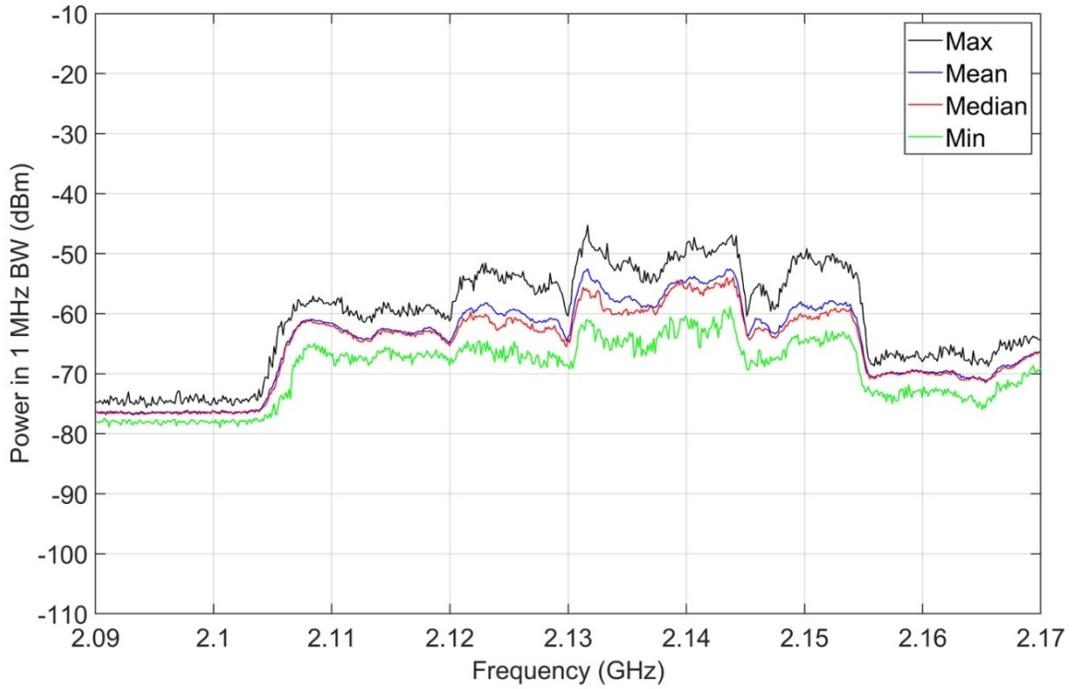


Figure A-23. M4 statistics, jammer on, 2090-2170 MHz, outdoor location O-2.

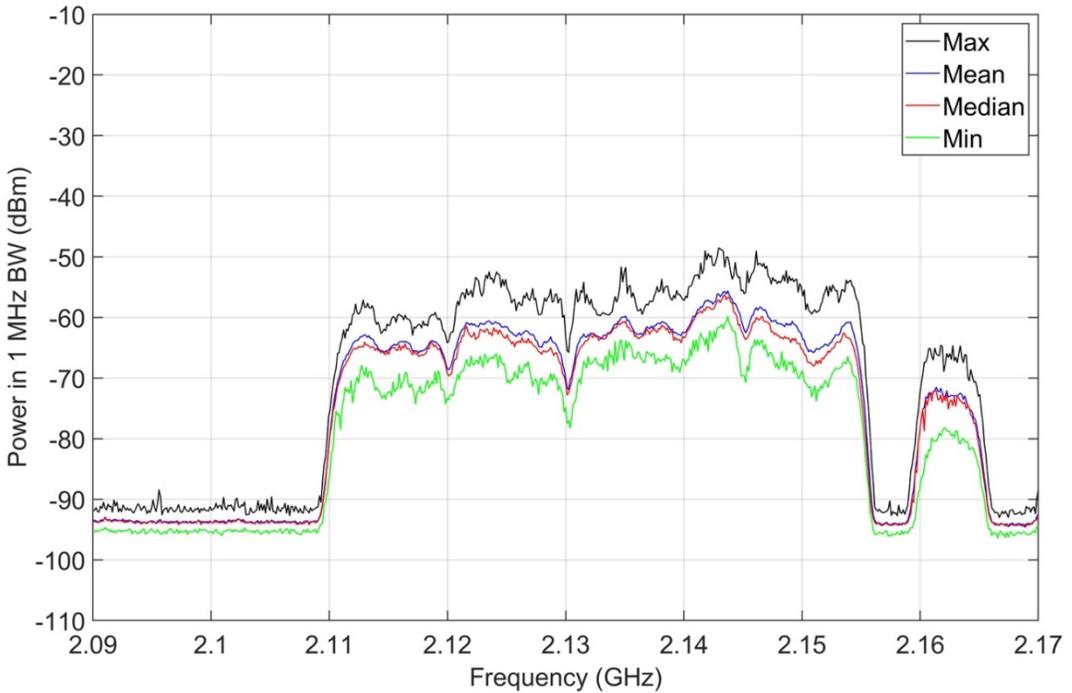


Figure A-24. M4 statistics, jammer off, 2090-2170 MHz, outdoor location O-1.

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION NO. TR-19-541	2. Government Accession No.	3. Recipient's Accession No.
4. TITLE AND SUBTITLE Emission Measurements of a Contraband Wireless Device Jammer at a State Prison		5. Publication Date September 2019
		6. Performing Organization Code NTIA/ITS.M
7. AUTHOR(S) Frank H. Sanders, Geoffrey A. Sanders, John E. Carroll		9. Project/Task/Work Unit No. 6867000-300 3171011-306
		10. Contract/Grant Number.
8. PERFORMING ORGANIZATION NAME AND ADDRESS Institute for Telecommunication Sciences National Telecommunications & Information Administration U.S. Department of Commerce 325 Broadway Boulder, CO 80305		11. Sponsoring Organization Name and Address Office of Security Technology Federal Bureau of Prisons U.S. Dept. of Justice 320 First St., NW Washington, DC
		12. Type of Report and Period Covered Technical Report, FY-19
14. SUPPLEMENTARY NOTES		
15. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.) This report describes emission spectrum measurements of a wireless jammer device operated temporarily inside a South Carolina state prison maximum security housing block. The measurements were intended to demonstrate the operation of the jammer in four commercial mobile radio service (CMRS) bands between 730 MHz to 2.155 GHz. Spectrum measurements of the jammer emissions were performed indoors and outdoors with two measurement bandwidths. Measurements at each location were performed with the jammer on versus off, so as to show the relative power levels of the jamming and ambient CMRS signals at each location. This report's data can be applied in future electromagnetic compatibility (EMC) analyses. However, the data provide no information as to whether a CMRS wireless device can or cannot perform its intended communications function in the presence of a competing signal of specified strength. Only thorough theoretical analysis, well-engineered simulation and modeling, plus selected measurements in controlled (laboratory) environments can objectively quantify the impact of interfering transmissions on CMRS wireless devices.		
16. Key Words (Alphabetical order, separated by semicolons) cellular jamming; commercial mobile radio service (CMRS) jamming; denial-of-service jamming; electromagnetic compatibility (EMC); harmful interference; communications jamming; micro-jammer; radio jamming; wireless device jamming		
17. AVAILABILITY STATEMENT <input checked="" type="checkbox"/> UNLIMITED. <input type="checkbox"/> FOR OFFICIAL DISTRIBUTION.	18. Security Class. (This report) Unclassified	20. Number of pages 65
	19. Security Class. (This page) Unclassified	21. Price:

NTIA FORMAL PUBLICATION SERIES

NTIA MONOGRAPH (MG)

A scholarly, professionally oriented publication dealing with state-of-the-art research or an authoritative treatment of a broad area. Expected to have long-lasting value.

NTIA SPECIAL PUBLICATION (SP)

Conference proceedings, bibliographies, selected speeches, course and instructional materials, directories, and major studies mandated by Congress.

NTIA REPORT (TR)

Important contributions to existing knowledge of less breadth than a monograph, such as results of completed projects and major activities.

JOINT NTIA/OTHER-AGENCY REPORT (JR)

This report receives both local NTIA and other agency review. Both agencies' logos and report series numbering appear on the cover.

NTIA SOFTWARE & DATA PRODUCTS (SD)

Software such as programs, test data, and sound/video files. This series can be used to transfer technology to U.S. industry.

NTIA HANDBOOK (HB)

Information pertaining to technical procedures, reference and data guides, and formal user's manuals that are expected to be pertinent for a long time.

NTIA TECHNICAL MEMORANDUM (TM)

Technical information typically of less breadth than an NTIA Report. The series includes data, preliminary project results, and information for a specific, limited audience.

For information about NTIA publications, contact the NTIA/ITS Technical Publications Office at 325 Broadway, Boulder, CO, 80305 Tel. (303) 497-3572 or e-mail ITSinfo@ntia.gov.