NTIA Report TR-18-533

# Emission Measurements of a Contraband Wireless Device Jammer at a Federal Prison

**Frank H. Sanders**
**Robert T. Johnk**
**Edward F. Drocella**


*report series*

U.S. DEPARTMENT OF COMMERCE · National Telecommunications and Information Administration

NTIA Report TR-18-533

# Emission Measurements of a Contraband Wireless Device Jammer at a Federal Prison

**Frank H. Sanders**
**Robert T. Johnk**
**Edward F. Drocella**


## U.S. DEPARTMENT OF COMMERCE

David J. Redl
Assistant Secretary for Communications and Information

June 2018

## 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.

## CONTENTS

## FIGURES

## TABLES

## ABBREVIATIONS/ACRONYMS

| | |
|---|---|
| $Atten_{circuit}$ | attenuator value in a circuit |
| $Atten_{wall}$ | attenuation value for a wall |
| $B_c$ | chirped-transmitter jammer bandwidth |
| $B_{emission}$ | bandwidth in which nearly all jammer emission power is contained |
| $B_{meas}$ | 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 |
| **ERP** | effective radiated power |
| **EMC** | electromagnetic compatibility |
| $f$ | frequency |
| **FCI** | Federal Correctional Institution |
| **FM** | frequency modulation or modulated |
| $FS$ | field strength |
| $G_{meas\_ant}$ | Gain of a measurement antenna |
| $G_{tx\_ant}$ | jammer device antenna gain |
| **GPIB** | General Purpose Interface Bus |
| **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) |
| **ms** | millisecond |
| **µsec** | microsecond |
| **ns** | nanosecond |
| **NTIA** | National Telecommunications and Information Administration |
| **OoB** | out of band |
| **OSM** | Office of Spectrum Management, NTIA |
| $P_{load}$ | power in a load (measurement circuit) |
| $P_{rad}$ | power effectively radiated by a jammer device |
| $P_{tx}$ | power produced by a jammer device and delivered to its antenna |
| **PC** | personal computer |
| **preamp** | preamplifier |

| | |
|---|---|
| **radhaz** | radiation hazard |
| **RB** | resource block |
| **RF** | radiofrequency |
| **RMS** | root mean square (average) radio power detection |
| **RSMS** | Radio Spectrum Measurement System |
| **RSMS-4G** | Radio Spectrum Measurement System Fourth Generation |
| **STA** | Special Temporary Authorization |
| $\tau$ | chirp interval of a jammer device |
| **W** | watts |

## EXECUTIVE SUMMARY

This report describes National Telecommunications and Information Administration (NTIA) emission spectrum measurements of a contraband wireless device jammer device. The relatively low-power, micro-jamming prototype device was used to demonstrate whether it could effectively disrupt wireless service in four radio spectrum bands utilized by Commercial Mobile Radio Services (CMRS). This demonstration occurred at the Department of Justice (DOJ) Bureau of Prisons (BOP) medium-security Federal Correctional Institution (FCI) at Cumberland, Maryland. NTIA assisted BOP and the manufacturer with site selection within the facility, but did not participate in the jammer installation or operation.

The jammer device was operated by the manufacturer, under BOP supervision, in four CMRS bands between 730 MHz and 2.155 GHz; NTIA measurements of the jammer emissions ranged from 723 MHz to 4.34 GHz. The jammer emissions were transmitted by a single device located in a closed compartment (a utility closet). The targeted jamming zone was an adjacent prison cell. The jammer's emissions were measured at two locations inside the targeted prison cell and at two locations outdoors, beyond the exterior wall of the targeted prison cell. 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 clearly show the jammer emission levels *versus* the ambient CMRS signal levels at each measurement location.

At the measurement locations inside the prison cell, measured differences in incident power between when the jammer was on *versus* off showed that jammer incident power levels were much greater than that of the ambient CMRS power levels. For the outdoor locations where jamming was not intended, the jammer's incident power was measurable even at 30.5 m (100 ft) from the building. However, outdoors the incident jammer power levels were lower than the ambient CMRS levels. This was because the jammer signal strength was lower outdoors than indoors, while the ambient CMRS signals were stronger outdoors than indoors.

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 Cumberland FCI or other facilities.

Analysis of the jammer's potential for harmful interference to licensed radio services, if any, outside the targeted prison cell is beyond the scope of this report. This limitation is due to (1) lack of accepted technical criteria for jammer effectiveness against CMRS receivers and (2) lack of knowledge of harmful interference thresholds for CMRS receivers. The data in this report could be compared to such criteria, if (or when) those criteria are ever developed. Noting this gap in knowledge, we recommend that quantitative engineering criteria for jammer effectiveness against contraband wireless devices and for harmful interference to non-targeted CMRS receivers need to be developed if jamming technology is to be further developed for application in prison environments.

Possible future aggregations of multiple jammer units as would be required to cover entire prison facilities would produce higher total levels of aggregate power than were measured for the one

jammer device at Cumberland FCI. Analysis of aggregate jammer emissions at prison facilities is beyond the scope of this report, as aggregate analysis would require detailed knowledge of specific facilities' physical characteristics, the exact placement of individual jamming transmitters within such facilities, and the exact electronic characteristics of the jamming transmitters.

## ACKNOWLEDGMENTS

The authors thank the Department of Justice, Bureau of Prisons (BOP), and especially Mr. Todd Craig, for providing access to, and coordinating the use of, the BOP Federal Correctional Institution (FCI) at Cumberland, Maryland, where the measurements described in this report were performed. Other BOP personnel were instrumental in making these measurements a success; without their support the work could not have been completed. These include particularly Cumberland FCI Warden, Timothy Stewart, and his staff, and two non-Cumberland BOP staffers, Brent Jensen and Keith McDaniel. The authors also thank NTIA engineers of the Institute for Telecommunication Sciences (ITS) Measurements Division, Geoffrey Sanders and John Carroll, for valuable support and assistance in preparing the measurement system in Boulder prior to the Cumberland FCI measurements. ITS Measurement Division Electronics Technician Ron Carey identified, collected, prepared, and packed the measurement gear that was used at the Cumberland FCI. Last but not least, Geoffrey Sanders is recognized and thanked for having rendered the FCI Cumberland MATLAB®-format raw measurement data files into report-ready graphics. Mr. Sanders was also instrumental in setting up the experimental gear for the laboratory experiment described in Appendix B.

# EMISSION MEASUREMENTS OF A CONTRABAND WIRELESS DEVICE JAMMERAT A FEDERAL PRISON

Frank H. Sanders,[1] Robert T. Johnk[1] and Edward F. Drocella[2]

This report describes emission spectrum and time domain measurements of a contraband wireless device micro-jammer that was operated temporarily in four Commercial Mobile Radio Service (CMRS) bands at a Federal Correctional Institution (FCI) at Cumberland, Maryland. The four jammed CMRS bands were between 730 MHz and 2.155 GHz. The micro-jammer targeted CMRS service indoors, in a single medium-security prison cell. Spectrum measurements of the jammer emissions were performed at two places inside the targeted prison cell and at two non-targeted nearby locations outdoors. Jammer emission measurements were performed at each location with multiple measurement bandwidths and detectors across a frequency range of 300 MHz to 4.34 GHz. Measurements at each location were performed twice, with the jammer device on *versus* off, so as to show the relative power levels of the jamming signal *versus* the ambient CMRS signals at each location. Aggregate emissions from multiple micro-jammer devices such as would be required to cover an entire prison facility were not measured. Jammer emissions are presented in units of power per unit bandwidth in measurement system circuitry; a table for conversion of those data to units of incident field strength in space is provided.

Key words: aggregate emissions; cellular communications jamming; commercial mobile radio service (CMRS) jamming; denial-of-service jamming; electromagnetic compatibility (EMC); emission bandwidth; harmful interference; in-band emissions; communications jamming; micro-jammer; radiation hazard (radhaz); 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 and an NTIA Office of Spectrum Management (OSM) engineer performed on radiated emissions produced by a prototype micro-jammer device[3] at a medium-security

[1] The first two authors are with the Institute for Telecommunication Sciences (ITS), National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, Boulder, Colorado.
[2] The third author is with the Office of Spectrum Management, NTIA, U.S. Department of Commerce, Washington, District of Columbia.
[3] "Micro-jammer" is a generic term used to describe the type of relatively low-powered jammer device that is the subject of this report. See, e.g., Department of Justice News Release, "Bureau of Prisons Tests Micro-Jamming Technology in Federal Prison to Prevent Contraband Cell Phones" (Jan. 17, 2018), available at https://www.justice.gov/opa/pr/bureau-prisons-tests-micro-jamming-technology-federal-prison-prevent-contraband-

Federal Correctional Institution (FCI) operated by the Federal Bureau of Prisons (BOP) at Cumberland, Maryland. This same facility was used to assess emissions from another jammer in 2010, as described in [1].

The micro-jammer transmitter radiated intentional 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 micro-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 and time domain measurements on micro-jammer signals inside and outside a targeted jamming zone at an actual correctional facility. The micro-jammer prototype device was designed by the manufacurer to operate at a relatively low power level so as to effectively disrupt communications from and to contraband wireless devices in a small (prison cell-sized) area indoors while not affecting other CMRS operations outdoors, outside the zone of intentional jamming.

Specific sub-objectives included:

1) Determination of the radiated power levels that the micro-jammer device produced inside and outside the zone of intentional jamming. The measurement locations were to be:

   a) inside a medium-security prison cell at a place relatively far from its window;
   b) inside the same cell at a second location closer to its window;
   c) a location 6.1 m (20 ft) outside the building and adjacent to the prison cell; and
   d) a location 30.5 m (100 ft) outside the building and adjacent to the prison cell.

2) Determination of the power levels of the ambient CMRS signals in the four identified jamming bands, at the same places where the jamming signals were measured.

3) Comparison of the micro-jammer field strength levels to the ambient CMRS signal levels at each measurement location.

---

cell-phones. In [2], we reported on emission measurements performed in a laboratory anechoic chamber on a jammer that operated at a power level of up to 100 watts in each of its operational bands.

4) Measurement of spectrum activity across frequency ranges of 300 MHz to 2.55 GHz and 3.84 to 4.34 GHz to verify that no measurable jammer emissions were observed in these other frequency ranges.

### 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 micro-jammer's effectiveness against contraband wireless devices within the targeted jamming zone

  and

- Technical assessment of the micro-jammer's potential for harmful interference to licensed radio service receivers outside the targeted jamming zone

Unfortunately, such assessments are rendered difficult or impossible 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., "after 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*: some sort of mathematical expression is needed in terms of *S/J* or something similar. Studies to determine such ratios can be performed, and indeed have been performed, for example, for LTE-type receiver performance in the presence of pulsed signals from radars (as described in, e.g., [3] and [4]). We are not aware of similar open-literature studies for the effects of intentional jamming against CMRS receivers with anything like the jammer modulation that is described in [1] and [2] and in this report. Jamming-effects engineering studies need to be performed against CMRS-type receivers if definitive criteria are to be developed for the effectiveness of jamming signals. Such criteria would allow engineers to assess the levels at which jamming power would be effective without being excessive.

A 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 interference, *I*, power levels than effective jamming, *J*, power levels.

Again, studies of harmful radio interference-effects thresholds on radio receivers can be performed and in fact have been performed by, e.g., one of the authors for radar receivers in the presence of interference from communication signals ([5] and [6]). 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., ability to place phone calls from some location *X* when a jammer was running nearby) are anecdotal. They lack the scientific strength of 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 cellular phone calls could be successfully connected.

In summary, it would be a desirable objective to compare the data collected in this study 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. But since such accepted technical criteria do not currently exist, we cannot perform these assessments.

We recommend that engineering studies combining theoretical modeling and analysis with controlled laboratory observations should be performed for the development of such criteria. Lacking such criteria at this time, we can only report the relative power levels of jammer signal strength and ambient CMRS signals, and point out that such comparative levels may eventually be subject to such assessments when appropriate technical criteria become available.

### 1.3 Approach

The study approach was as follows:

1) On behalf of the BOP, Department of Justice (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 actual prison facility.[4]

2) The device manufacturers, with BOP's cooperation and supervision, temporarily installed the device inside a utility closet in a medium-security Cumberland FCI building. NTIA engineers participated in the measurement-site selection process and assisted in coordination of the use of the site between the BOP and the manufacturer, but did not participate in or direct any aspect of the jammer installation or configuration. In addition to the jammer device, the manufacturer temporarily installed a commercially available reflective window coating on the outside of the prison cell window. The coating was intended to reduce the amount of jammer power that radiated outside the prison housing unit structure.

[4] 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. 2015 revision of the May 2013 Edition). As a condition of the STA, DOJ coordinated in advance with commercial wireless carriers in the Cumberland area.

3) NTIA engineers collected jammer emission measurements at two locations inside the targeted jamming zone (a medium security prison cell directly adjacent to the utility closet where the jammer was located) and at two outdoor locations outside the targeted prison cell. The outdoor locations had line-of-sight (LOS) propagation to the building. The distances were 6.1 m (20 ft) and 30.5 m (100 ft) from the outside building wall.

4) NTIA engineers used an ITS-designed portable, battery-powered measurement system to measure the in-band, adjacent band, out of band (OoB), spurious and harmonic emission levels of the jammer at frequencies as high as the second harmonic of the highest-frequency jammer band. 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.

5) NTIA engineers reduced the raw measurement data to graphical plots, which are provided in this report (Section 4: Measurement Results and Appendix A) and conducted pertinent data analysis. The plots show received power in the 50 ohm circuitry at the measurement antenna terminals in units of decibels relative to a milliwatt (dBm) per unit bandwidth in a specified detector mode (e.g., root mean square (RMS) average-detected power in dBm in 100 kHz bandwidth in 50 ohms). Section 5 (Data Analysis) of this report provides for conversion of these power levels to units of incident field strength in space per unit bandwidth (e.g., RMS power in dBμV/m in 100 kHz bandwidth in free space). The relative levels of the jammer signals and the ambient CMRS signals are observed by comparing the jammer-on *versus* jammer-off data graphs.

## 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 the modulation parameters in detail. The jammer repetitively tuned a carrier wave across each targeted band. Such swept frequency-modulated (FM) tuning is commonly called "chirping." In each of the four jamming bands, the chirped signal was repetitively ramped up and then down in frequency. A full chirp cycle included both an up-ramp and a down-ramp in frequency. The frequency-tuning behavior would look like a sawtooth pattern if the tuned frequency were plotted as a function of time in each band, as shown schematically in Figure 1.

Table 1. Micro-jammer transmitter technical characteristics.[5]

| Jammer Technical Characteristic | Parameter Value |
|---|---|
| Operational Band 1 | 729–757 MHz |
| Operational Band 2 | 869–894 MHz |
| Operational Band 3 | 1930–1990 MHz |
| Operational Band 4 | 2110–2155 MHz |
| Transmitter Power | 0.9 watt per band6 |
| Antenna Gain | +3 dBi |
| Antenna Polarization | Vertical and Horizontal |
| Modulation | Swept frequency (chirped) carrier wave |
| Emission Line Spacing | 70.4 and 140 kHz (see Table 2) |

Table 2. Micro-jammer transmitter frequency modulation (chirping) details.

| Low Freq. (MHz) | High Freq. (MHz) | Sweep Rate (kHz) | Half Cycle Interval (μs) | Full Cycle Interval (μs) | Peak Detected Emission Bandwidth[7] (MHz) | Average Detected Emission Bandwidth7 (MHz) |
|---|---|---|---|---|---|---|
| 729 | 757 | 70.4 | 7.1 | 14.2 | ≈ 1.40 | > 28 |
| 869 | 894 | 140.1 | 3.57 | 7.14 | ≈ 1.87 | > 25 |
| 1930 | 1990 | 70.4 | 7.1 | 14.2 | ≈ 2.06 | > 60 |
| 2110 | 2155 | 140.1 | 3.57 | 7.14 | ≈ 2.51 | > 45 |

[5] The jammer device was, physically, a set of four independent prototype transmitters that were all built into one box. Each of the individual transmitters in that box operated individually in one of the respective frequency bands shown in Table 1. For simplicity we refer in this report to the "jammer device" as a singular entity.

[6] The manufacturer asserts that this value is effectively less than the 0.9 W value listed in the STA. This topic is discussed in Section 2.4.

[7] See Appendix B for further description and discussion of peak-detected and average-detected emission bandwidths.

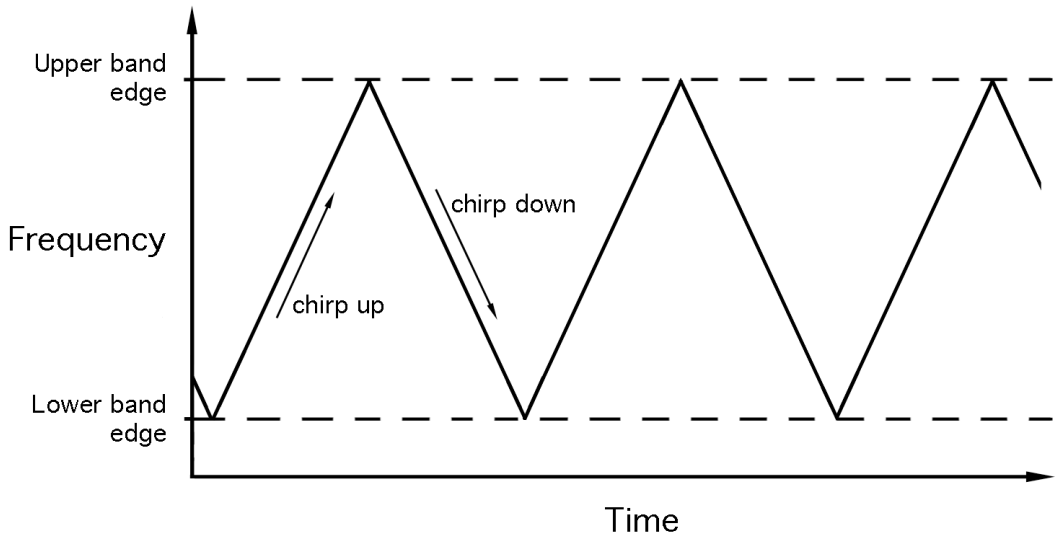


Figure 1. Jammer frequency modulation (chirping) behavior in time. Each ramp is a half-cycle. A full cycle is any *pair* of one-way ramps.

### 2.2 Jammer Emission Bandwidth

The jammer's sawtooth FM (chirped) emission (Figure 1) produces two emission bandwidths. If the jammer power is measured with an averaging detector, then the full power is contained in a bandwidth slightly wider (by about ten or eleven per cent) than the chirp bandwidth, $B_c$. If the power is measured with a positive-peak detector, then the emission bandwidth is approximately (from [7]):

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

where:

$B_{emission}$ = bandwidth in which most peak-detected jammer emission power will be contained (MHz);

$B_c$ = chirp bandwidth (MHz);

$\tau$ = full-cycle (any pair of frequency ramps) chirp interval (μs).

Based on these relationships, the computed peak and average $B_{emission}$ values for the jammer are shown, on a band-by-band basis, in the last two columns of Table 2. The jammer's emission bandwidth for a given type of detection is important to know because, for any measurement or receiver bandwidths that are narrower than these values for each detection mode, the measured power will *not* be the transmitter's full power. This topic is discussed in detail in Appendix B of this report.

For the Cumberland FCI measurements, all measurement bandwidths, $B_{meas}$, were less than the $B_{emission}$ values of Table 2. Therefore the power measured at Cumberland was always less than

the jammer's total power and always varied with $B_{meas}$. The wider the value of $B_{meas}$, the higher the measured power. As noted in Section 3 of this report and as discussed further in Appendix B, measurements performed in multiple bandwidths less than $B_{meas}$ at Cumberland allowed us to observe the *rate* at which power in any receiver varies 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. A further experiment on this topic was performed at the ITS Boulder laboratory and is described in Appendix B.

### 2.3 Targeted Jamming Space

Figure 2 shows, schematically, the jammer installation, the adjacently located targeted prison cell space, and the four locations of the measurement system antenna. The targeted prison cell was one of many in a large housing unit. The housing unit construction was of poured concrete with (we assume) internal steel reinforcement. Concrete thicknesses, composition, and reinforcement details are unspecified. The targeted prison cell was on the housing unit's ground floor.

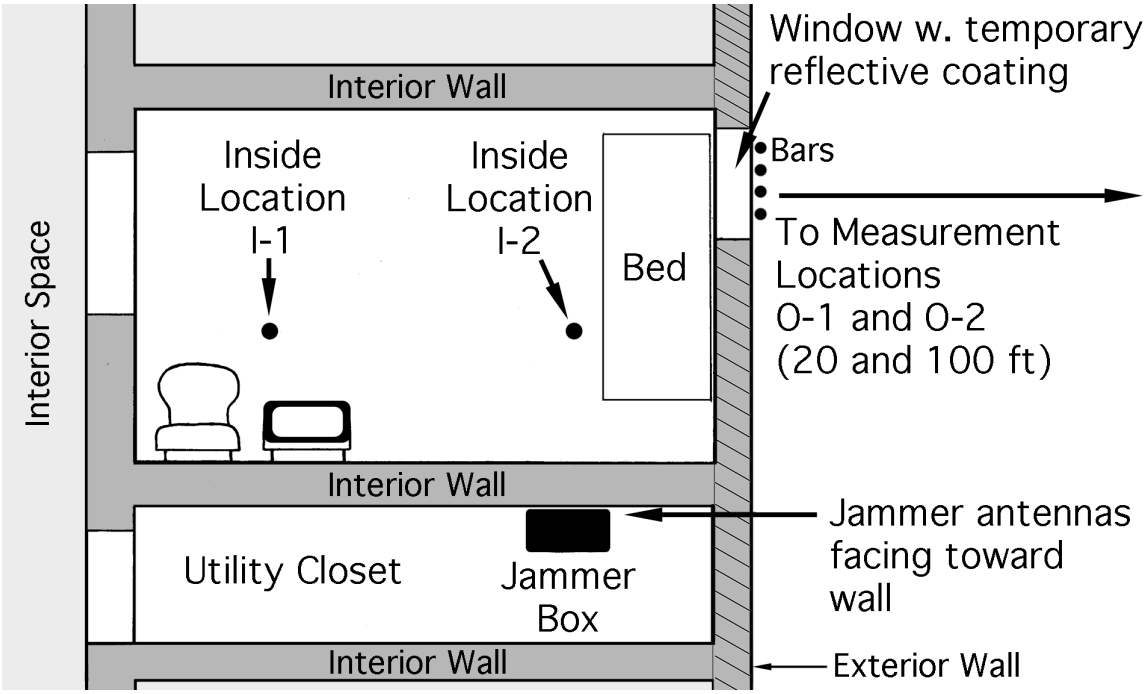


Figure 2. The Cumberland FCI jammer installation, targeted adjacent medium-security prison cell, and measurement antenna locations. Wall, door, and window thicknesses, positions and dimensions are only approximate.

The approximate prison cell interior dimensions were 4 m (13 ft) long by 2.4 m (8 ft) wide by about 3 m (10 ft) high. Fixed interior infrastructure included a toilet, sink, and a pair of bunk beds. The door was made of steel. The space had a single exterior window with dimensions on the order of a few feet wide and high. Vertically oriented bars (presumably steel) spaced on the order of a few inches apart were on the exterior side. Electrically, the targeted space could be considered to be an empty six-sided steel-and-concrete rectangular box of these dimensions, with a single medium-sized, steel-barred exterior aperture (the window with its bars) in one of the narrower-side walls.

A temporary modification was made to the targeted jamming space by the device manufacturer's personnel. They applied a semi-transparent reflective coating to the exterior of the window for the duration of the measurements. The coating was applied as a single adhesive sheet. It was a light-reflective material that is intended to reduce the amount of sunlight passing through a window. Its electrical characteristics and brand name are unknown to us; the jammer manufacturer stated that they procured it at a retail hardware outlet. It was installed to reduce the amount of jammer power that radiated out of the housing unit building. We do not know its effectiveness in this respect.

### 2.4 Jammer Installation and Effective Radiated Power (ERP)

The micro-jammer's enclosure was made of what appeared to be gray-enameled metal; it weighed a few pounds and was about the size of a pair of side-by-side shoeboxes. It was installed flush to the wall of a utility closet next to the targeted space, as shown in Figure 2. The jammer was mounted about 1.5 m (5 ft) above the floor. Its only exteriorly visible feature was a three-wire power cord that was plugged into a grounded power outlet inside the closet.

According to the manufacturer, the micro-jammer's antennas (which were inside the jammer box and not exteriorly visible) were situated on the side of the box that faced the wall, and thus were themselves nearly flush to the wall (with only the side-wall of the box being between them and the housing unit wall). We understand that there were four such antennas in the jammer box, one for each operational band. We further understand that each antenna was connected to its own transmitter inside the box. As shown in Table 1 (itself derived from the DOJ STA data), each antenna had 3 dB more gain than isotropic (+3 dBi), with both vertical and horizontal components.

The manufacturer stated that the transmitter power level of 0.9 W per band shown in Table 1, which is the STA-specified power value that each transmitter delivered to each respective antenna, should not be taken as the effective power of each transmitter in each band for purposes of operational assessments. The reason, they stated, is that the micro-jammer is intended to always be mounted flush to a prison wall structure, and that the power that is effectively radiated into targeted spaces should be reduced by the amount that any given wall will attenuate the power output of the entire jammer system. They refer to this wall-attenuation aspect of their micro-jammer design as being "shielded." The amount of wall attenuation ("shielding," as described by the manufacturers) is not known for the Cumberland FCI installation. It would in general be difficult to assess and will be expected to vary from one installation to the next, both within and between various correctional institutions.

Physically and mathematically, it does not matter whether a radiated signal is attenuated by a physical, discrete-component attenuator placed within a circuit between a transmitter and its antenna, *versus* whether the signal is attenuated outside the antenna by (in this case) a concrete-and-steel wall. In both cases the attenuation is a physical power-loss factor. The equation for radiated power with an attenuator in the transmitter's circuit is:

$$P_{rad} = P_{tx} - Atten_{circuit} + G_{tx\_ant}.$$

The equation for radiated power with no discrete-component attenuator but with a wall that instead provides attenuation is:

$$P_{rad} = P_{tx} + G_{tx\_ant} - Atten_{wall},$$

where:

$P_{rad}$ = power radiated into the targeted jamming space or zone;

$P_{tx}$ = power produced by the jammer transmitter;

$G_{tx\_ant}$ = gain of the jammer antenna relative to isotropic;

$Atten_{circuit}$ = attenuation in a circuit between the transmitter and the jammer antenna;

$Atten_{wall}$ = attenuation produced by a wall outside (adjacent to) the jammer antenna.

The attenuation terms (always positive in these equations, so that the minus signs make them always *reduce* the overall power, $P_{rad}$) give the same result in either case, if they are equal in the two equations. But for the Cumberland FCI jammer or any other such installation, the configuration of the second equation reflects physical reality. In that equation, the value of $P_{tx}$ should be set to 0.9 W (+29.5 dBm) as specified by the STA, with $G_{tx\_ant}$ = +3 dBi per the corresponding STA datum.

The $Atten_{wall}$ term will have an unspecified value that will, as already noted, vary from one wall to another; $P_{rad}$ will itself vary with $Atten_{wall}$. Further, $Atten_{wall}$ will be expected to vary with frequency. This variation will depend on wall structure and composition. Therefore $P_{rad}$ will likewise be expected to vary across the spectrum, from one jamming frequency band to the next, with each individual wall installation. For any given wall installation, only the inequality

$$P_{rad} < (P_{tx} + G_{tx\_ant})$$

will be known for certain. For the Cumberland FCI installation, where $(P_{tx} + G_{tx\_ant})$ = (+29.5 dBm + 3 dBi) = +32.5 dBm, we know that the effective radiated power (ERP) was:

$$P_{rad\_Cumberland} < (+32.5 \text{ dBm}) \text{ total power per jamming band.}$$

### 2.5 Jammer Operation

The manufacturer's personnel, under the direct supervision and control of BOP staff, operated the jammer. The jammer device had two states, transmitter on and transmitter off. It had no external, operator-accessible controls or settings. The jammer was turned on by plugging it into a power outlet and turned off by pulling the power plug out of its outlet. Power-off was instantaneous with the pulling of the power cord. Power-on was always given a 20 minute interval for complete warm-up and stabilization of the jammer unit after the power cord was plugged into the wall outlet. All jammer-on measurements were always performed only after this 20 minute power-up waiting interval had elapsed.

## 3. MEASUREMENT DESCRIPTION

### 3.1 Measurement System Hardware

The measurement system is shown schematically in Figure 3. A photograph of the system as deployed at Cumberland on a portable equipment cart is shown in Figure 4.

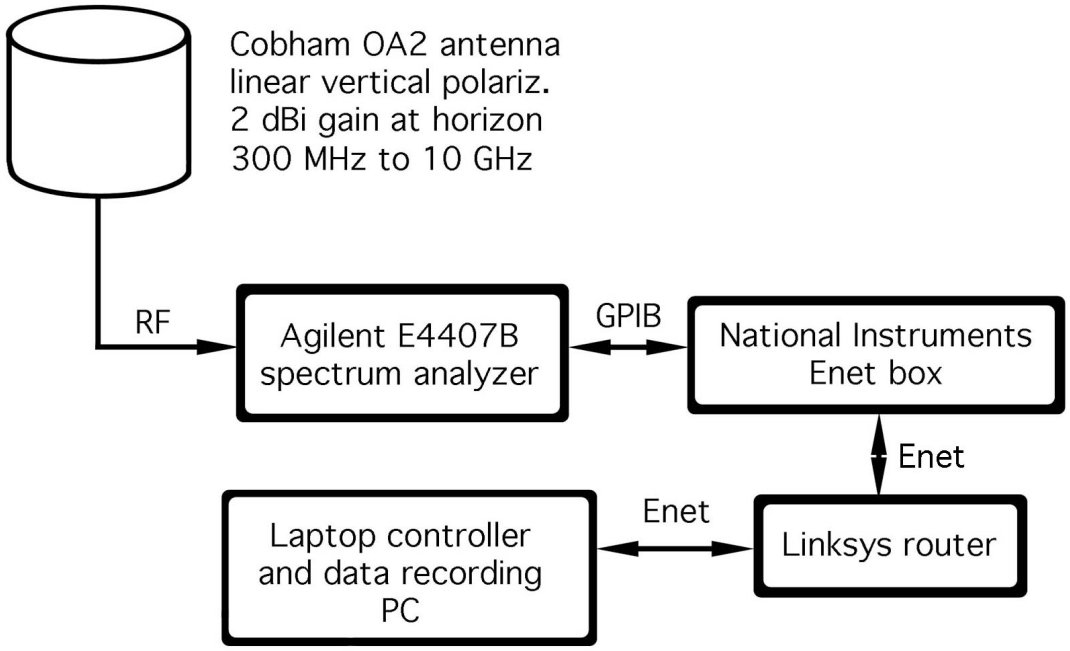


Figure 3. Block diagram schematic of the jammer emission measurement system used at Cumberland FCI.[8]

The measurement system used an omnidirectional, vertically polarized antenna with a calibrated frequency response range of 300 MHz to 10 GHz. Its gain in the direction of the horizon was +2 dBi. The antenna was connected via a short length of low-loss radiofrequency (RF) coaxial line to the input of an Agilent E4407B portable spectrum analyzer. The analyzer was controlled via ITS-written software (called Radio Spectrum Measurement System 4th Generation, or RSMS-4G) installed on a laptop personal computer (PC).

Via intermediary communication boxes shown in 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.[9] The data from all of these measurements were sent from the spectrum analyzer to the same PC, where they were recorded on the PC's hard drive as MATLAB®-format files. Subsequent to the measurement series on January 17, 2018, all of the data were backed up on additional platforms.

[8] The antenna Cobham OA-2 antenna is further identified as V1505, serial number 408158-0002.

[9] For all measurements, the spectrum analyzer data trace was set at 1001 bins per screen sweep.

Data processing and report ready graphic production were subsequently performed by ITS engineers at the ITS laboratory in Boulder, Colorado.

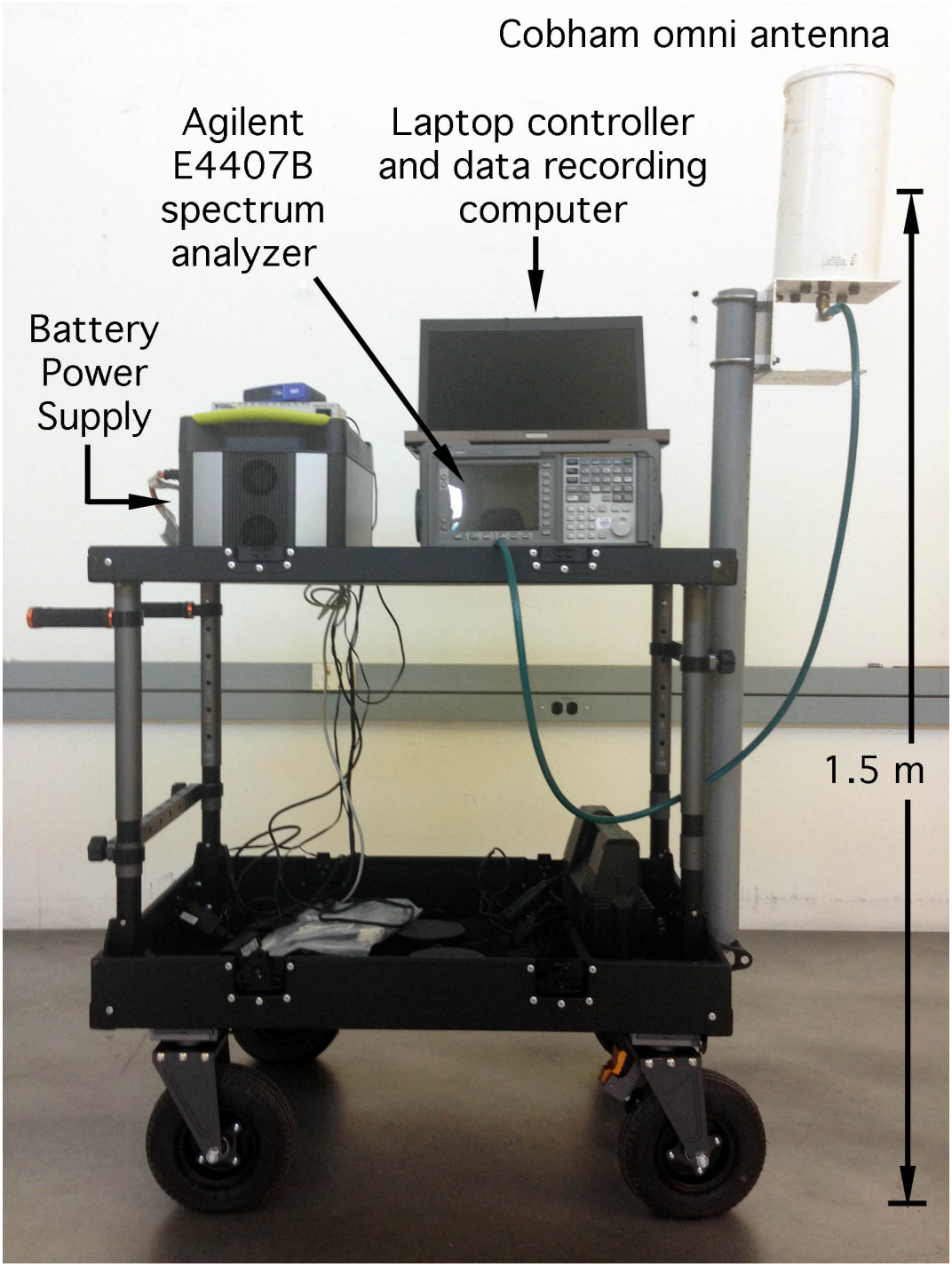


Figure 4. Photograph of the ITS measurement system on a rolling equipment cart as deployed at Cumberland FCI.

### 3.2 Measurement Parameters

The jammer emission measurement parameters are shown in Table 3.

Table 3. Parameters for in-situ prison jammer emission measurements.

| Freq. Range (MHz)[10] | IF Stage (Resolution) Bandwidth (kHz) | Video Band-width (kHz) | Detector | Sweep Time (sec) | Freq Bin Size (kHz) | Dwell per Bin (μs) | Total Jammer Sweeps per Bin |
|---|---|---|---|---|---|---|---|
| 723–763 | 100 | 300 | Peak, 50 sweeps | 0.28 | 40 | 280 | 20 |
| 723–763 | 100 | 300 | RMS Average | 28 | 40 | 2800 | 200 |
| 723–763 | 1000 | 3000 | Peak, 50 sweeps | 0.28 | 40 | 280 | 20 |
| 860–900 | 100 | 300 | Peak, 50 sweeps | 0.14 | 40 | 140 | 20 |
| 860–900 | 100 | 300 | RMS Average | 14 | 40 | 1400 | 200 |
| 860–900 | 1000 | 3000 | Peak, 50 sweeps | 0.14 | 40 | 140 | 20 |
| 1920–2000 | 100 | 300 | Peak, 50 sweeps | 0.28 | 80 | 280 | 20 |
| 1920–2000 | 100 | 300 | RMS Average | 28 | 80 | 2800 | 200 |
| 1920–2000 | 1000 | 3000 | Peak, 50 sweeps | 0.28 | 80 | 280 | 20 |
| 2090–2170 | 100 | 300 | Peak, 50 sweeps | 0.14 | 80 | 140 | 20 |
| 2090–2170 | 100 | 300 | RMS Average | 14 | 80 | 1400 | 200 |
| 2090–2170 | 1000 | 3000 | Peak, 50 sweeps | 0.14 | 80 | 140 | 20 |
| 300–1050 | 1000 | 3000 | Peak, 30 sweeps | 1 | 750 | 1000 | 70 and 140 |
| 1050–1800 | 1000 | 3000 | Peak, 30 sweeps | 1 | 750 | 1000 | 70 and 140 |
| 1800–2550 | 1000 | 3000 | Peak, 30 sweeps | 1 | 750 | 1000 | 70 and 140 |
| 3840–4340 | 1000 | 3000 | Peak, 30 sweeps | 1 | 500 | 1000 | 70 and 140 |

#### 3.2.1 Measurement Frequency Bands

As shown in Table 3, the frequency bands identified for the jammer emission measurements were:

- The four intentionally jammed CMRS bands (723–763 MHz, 860–900 MHz, 1920–2000 MHz, and 2090–2170 MHz), including a small additional margin on the lower side and upper side of each band. The margins were added to show the OoB roll-off of the jammer emissions in adjacent spectrum. Detailed measurements were taken in each of these bands.

- All frequencies from 300 MHz to 2550 MHz. This covered, continuously, frequencies from below the half-harmonic of the lowest-frequency jammer frequency, through all four of the CMRS bands, and well into the spurious emission region for the highest-frequency jammer

[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.

band. It also covered the second harmonics of the first and second CMRS bands. As shown in Table 3, this frequency range was divided into three sub-ranges of 750 megahertz each (300–1050 MHz, 1050–1800 MHz, and 1800–2550 MHz).

- All frequencies from 3840 to 4340 MHz. This covered the second harmonics of the two upper (third and fourth) CMRS bands.

### 3.2.2 Measurement Bandwidths

In the CMRS bands, both peak-detected and RMS-average data were acquired in a 100 kHz measurement (also called resolution, or intermediate frequency (IF)) bandwidth.[11, 12] Additional peak data were acquired in a 1 MHz bandwidth.

This pair of bandwidths was selected for multiple reasons. First, 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 future electromagnetic compatibility (EMC) analysis studies that might involve receivers having any given bandwidth. (See further discussion in Appendix B.)

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* $10 \cdot \log(180/100) = 2.5$ dB more power than in 100 kHz. Power and bandwidth-dependence comparisons or assessments for such paired bandwidth measurements should be performed using the pairs of peak-detected, 50-sweep measurements made in a 100 kHz and 1 MHz bandwidth in each of the CMRS bands, as shown for the measurement events for each band in Table 3.

The power levels of the CMRS signals themselves will also vary with bandwidth. This is the second reason for acquiring data in the two bandwidths of 100 kHz and 1 MHz. The rate of variation of any ambient signal in any CMRS band can be compared between any pair of measurements (again, the pairs being 50 sweeps each with a peak detector in each CMRS band in each of the two measurement bandwidths of 100 kHz and 1 MHz, as described in Table 3).

If the CMRS signal power were found, for example, to be proportional to measurement bandwidth (a 10 dB increase in power in 1 MHz relative to power in 100 kHz), then in the 180 kHz LTE RB the increase from power measured in 100 kHz would again be 2.5 dB, as shown above. In this case, since the jammer power and LTE power would *both* be directly

[11] An ideal bandwidth for comparison to power in the 180 kHz RB bandwidth of LTE receivers would have been 180 kHz. But the E4407B does not have that bandwidth available. The next-smaller bandwidth was 100 kHz.
[12] The spectrum analyzer's baseband, lowpass filter, called a video filter, was always set to be wider than the resolution bandwidth so as to not affect the overall measurement result for any given resolution bandwidth setting.

proportional to receiver bandwidth, the *offset* seen between them in any 100 kHz measurement bandwidth would be *identical* to what would be seen (measured) in the receivers' own RB bandwidth of 180 kHz. No offset adjustment between jammer power and CMRS signal power would be necessary from what was measured in 100 kHz or 1 MHz.

Conversely, if the jammer signal power were to be found to vary by, for example, 1.5 dB between 100 kHz and 180 kHz, whereas the CMRS signal were found to vary by, for example, 2.2 dB between those same two bandwidths, then the offset observed in the 100 kHz measurement data would need to be adjusted upward by (2.2 – 1.5) = 0.7 dB in any 180 kHz LTE RB.

This brings us to a second reason for performing the measurements in a pair of bandwidths. For general EMC studies, it cannot be assumed that any and all communication signal bandwidths will have any particular value. The 180 kHz LTE RB bandwidth, although currently common in many CMRS radios, may not remain constant or common in the future; other existing and future communication systems may use different bandwidths from 180 kHz. If all measurement data were simply acquired in a single bandwidth (say, 180 kHz) there would be no way to know how the signal power would vary for other receiver bandwidths. 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 bandwidths between 100 kHz and 1 MHz, and to some extent to systems with bandwidths that are a bit narrower or wider than those measurement bandwidths.

For measurements in non-CMRS parts of the spectrum (between 300 MHz and 4.34 GHz, as shown in Table 3), no jammer signal was expected to be seen and no in-band CMRS signals were expected. Here, there could be no comparison between jammer power levels and ambient CMRS signal levels.[13] Therefore there was no need to take data in a 100 kHz and 1 MHz bandwidth. Moreover, the spectrum spans that needed to be examined were quite large, on the order of 4 GHz. Therefore a single, fairly wide bandwidth needed to be used in order to complete the non-CMRS band measurements at each location in a timely manner. For these non-CMRS spectrum spans, a measurement bandwidth of 1 MHz was selected because it was large enough to cover the wide-band spectrum spans expeditiously while being narrow enough to still show good spectral detail. Also, 1 MHz is a commonly used reference bandwidth for EMC studies. Thus all of the non-CMRS band measurement bandwidths in Table 3 are 1 MHz.

### 3.2.3 Measurement Detection Modes and Frequency-Span Sweep Times

Two detection modes, peak and RMS average, were used to measure emissions in the CMRS bands. 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 peak-latch circuit (in analog spectrum

[13] Even if jammer signals were to be observed in the non-CMRS spectrum band measurements, that is, there could not, by definition, be any intentional CMRS emissions in those bands.

analyzers) or a software peak-latch function (in digital analyzers such as the E4407B) retains the highest-power value that goes though 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.

This may best be understood via an example. Suppose that a spectrum analyzer has been set to show 1001 bins per trace (as was our E4407B during the jammer measurements) and that the analyzer's sweep time is set to 1 second. Then the time spent per bin per sweep is 1/1000 second = 1 millisecond. (The counting works out to exactly 1 millisecond per bin because the first of the 1001 display bins is counted as the zeroth bin.) The machine's digitizer delivers, for example, 100,000 independent measurement values per second when a 100 kHz resolution bandwidth has been selected. (It is actually a somewhat larger value, but for this example 100,000 digitized data points per second will make the arithmetic easy.) 100,000 digitized points per second divided by 1 millisecond per trace bin yields 100 digitized points delivered to each bin as each sweep progresses. In peak detector mode, however, only *one* of those 100 points delivered from the digitizer during each bin interval will be displayed in each bin. That specially selected (peak-latched) point shown in each bin in each trace will be the *highest-power* digitized point out of the 100 that were delivered. This process of peak-latching is repeated for every bin in every trace. At the end of each swept trace, all bins are zeroed and the process is repeated for the next sweep; peak-detected values are not retained from one sweep to the next.[14]

In RMS average detection mode, the *linear average power* (rendered as a decibel quantity) of the same (hypothetical, from above) 100 points delivered in a 100 kHz bandwidth to each spectrum analyzer bin during each trace sweep is displayed. A digital spectrum analyzer does this by dividing each decibel-power digitized sample by 10, then taking the antilog to get linear power, then adding 100 of those linear power values together, dividing by 100 to get their linear average power, and then rendering the result back into a decibel value for the bin's screen display.[15]

The two detector modes, peak and average, were both used in the measurement series to examine different aspects of the jammer's emission characteristics. Peak detection captures any short-term, transient, impulsive emissions. Peak detection shows the maximum power that ever occurs on any given frequency in any given bandwidth.

Average detection, in contrast, discriminates *against* short-term, impulsive, transient-type emissions. RMS average (when measured properly, with a statistically significant number of input samples such as we have described) shows power levels in a bandwidth that are maintained with some degree of steadiness as time progresses.

---

[14] Note that this example does *not* show how maximum-hold trace mode works. Peak detector mode is *not* maximum-hold trace mode. In maximum-hold trace mode, the highest power level so far seen for each bin *on each trace in a series of traces* is retained from one spectrum analyzer sweep to the next. Maximum-hold trace mode is a screen display mode, *not* a detector mode. It is a display mode that can be implemented with *any* of a spectrum analyzer's detectors, e.g., RMS average detection mode or even negative-peak detection mode.

[15] For analog analyzers, a close approximation to RMS average is obtained by setting the video bandwidth to a much smaller value than the resolution bandwidth.

As noted below, only RMS average should be used for assessment of emissions for purposes of comparison to radhaz levels. Peak levels should not be used for radhaz assessments.[16]

With the detector modes explained, we describe how the sweep times were calculated. For peak-detected measurements, even a single high-power event in the time domain will latch the detector during each bin interval. A total of 10 such events per bin interval would result in a near-unity probability of ensuring that a true peak power level was latched during any given bin interval. For RMS average measurements, however, a larger number of digitized points needs to be sampled and averaged during each bin interval if the resulting average for each bin is to be statistically valid. Not less than 100 such points should be averaged during each bin interval for a good RMS average.

For these measurements, we chose to double those values for each bin. That is, we would require 20 possible peak events and 200 good RMS samples per spectrum analyzer bin in each trace, just to be certain that we were obtaining valid numbers in our final statistics. Given that we set the number of bins to 1001 per trace (so as to get good frequency resolution per bin; see the sixth column of Table 3), and given that the jammer had a set rate of sweeping across each CMRS band (taken from the data in Table 2), the required spectrum analyzer *sweep time* for each CMRS band measurement was thus fully determined.

Consider, for example, the first row of Table 3. The CMRS band for that row is 723–763 MHz. This range is 40 MHz wide. So the bandwidth per displayed bin would be 40 MHz divided by 1001 display bins, which gives 40 kHz per display bin. This is less than the selected resolution bandwidth of 100 kHz for that row, meaning that the resolution of the displayed trace will be determined by the analyzer's 100 kHz resolution bandwidth and not by the 40 kHz width of each of the display bins.

Next, we examine Table 2 and look up the time that it takes the jammer to complete each of its chirped-tuned cycles in this CMRS band. We find that this interval is 14.2 microseconds. For peak detection, we want (need) 20 such cycles for each of the analyzer's bins. This gives a total of 284 microseconds required per bin. Multiplying this by 1001 bins gives 0.284 seconds per sweep for the peak-detected measurements in Row 1 of the table. (The time is rounded to 0.28 seconds as that represents the accuracy limit of the E4407B spectrum analyzer's sweep timing.)

For the RMS average measurements in Row 1 of the table, we follow the same procedure but obtain a different result. Because (as noted above) we need 200 jammer frequency sweeps to occur for each of the RMS average values that we compute in each bin, the final value for the sweep time will be 10 times longer than the 0.28 seconds that we set for the peak-detected measurements (where we only needed 20 jammer frequency sweeps per spectrum analyzer bin).

[16] Peak levels should nt be used because radhaz limits, standards, and recommendations are based on total amounts of energy that may be loaded into body tissues or ordnance by radio waves over given time intervals. These amounts are measured in terms of incident energy per unit time (incident power) per unit of target surface area or target mass that is exposed, the exposure itself needing to be being averaged over appreciable, specified intervals. Peak detected power levels may show incident-power events that are too brief to affect average loading levels.

This means that each RMS average data trace must be 28 seconds long.[17] This process, repeated for each of the CMRS bands, provides the measurement parameters for all of the CMRS bands in Table 3.

For the non-CMRS bands (the bottom four rows in Table 3, we increased the number of jammer sweeps that we would obtain for each peak-detected bin. We did this so that we could have a good chance of seeing the even less-likely peak events that might occur in the non-CMRS bands where any jammer emissions would be unintentional. Only peak detection was used in the non-CMRS bands because such emissions were considered unlikely and, if they occurred at all, they might well be sporadic and thus might only be observable with peak detection. If nothing appears in a peak-detected measurement such as in the last four rows of Table 3, then there will obviously be no measurable RMS average.

### 3.2.4 Frequency-Span Sweep Times and Derived Jammer Emission Statistics

With the measurement bandwidths, detector modes, and spectrum analyzer sweep times all determined (Table 3), the only remaining parameter to calculate was the total number of spectrum analyzer traces (sweeps) that needed to be collected for each row in the measurement table. This number needed to be as large as possible, so as to obtain valid statistics. The limiting factor on this number was the total amount of time available to perform all measurements at Cumberland FCI.

The number of sweeps per row in Table 3 was determined as follows. All data needed to be collected within a single working day at Cumberland FCI. Allowance needed to be made for the time to enter the facility, set up, warm up and calibrate the measurement equipment, provide an in-briefing for the day's work, move around inside the facility from place to place, and accommodate the necessary 20-minute intervals for jammer warm-up and stabilization whenever the jammer was re-activated after a jammer-off measurement. Additional time would be needed to allow for any possible technical problems that might arise, and then finally to provide a de-briefing, take apart the measurement system, and exit the facility. Estimating these required intervals, we decided that all measurements needed to be acquired in about two hours of actual spectrum analyzer data acquisition time. Since four measurement locations were planned, all data had to be taken at each measurement location in about 30 minutes. Moreover, because all of the measurements in Table 3 had to be taken twice at each location (once with the jammer on and once with the jammer off), each complete set of measurements in that table needed to be taken in 15 minutes.

Empirical testing at the ITS Boulder laboratory prior to deployment to Cumberland showed that a total of 50 spectrum analyzer sweeps per row in Table 3 for the CMRS bands, with 30 sweeps of one second each for the remaining rows (non-CMRS bands), plus additional intervals for the

[17] The most technically correct number would be 28.4 seconds per sweep for the RMS averages, but for simplicity we simply multiplied the peak-trace times by a factor of 10.

single-sweep measurements shown in the table, met the criterion of 15 minutes of operational time for completion of all measurements in that table.[18]

For 50 traces in each CMRS band measurement iteration, and with 20 jammer sweeps occurring for each of those 50 accumulated spectrum analyzer traces, there were a total of 1,000 (50 × 20) jammer sweeps accumulated for each measured frequency bin. Those data were post-processed to show the maximum, minimum, median and mean statistical peak-power levels recorded in each peak-detected spectrum analyzer bin across all 50 spectrum analyzer sweeps and 1,000 jammer sweeps. These statistics from the raw data are called peak-swept M4 outputs, referring to the measurement detection mode, the analyzer's frequency-sweeping behavior, and the four statistical M's (maximum, minimum, mean, and median) in the output.

For the RMS averaging mode, where 200 jammer sweeps occurred per bin per spectrum analyzer trace, a total of 50 spectrum analyzer traces yielded 50 × 200 = 10,000 total jammer sweeps for the average power measurement in each jammer band. Similarly for the peak-detected measurements, those data were analyzed for their average-swept M4 outputs across all 50 analyzer sweeps and 10,000 jammer sweeps.

For the additional spectrum measurements in non-CMRS bands across 300 MHz to 2.55 GHz, the measurement resolution bandwidth was set at 1 MHz for the reasons noted in the sub-section above (expedience in measurement time plus the usefulness of 1 MHz as a reference bandwidth) In these scans, either 70 or 140 jammer sweeps occurred for each measured frequency bin during each spectrum analyzer frequency sweep, depending on the jammer band (see Table 2). This is the number of jammer sweeps that occurred per measured spectrum bin per spectrum analyzer sweep. The measurement team collected 30 maximum-hold mode sweeps in each of those scans. This resulted in a total of 30 × (70 or 140) = 2100 or 4200 total jammer sweeps per measured frequency bin for each of the scanned bands, again the result depending on which jammer band (Table 2) was being measured. The corresponding M4 statistics were later processed for each measured analyzer frequency bin.

For the final scans performed at each measurement location across 3.84 to 4.34 GHz (the frequency range covered any jammer second harmonics not otherwise already measured within 300 MHz to 2.55 GHz), we allowed maximum-hold mode to run for 30 sweeps. This again resulted in a total of 2100 or 4200 total jammer sweeps per measured frequency bin for the scanned band, again depending on which jammer band (Table 2) is referenced. The resulting M4 statistics were later processed for each measured frequency bin.

### 3.3 Spectrum Analyzer Preamplifier

The 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

[18] Arithmetic shows that the computed total time for all measurements in Table 3 is only about 5 minutes. Overhead factors in the measurement system, however, including sweep-to-sweep termination and re-triggering intervals and data-transfer intervals between the spectrum analyzer and its laptop computer controller, increased the overall operational interval for all of the measurements to a total of 15 minutes.

its sensitivity) by 10 dB when it is turned on. Thus the preamp can make weak signals visible (e.g., second harmonics of jammer emissions), signals which would have otherwise been below the spectrum analyzer's noise floor.[19]

However, the analyzer's power-overload point is reduced by 10 dB with the preamp activated. So, the preamp should only be used when the *sum total* power from all signals in its response range (0–3 GHz for the E4407B) does not exceed its overload capacity (about -30 dBm). Since it can be difficult to know the total, integrated power in all such signals, some empirical work sometimes needs to be done on the spot at any given measurement site to determine whether the preamp's use is appropriate or not. Such an empirical test was performed inside the prison cell after a set of non-preamp data was initially acquired, as noted in the chronology below. Based on this datum it was determined that overload of the preamp did not occur.

### 3.4 Time-Domain Data Collection

In each of the targeted CMRS bands, the spectrum analyzer was operated in a zero-hertz span mode at one of the prison-cell measurement locations to collect time-domain data. These data showed the chirping behavior of the jammer. The jammer's emissions will appear pulse-like when seen on single frequencies in the time domain. This is because the jammer sweeps through each individual frequency for a limited interval during each complete band sweep.

### 3.5 Measurement System Calibration

Because the measurement system consisted only of the E4407B spectrum analyzer, and because the measurement data were to be primarily comparative (power on a frequency with the jammer on *versus* off) rather than absolute, 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 was negligible.) All power measurements in this report's graphics are calibrated in units of dBm per unit measurement bandwidth in the 50 ohm circuitry at the measurement antenna terminals. A field strength correction table is provided in the Data Analysis section of this report, to convert power in the measurement circuitry into incident power per unit area in space at the antenna.

### 3.6 Measurement Control Software

The spectrum analyzer was controlled by a laptop PC running ITS-developed data acquisition software called Radio Spectrum Measurement System 5$^{th}$ Generation (RSMS-5G). The software was configured prior to the Cumberland trip to automatically run the measurements shown in Table 3. The software ran each of the measurements listed in that table twice at each

[19] The spectrum analyzer's noise figure, *NF*, was 37 dB with preamp off, zero attenuation, and reference level set to -10 dBm; it was 17 dB when the preamp was turned on. Peak detection adds approximately 10 dB to noise floor. The noise floor in any bandwidth was: (-174 dBm + 10 log($B_{meas}$) + *NF* + (10 dB for peak detection, if used)). For example, in 100 kHz resolution bandwidth with the preamp on and positive peak detection in use, the analyzer's noise floor was about (-174 dBm + 50 dB + 17 dB + 10 dB) = -97 dBm.

measurement location. The two runs were performed, 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 measurements in the 300 MHz to 2.55 GHz and 3.84 GHz to 4.34 GHz frequency ranges were likewise run twice at each measurement location, once with the jammer on and once with the jammer off.

### 3.7 Data Recording and Format

The spectrum measurement data were automatically retrieved from the spectrum analyzer after every individual analyzer sweep was completed. Frequency sweep data were stored on the measurement PC's hard drive in MATLAB® format. They consisted of power as a function of frequency. Time-domain data were stored as power as a function of time.

### 3.8 Measurement Chronology

All measurements were performed at Cumberland FCI on January 17, 2018. The measurement gear had been previously shipped to Cumberland from Boulder and had been preliminarily tested the night before at the authors' hotel lodging. On the morning of January 17, the NTIA engineers assembled the measurement system, including the portable equipment cart, in the Cumberland FCI 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 the on-board battery power supply). The measurement system was then rolled to a ground-level medium security prison cell (Figure 2).

The jammer manufacturer's personnel turned on the jammer device located in the utility closet adjacent to the targeted prison cell (Figure 2). The measurement system was rolled inside the cell and the antenna was positioned at measurement location Interior-1 (I-1 in Figure 2 and Table 4). The spectrum analyzer's preamplifier was turned off and the data were collected in accordance with Table 3. A set of representative time-domain pictures were captured at I-1, as well. Next, with the jammer still on, the measurement antenna was positioned at I-2 and the Table 3 data were again collected (still with the analyzer's preamp off). The jammer was then turned off and data sets were once again collected at positions I-1 and I-2 with the analyzer's preamp off. Table 4 summarizes the subsequent data collection and chronology for the day.

Table 4. Data collection summary for Cumberland FCI, January 17, 2018.

| Data File Number[20] | Starting Time (EST) | Measurement Location | Jammer State | Spectrum Analyzer Preamp State |
|---|---|---|---|---|
| 9 | 1000 | I-1 | On | Off |
| 10 | 1013 | I-2 | On | Off |
| 11 | 1029 | I-2 | Off | Off |
| 12 | 1042 | I-1 | Off | Off |

[20] These are RSMS-4G data file numbers; data files 1-8 were collected during earlier measurement system check-out and testing in Boulder and at the Cumberland hotel.

| Data File Number[20] | Starting Time (EST) | Measurement Location | Jammer State | Spectrum Analyzer Preamp State |
|---|---|---|---|---|
| 13 | 1126 | I-1 | Off | On |
| 14 | 1220 | O-1 | On | On |
| 15 | 1243 | O-2 | On | On |
| 16 | 1257 | O-2 | Off | On |
| 17 | 1311 | O-1 | Off | On |

One more set of data was collected in the targeted cell during the lunch break. For this final indoors data set, the jammer was off and the spectrum analyzer preamp was, for the first time that day, turned on. This final data collection showed relatively weak ambient CMRS signals inside the targeted cell better than in the earlier data, because the analyzer's noise floor was improved by 20 dB.

The outdoor measurements were performed in the afternoon. Two measurement locations in the prison yard were marked at distances of 6.1 m (20 ft) and 30.5 m (100 ft) directly outside the window of the targeted prison cell. The locations, identified respectively as O-1 and O-2 (Figure 2) were on short grass with a couple of inches of snow, and with clear LOS to the cell's window. The measurement antenna was at the same height as the central level of the window. All outdoor measurements were performed with the analyzer's preamp turned on, due to lower incident power from the jammer signal and the need to see detail in those weaker jammer signals. (The combined power of the jammer signal and the ambient CMRS signals was observed to be less than the analyzer's overload threshold.)

With the jammer turned on and warmed up, data sets were collected at O-1 and O-2. Then the jammer was turned off and the data sets were collected again, in reverse order (O-2 followed by O-1).

This concluded the data collection at Cumberland FCI. The NTIA engineers subsequently out-briefed government staffers in a Cumberland FCI conference room, disassembled and re-packed their gear for return shipment to Boulder, and exited the facility.

## 4. MEASUREMENT RESULTS

Table 5 summarizes the data graphs in this report. 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 Cumberland FCI data. All data sets in Table 5 contain comparative jammer-on *versus* jammer-off pairs except Figures 5–8 (the time domain plots) and Figures 42–44 (taken only to show more detail for the ambient CMRS signals inside the targeted prison cell). Appendix A provides peak-detected measurements in 1 megahertz bandwidth as Figures A-1 through A-32.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.

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

Table 5. Key for data figures in this report.

| Figures | Location | Frequencies | Bandwidth | Detection | Preamp |
|---|---|---|---|---|---|
| 5–8 | I-1 | All CMRS bands | 1 MHz | Peak | off |
| 9–16 | I-1 | All CMRS bands | 100 kHz | Peak | off |
| 17–24 | I-1 | 300 – 4340 MHz | 1 MHz | Peak | off |
| 25–32 | I-2 | All CMRS bands | 100 kHz | Peak | off |
| 33–40 | I-2 | 300 – 4340 MHz | 1 MHz | Peak | off |
| 41–44[21] | I-1 | All CMRS bands | 100 kHz | Peak | on |
| 45–52 | O-1 | All CMRS bands | 100 kHz | Peak | on |
| 53–60 | O-1 | 300 – 4340 MHz | 1 MHz | Peak | on |
| 61–68 | O-2 | All CMRS bands | 100 kHz | Peak | on |
| 69–76 | O-2 | 300 – 4340 MHz | 1 MHz | Peak | on |
| 77–84 | I-1 | All CMRS bands | 100 kHz | Average | off |
| 85–92 | I-2 | All CMRS bands | 100 kHz | Average | off |
| 93–100 | O-1 | All CMRS bands | 100 kHz | Average | on |
| 101–108 | O-2 | All CMRS bands | 100 kHz | Average | on |
| A-1–A-8 | I-1 | All CMRS bands | 1 MHz | Peak | off |
| A-9–A-16 | I-2 | All CMRS bands | 1 MHz | Peak | off |
| A-17–A-24 | O-1 | All CMRS bands | 1 MHz | Peak | on |
| A-25–A-32 | O-2 | All CMRS bands | 1 MHz | Peak | on |

[21] These measurements were taken inside the targeted prison cell with the preamp turned on and the jammer turned off. They were taken with the preamp on to better show the ambient CMRS signals inside the cell; without the preamp those CMRS signals were difficult to observe in any detail inside the cell.

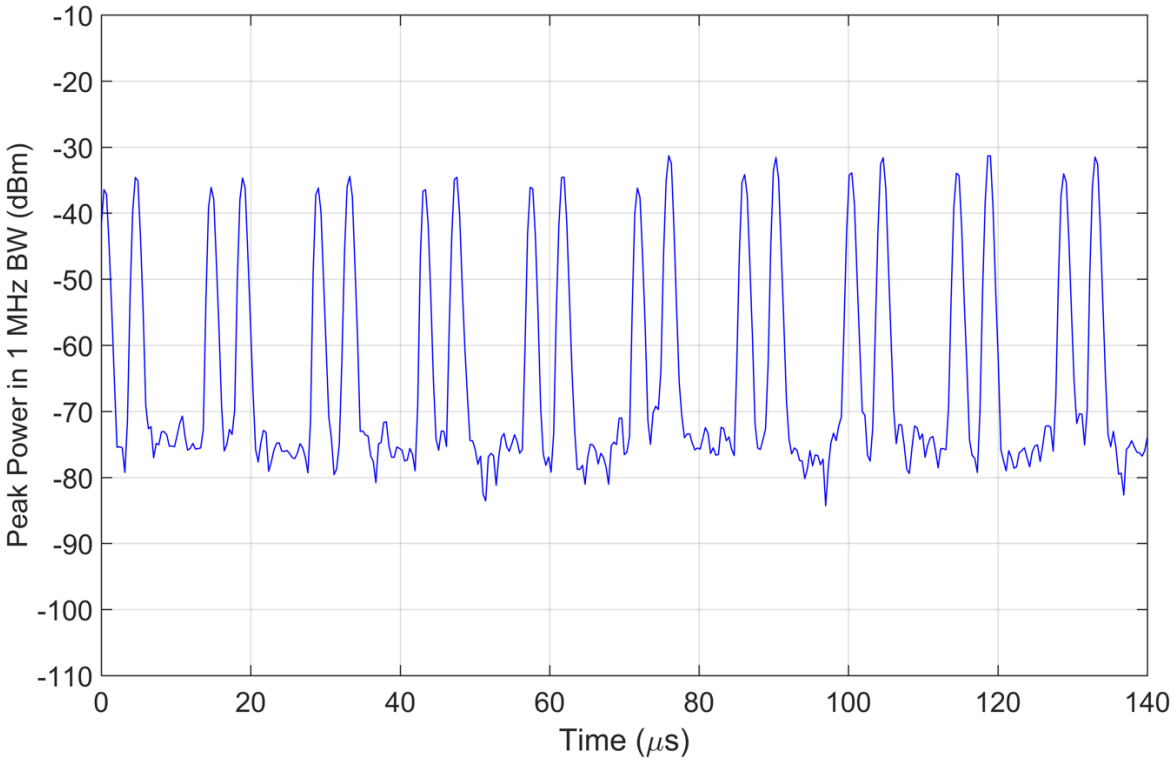


Figure 5. Example of jammer time domain emission at 750 MHz in a CMRS band.

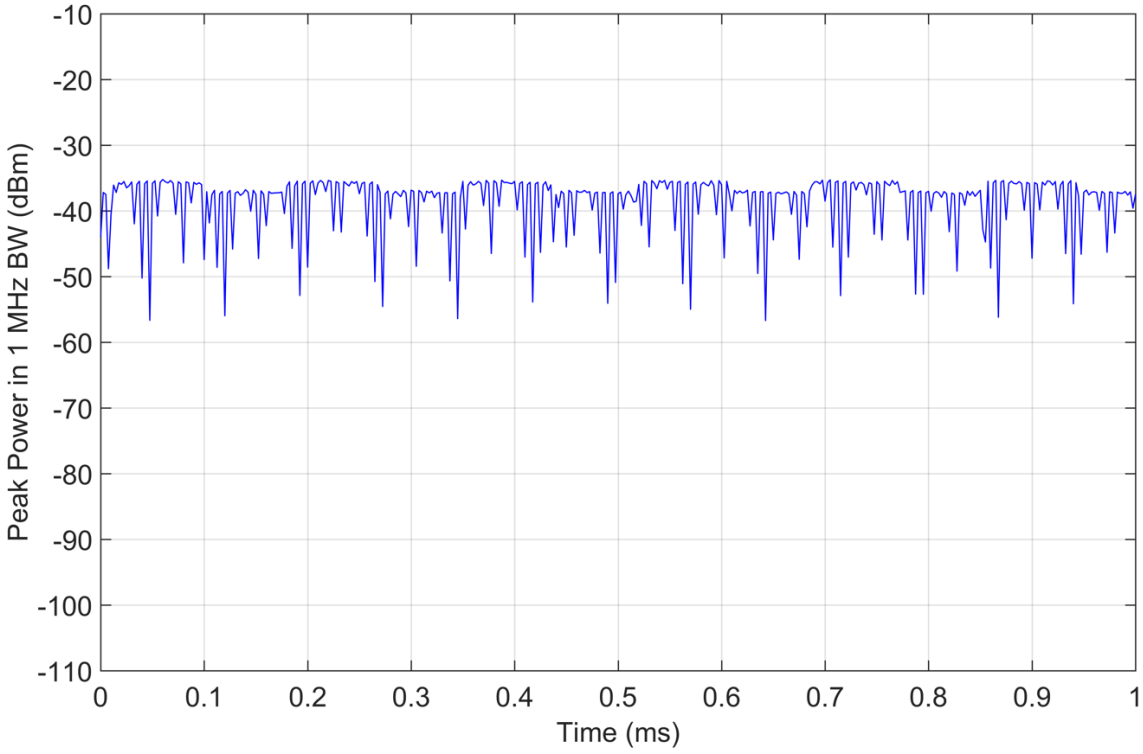


Figure 6. Example of jammer time domain emission at 883 MHz in a CMRS band.

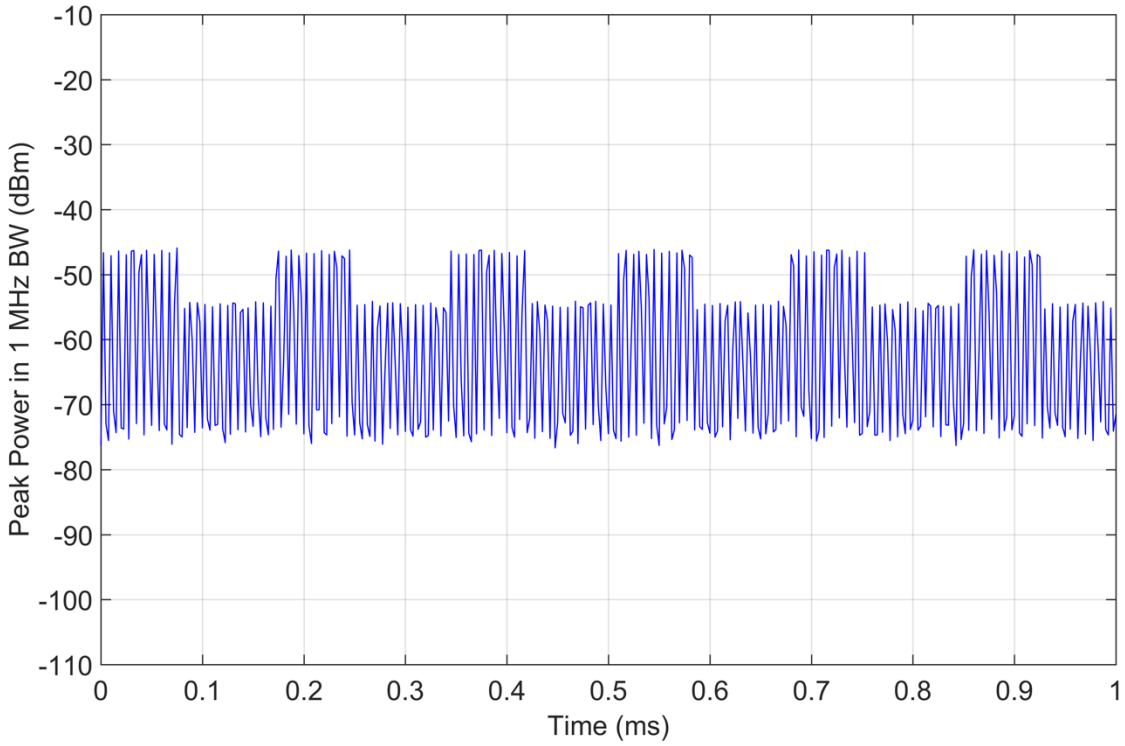


Figure 7. Example of jammer time domain emission at 1961 MHz in a CMRS band.

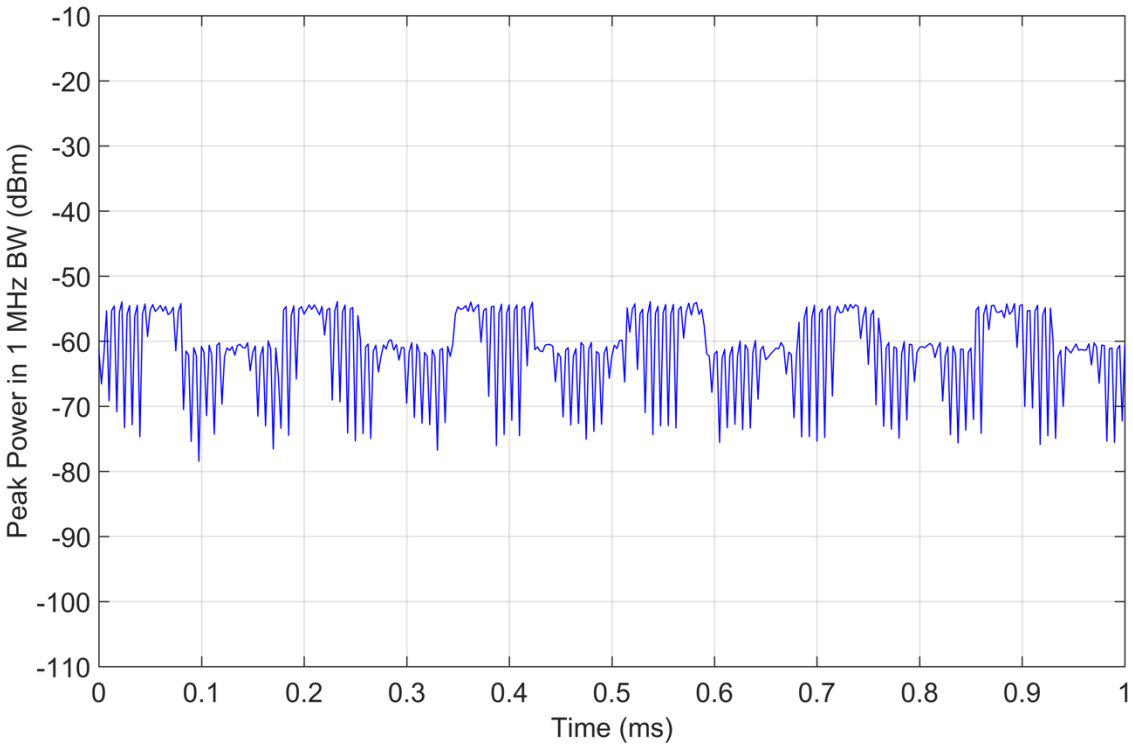


Figure 8. Example of jammer time domain emission in the 2110–2155 MHz CMRS band.

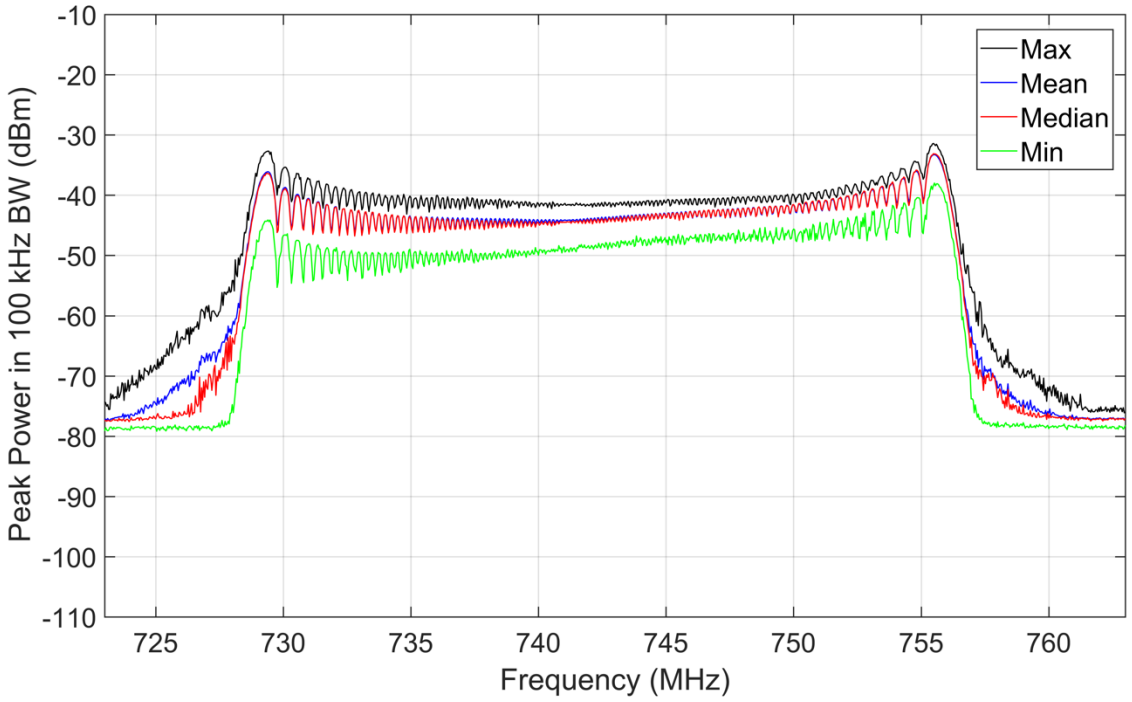


Figure 9. M4 statistics, peak detection, jammer on, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

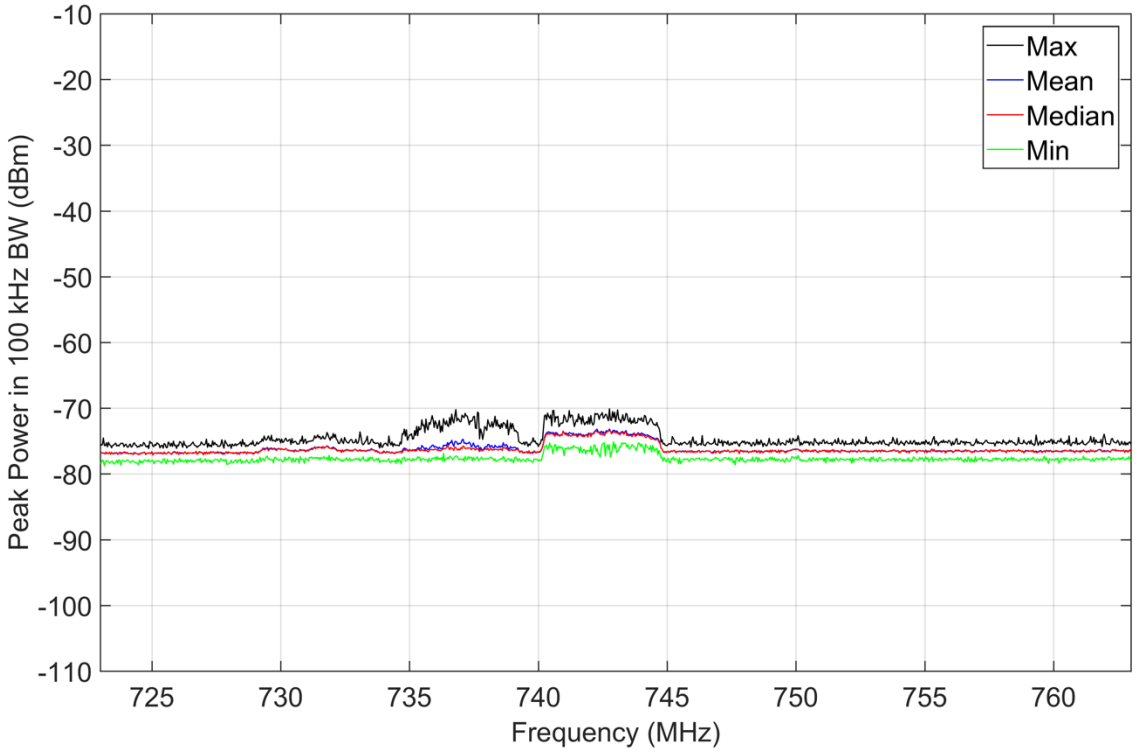


Figure 10. M4 statistics, peak detection, jammer off, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

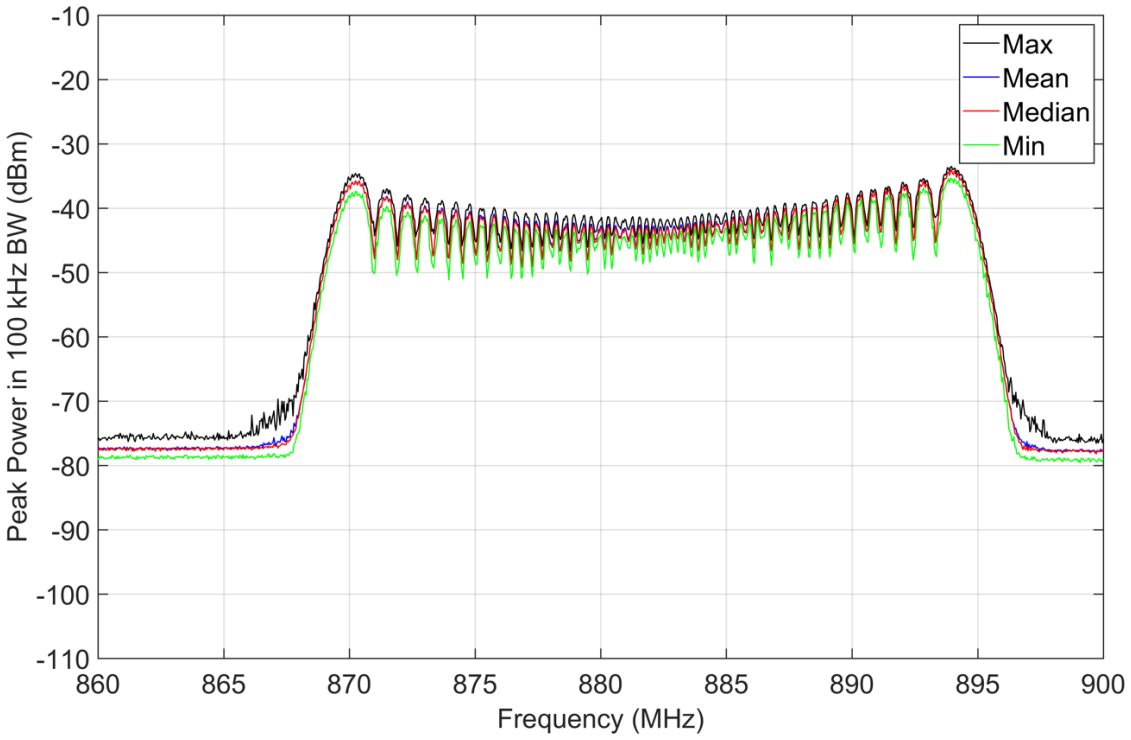


Figure 11. M4 statistics, peak detection, jammer on, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

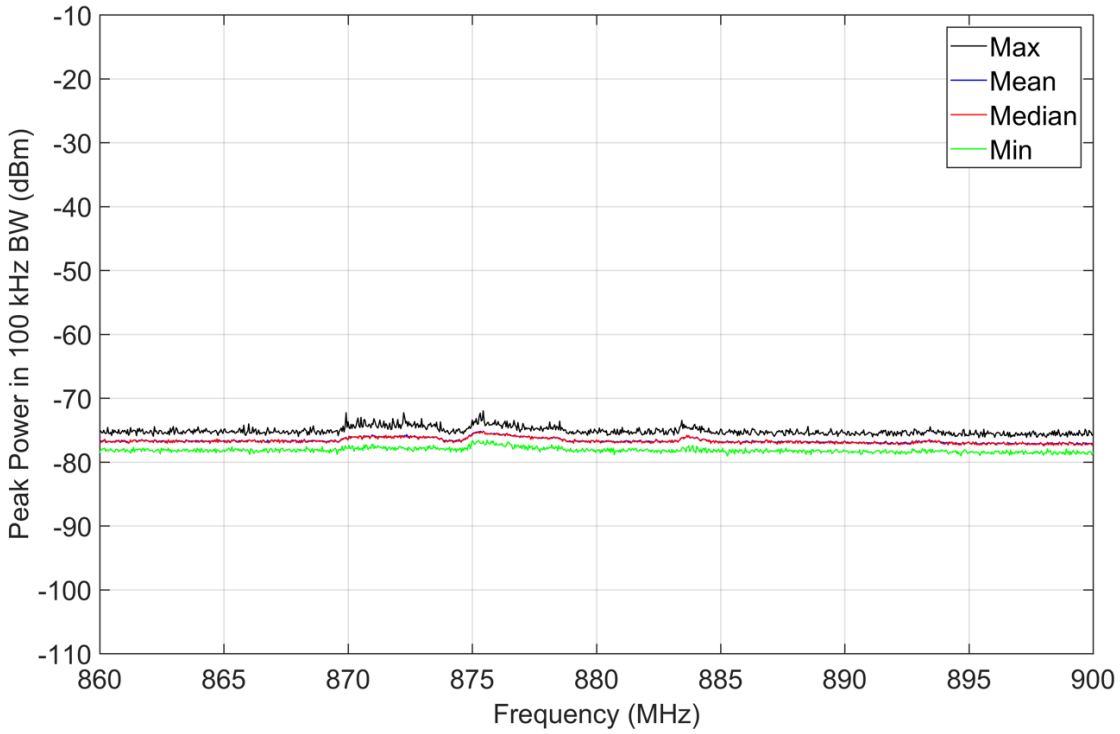


Figure 12. M4 statistics, peak detection, jammer off, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

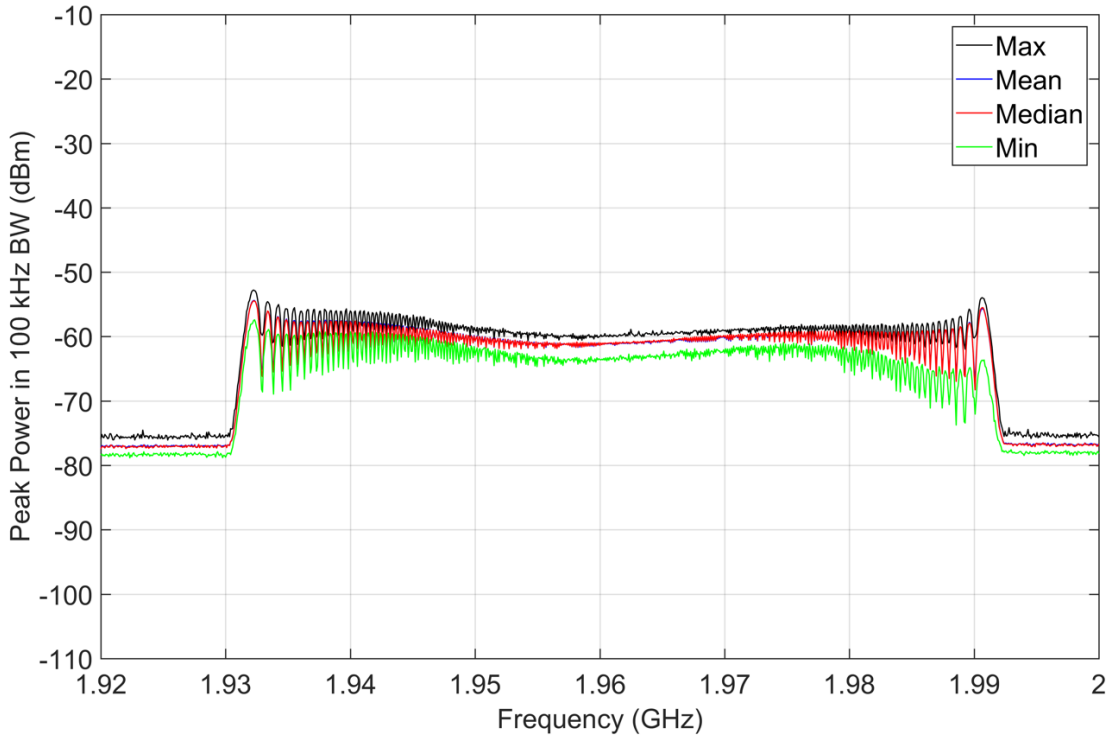


Figure 13. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

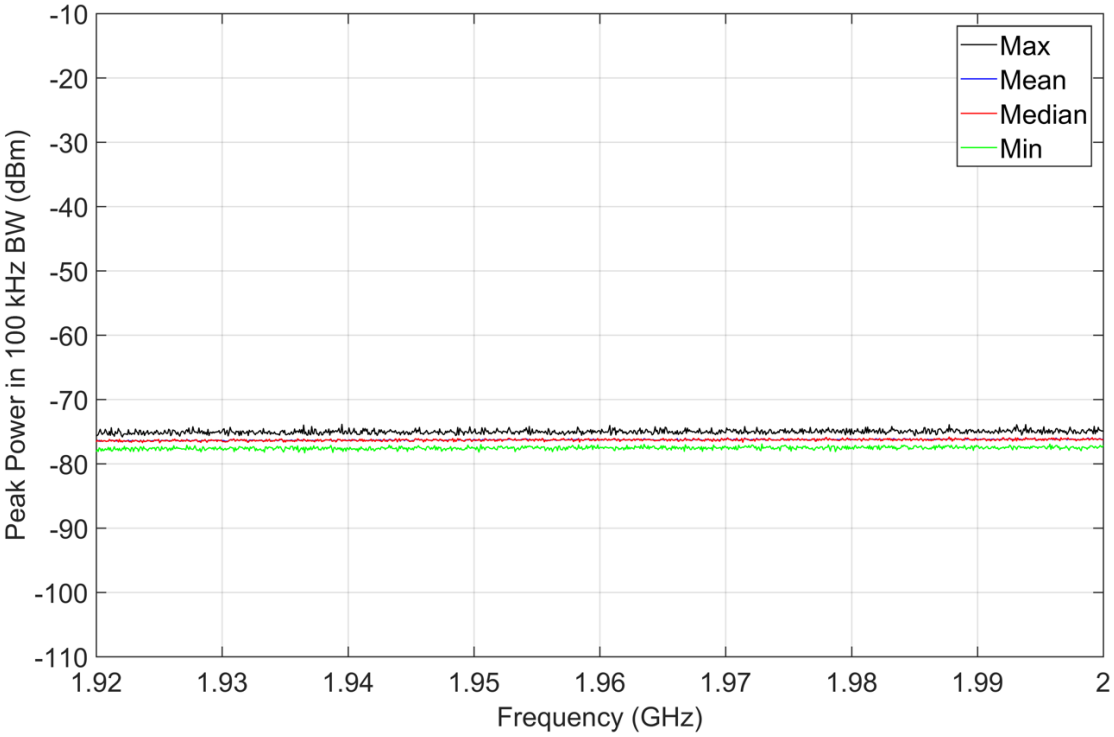


Figure 14. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

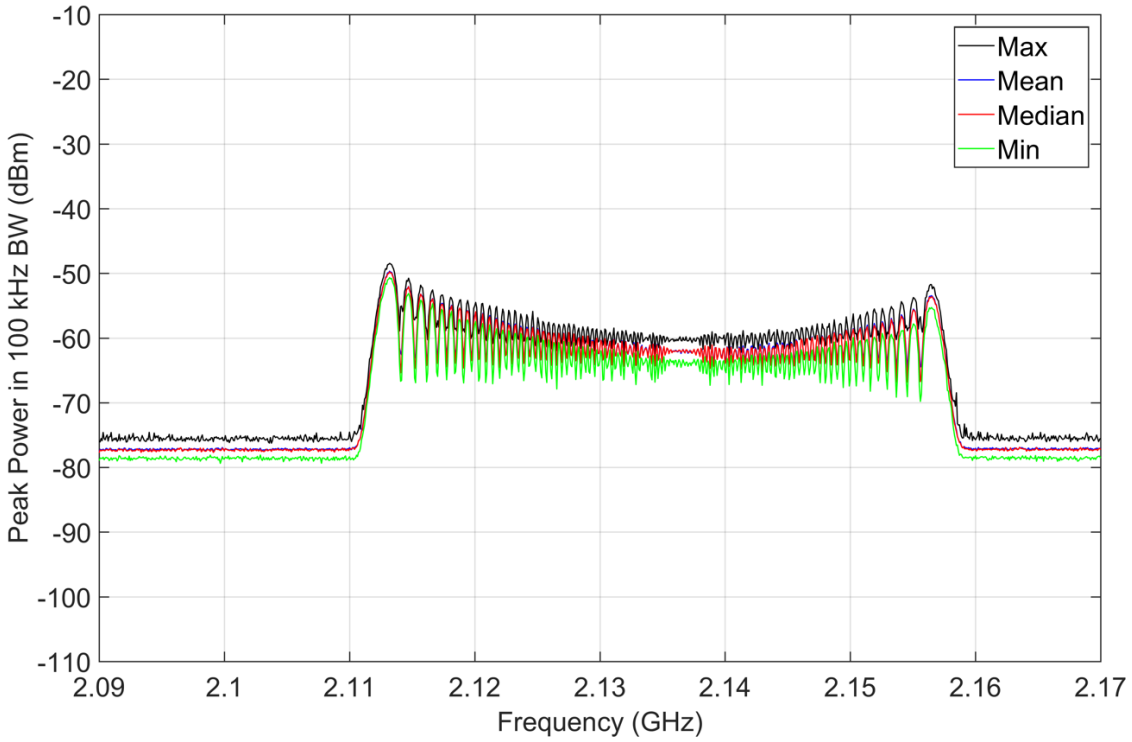


Figure 15. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

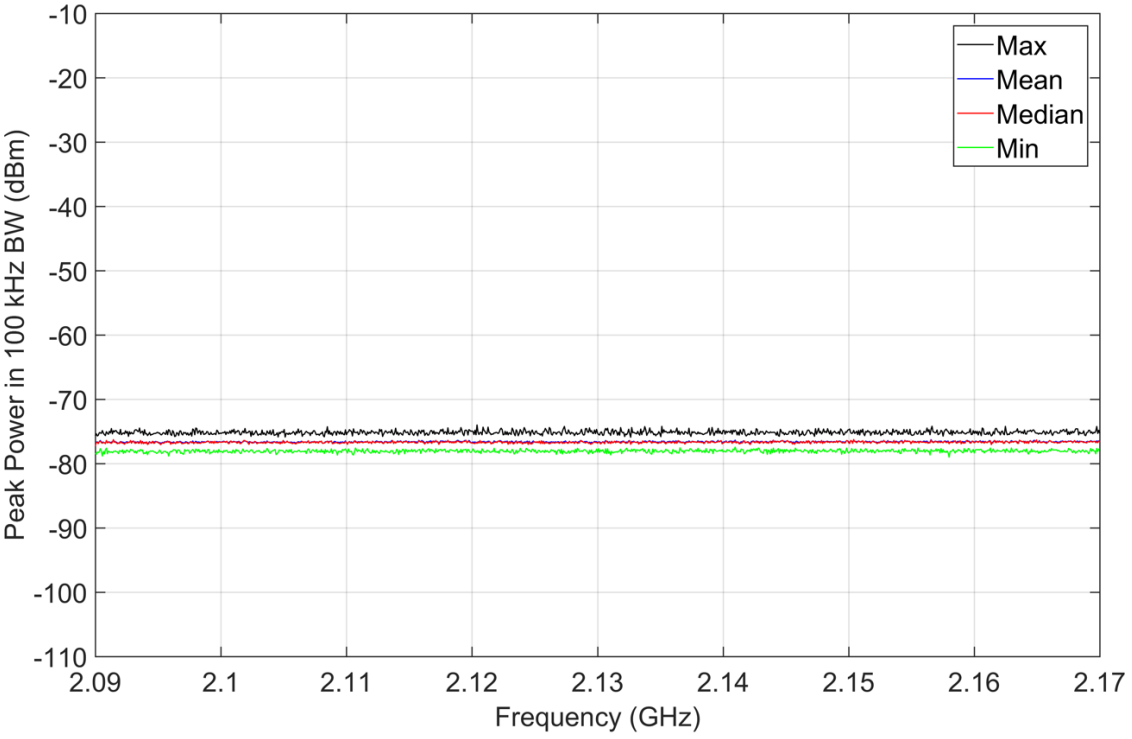


Figure 16. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

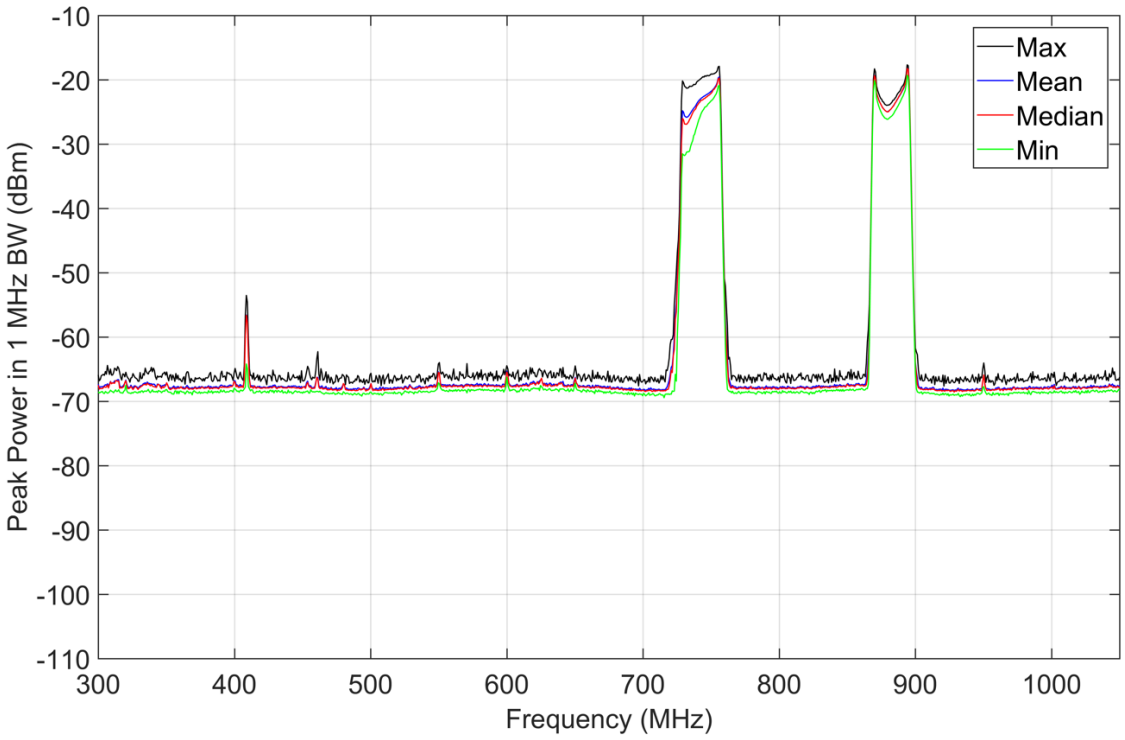


Figure 17. M4 statistics, peak detection, jammer on, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

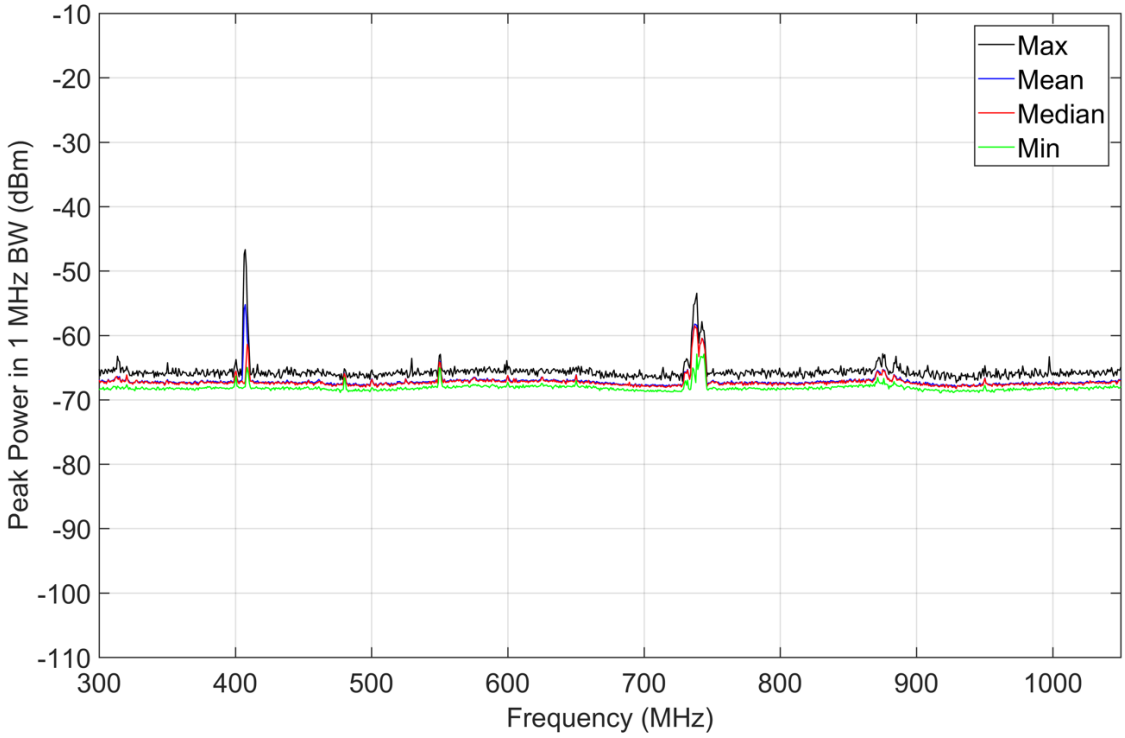


Figure 18. M4 statistics, peak detection, jammer off, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

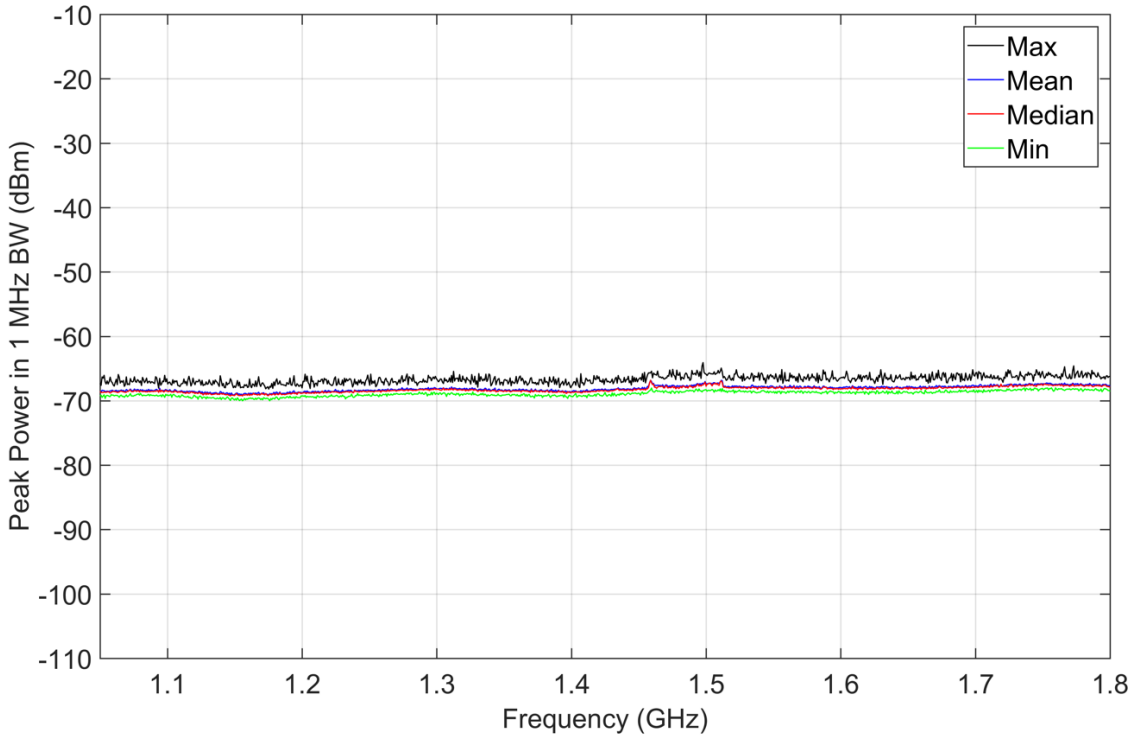


Figure 19. M4 statistics, peak detection, jammer on, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

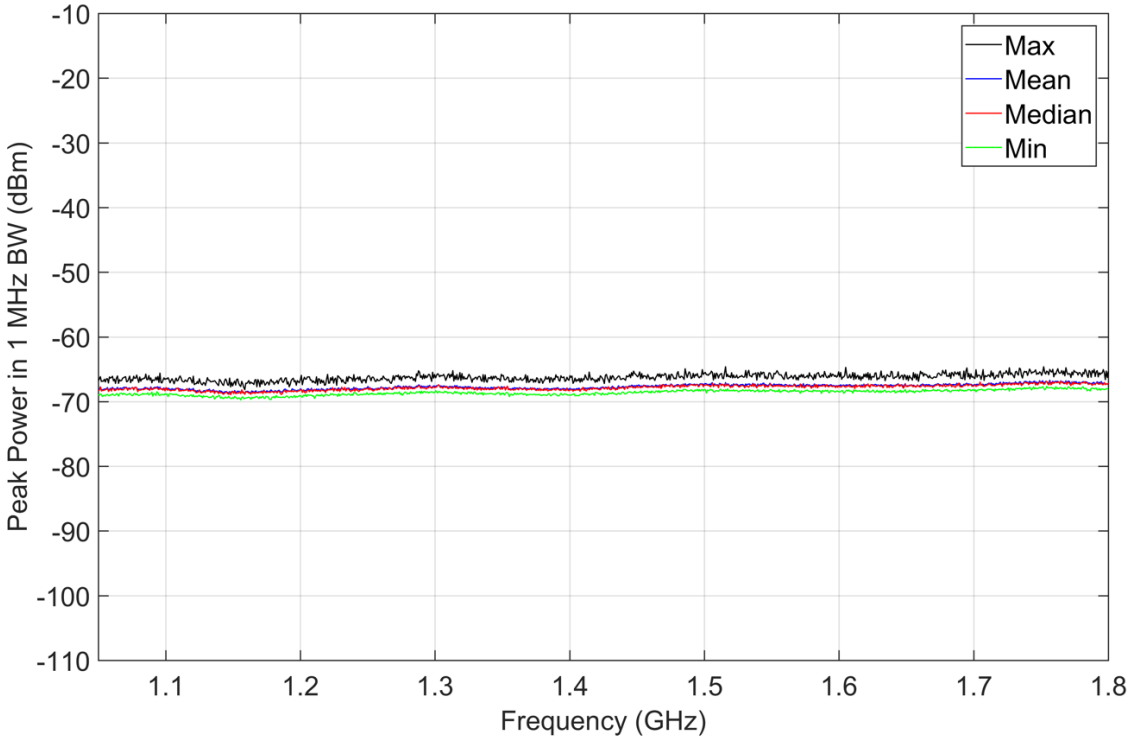


Figure 20. M4 statistics, peak detection, jammer off, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

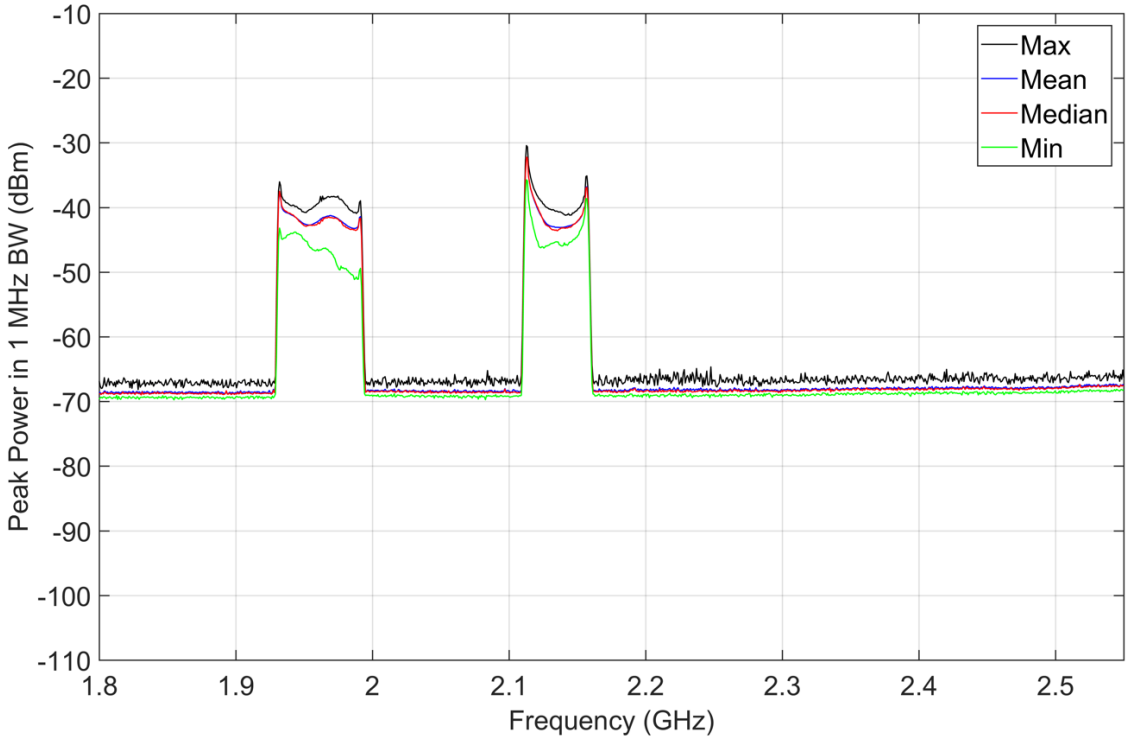


Figure 21. M4 statistics, peak detection, jammer on, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

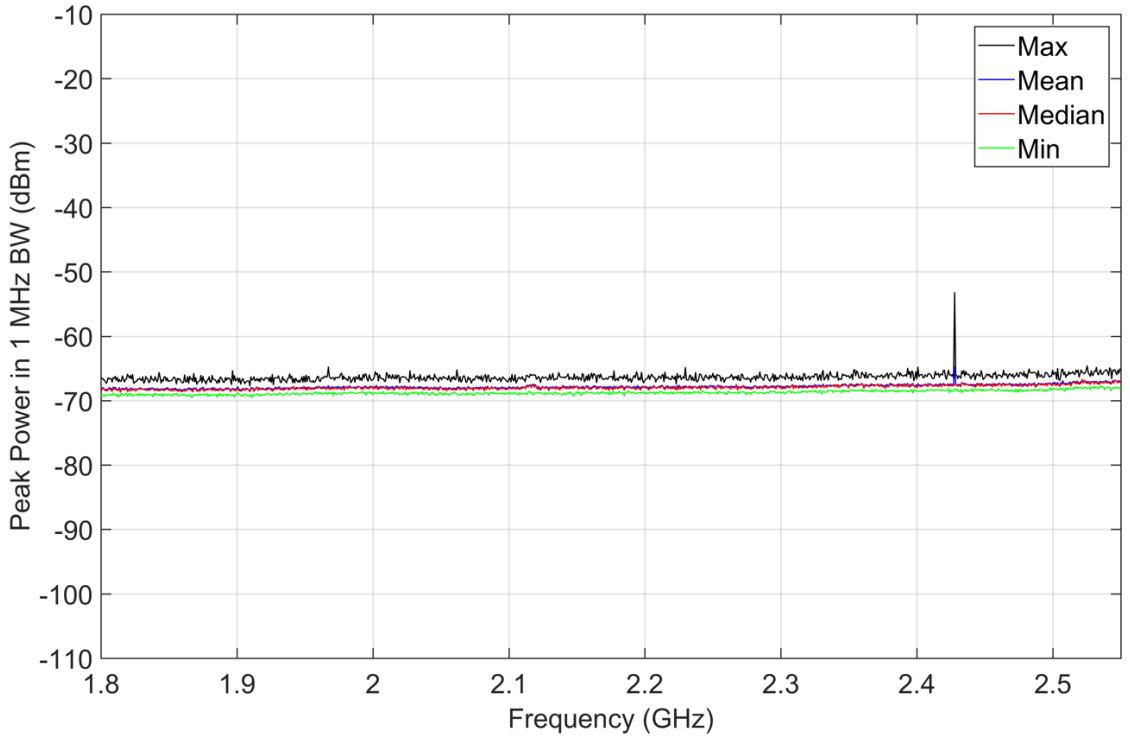


Figure 22. M4 statistics, peak detection, jammer off, 1800–2550 off MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

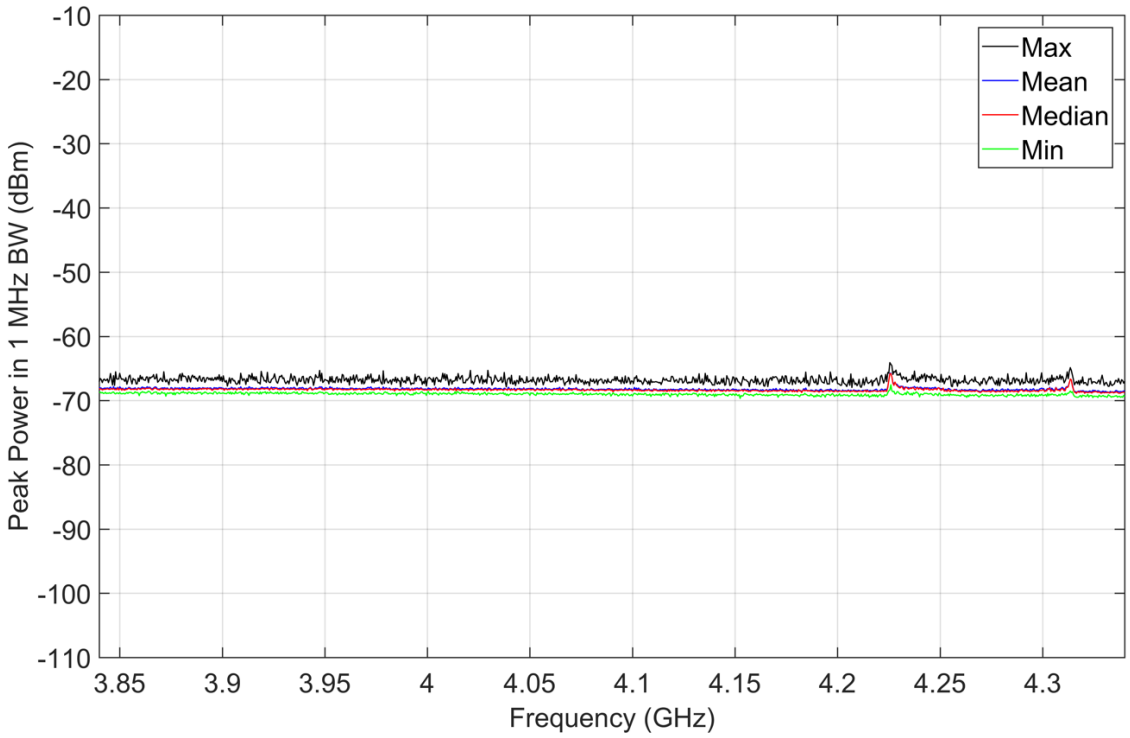


Figure 23. M4 statistics, peak detection, jammer on, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

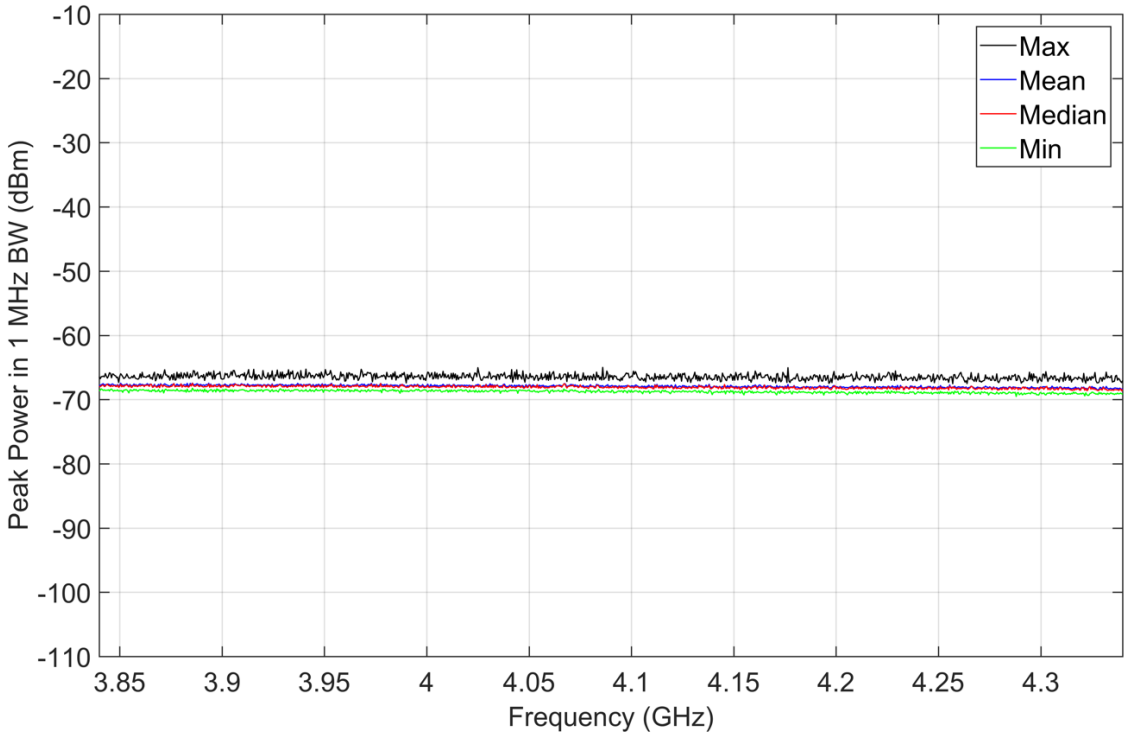


Figure 24. M4 statistics, peak detection, jammer off, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

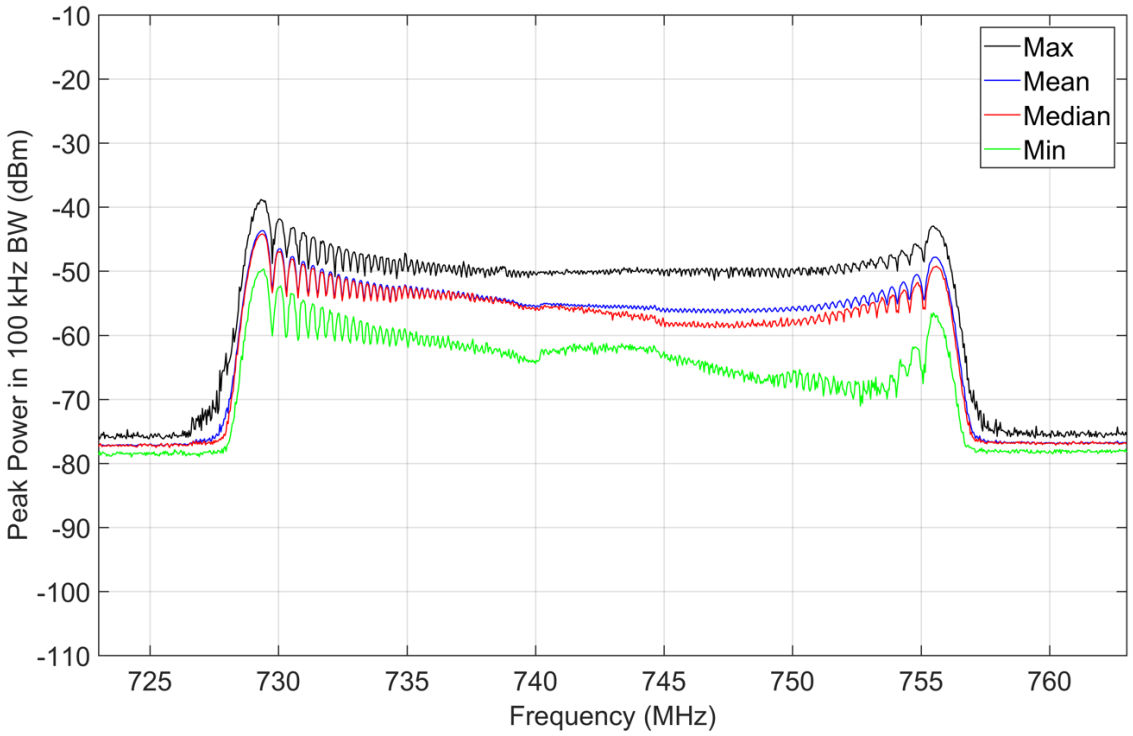


Figure 25. M4 statistics, peak detection, jammer on, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

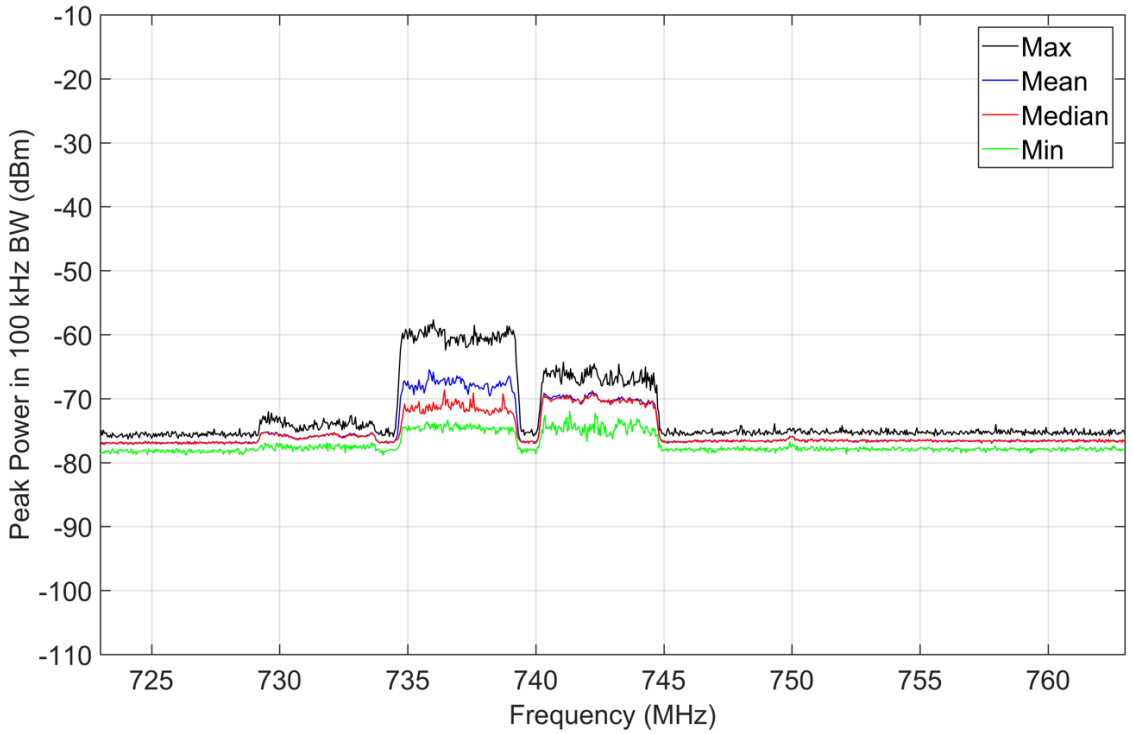


Figure 26. M4 statistics, peak detection, jammer off, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

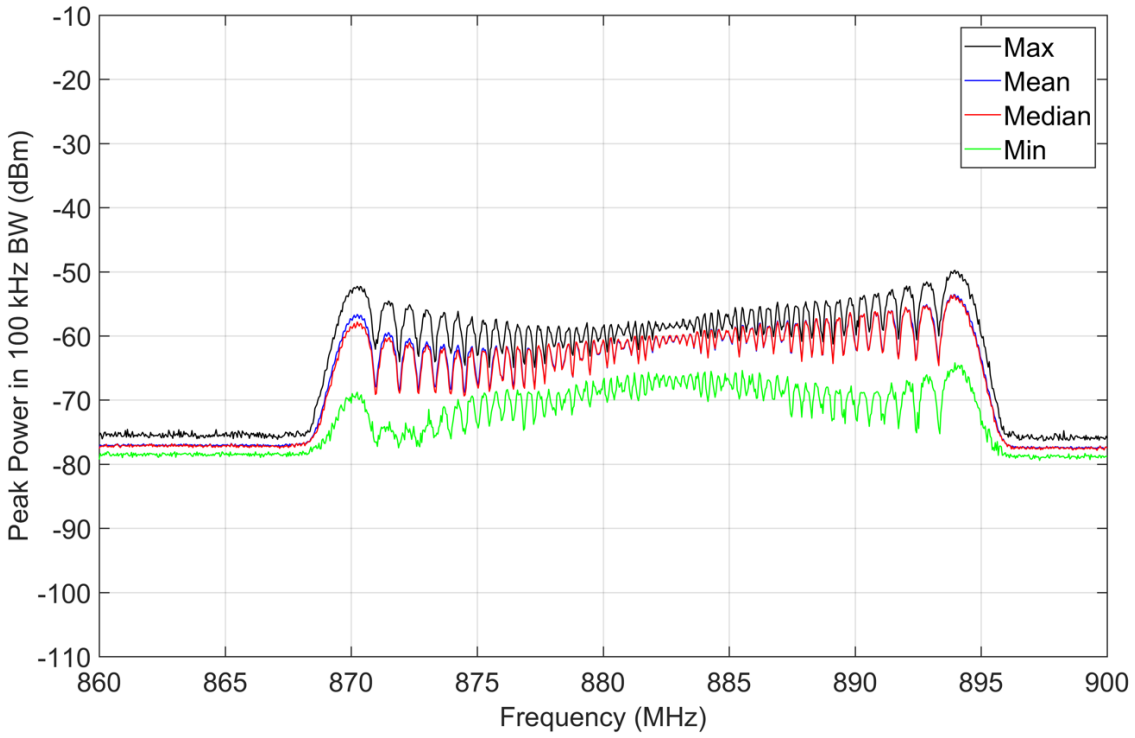


Figure 27. M4 statistics, peak detection, jammer on, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

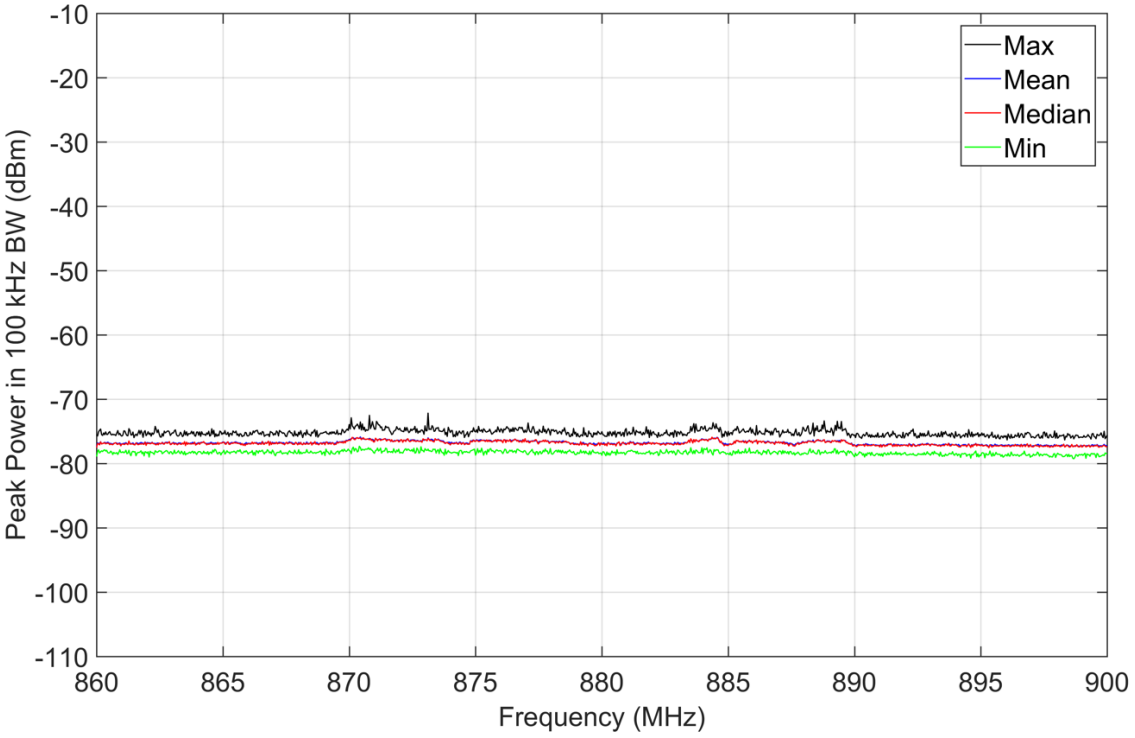


Figure 28. M4 statistics, peak detection, jammer off, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

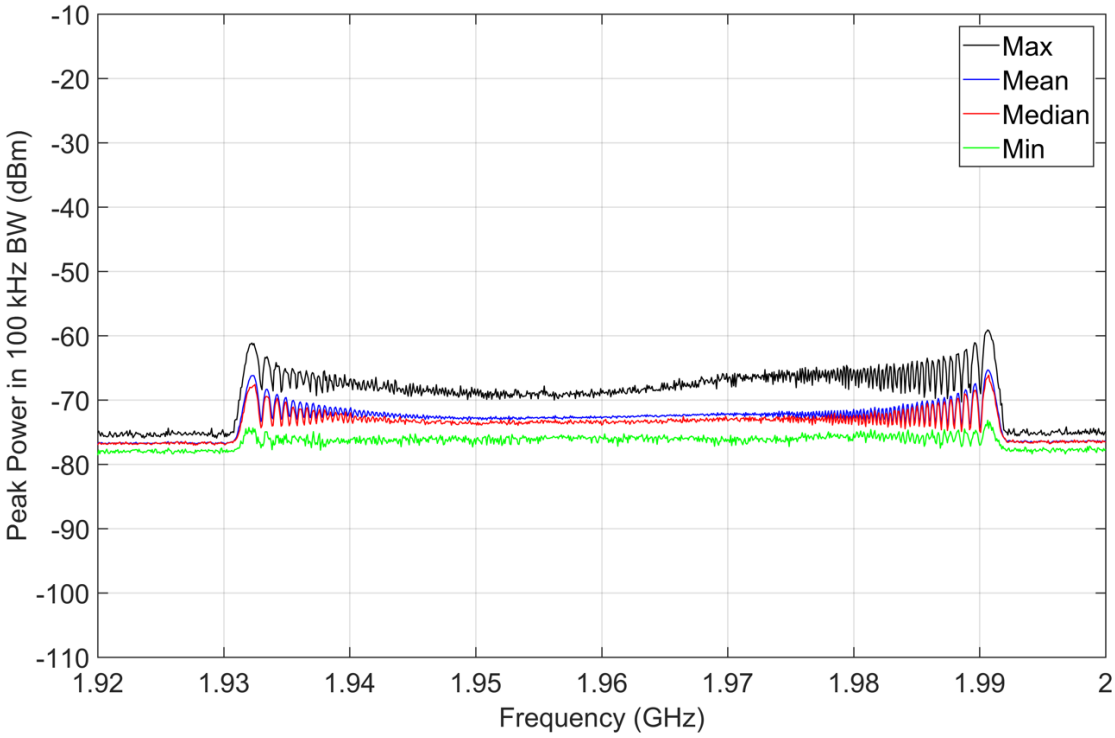


Figure 29. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

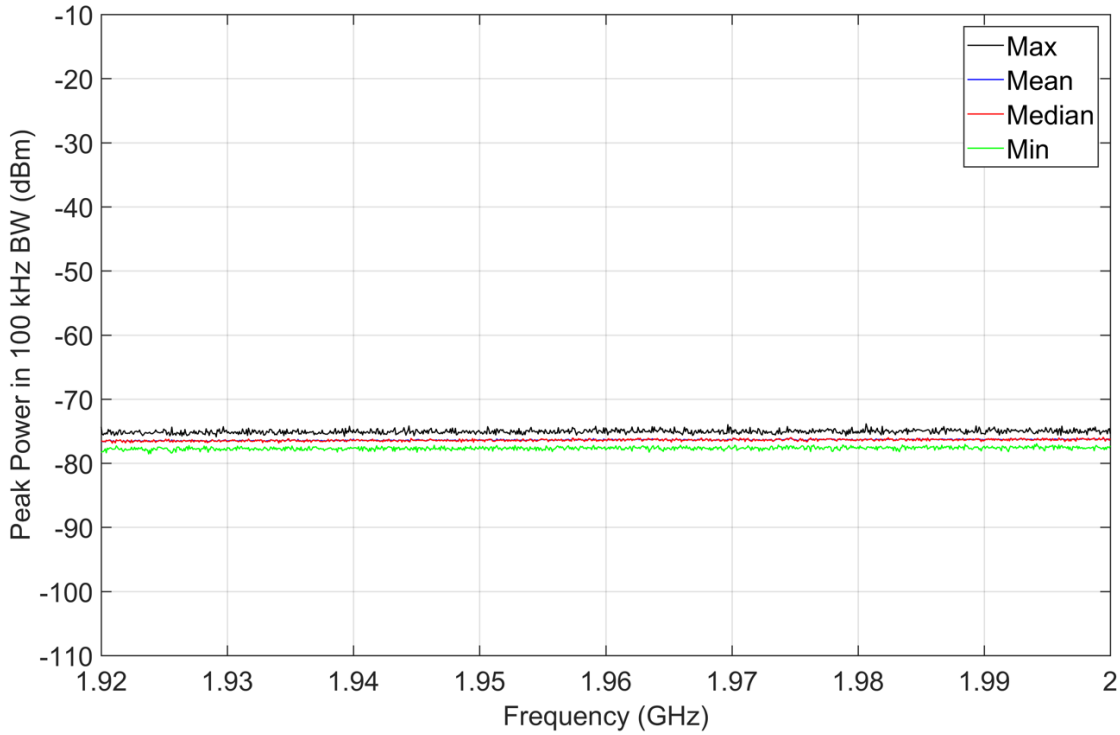


Figure 30. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

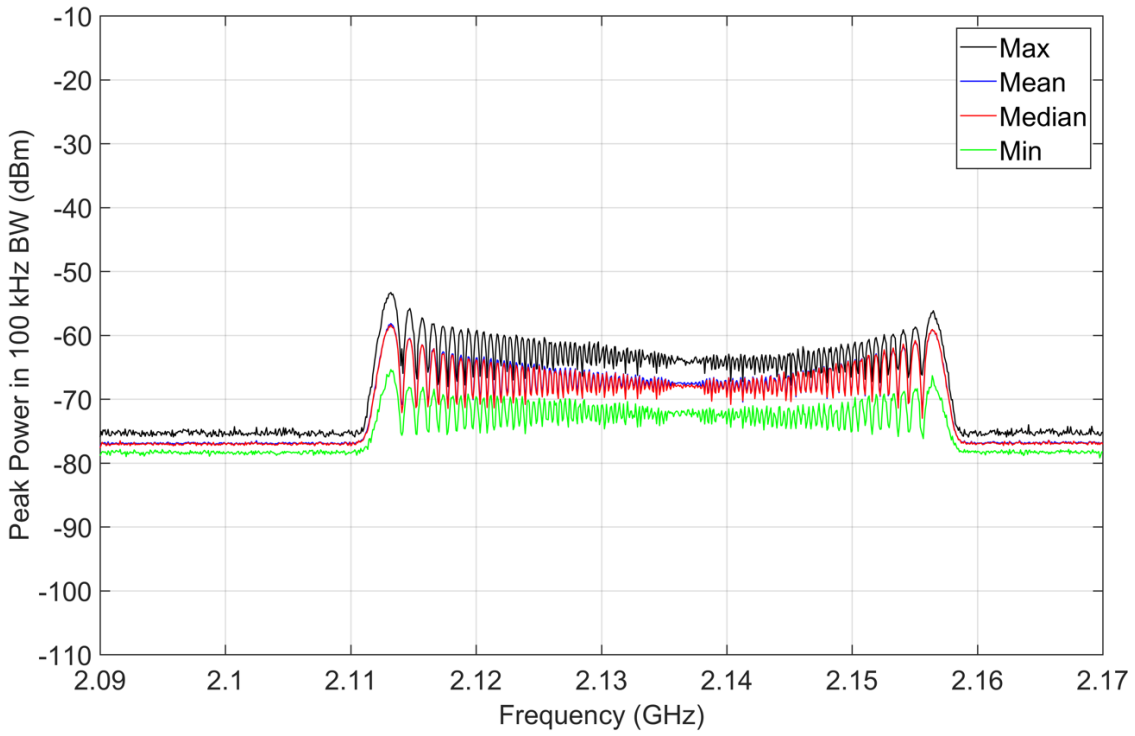


Figure 31. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

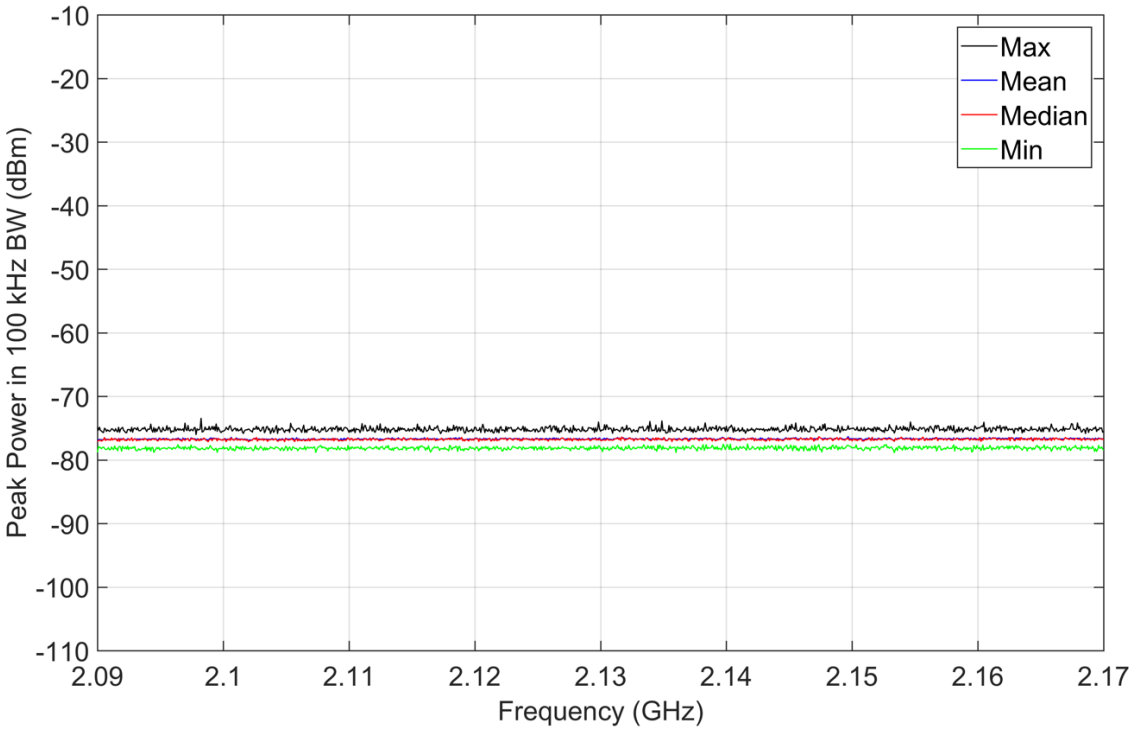


Figure 32. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

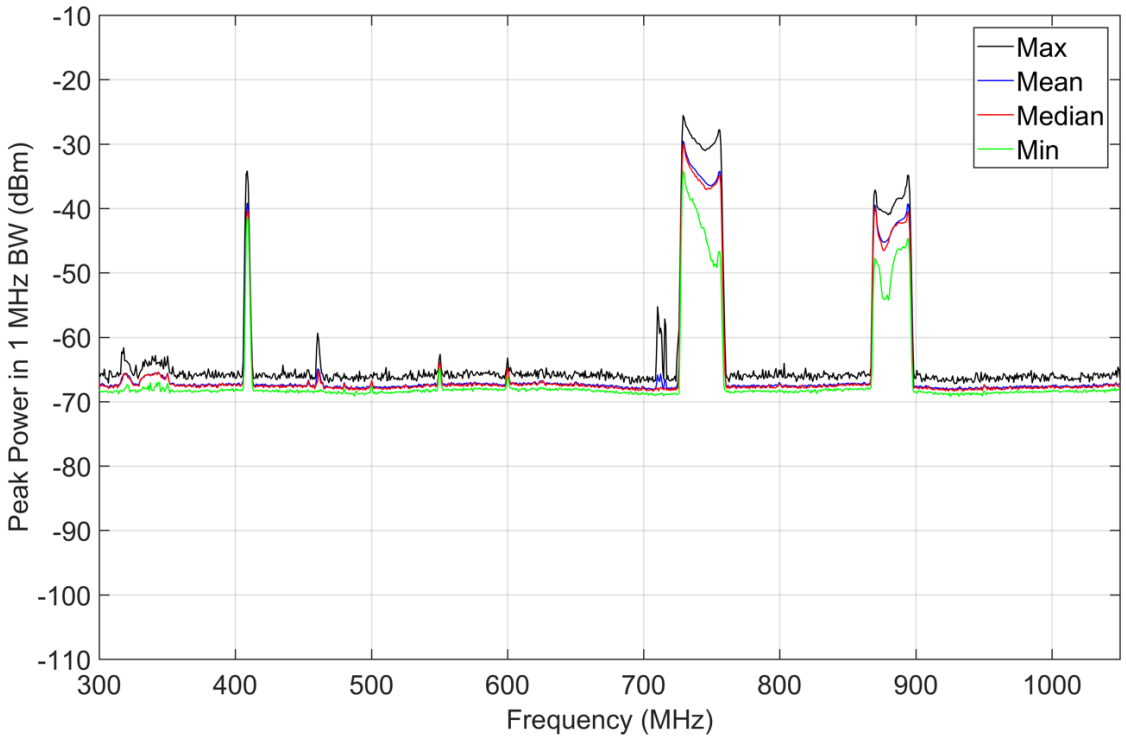


Figure 33. M4 statistics, peak detection, jammer on, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

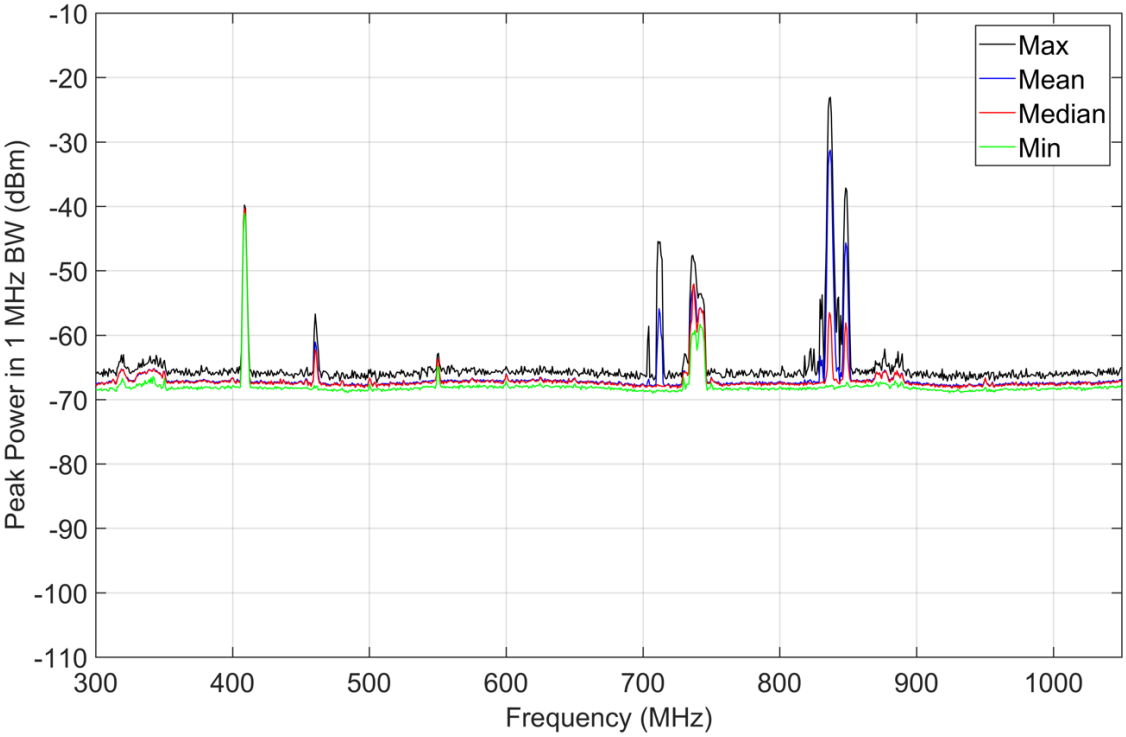


Figure 34. M4 statistics, peak detection, jammer off, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

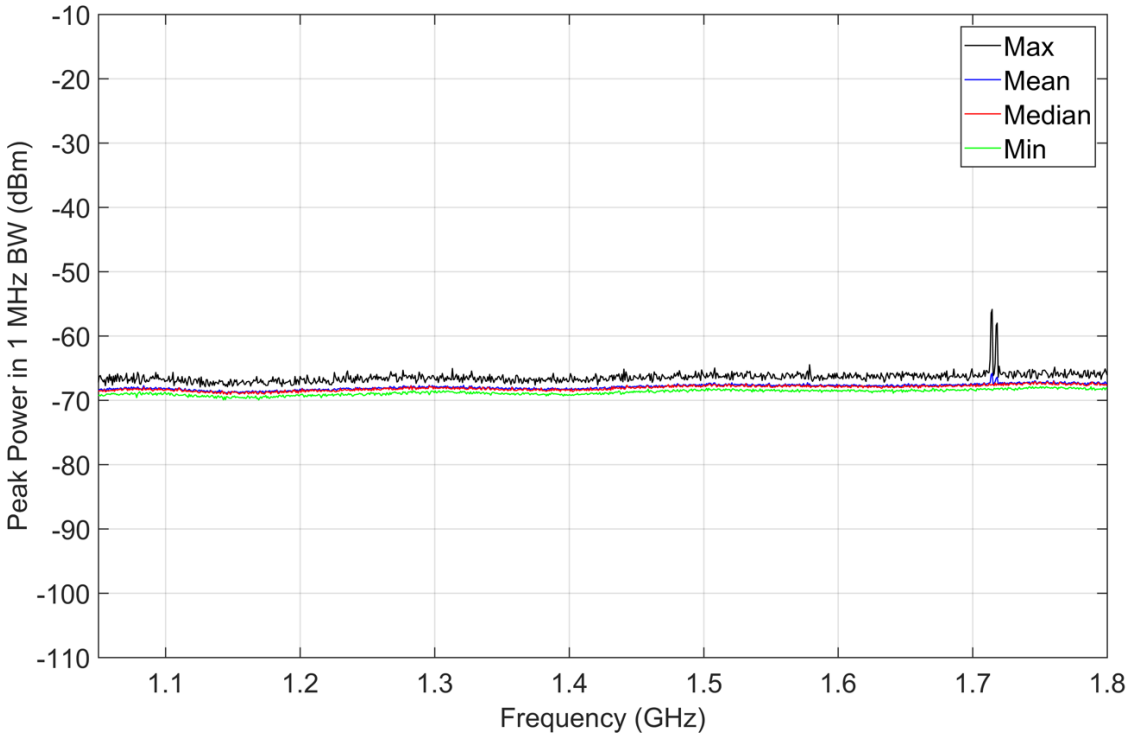


Figure 35. M4 statistics, peak detection, jammer on, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

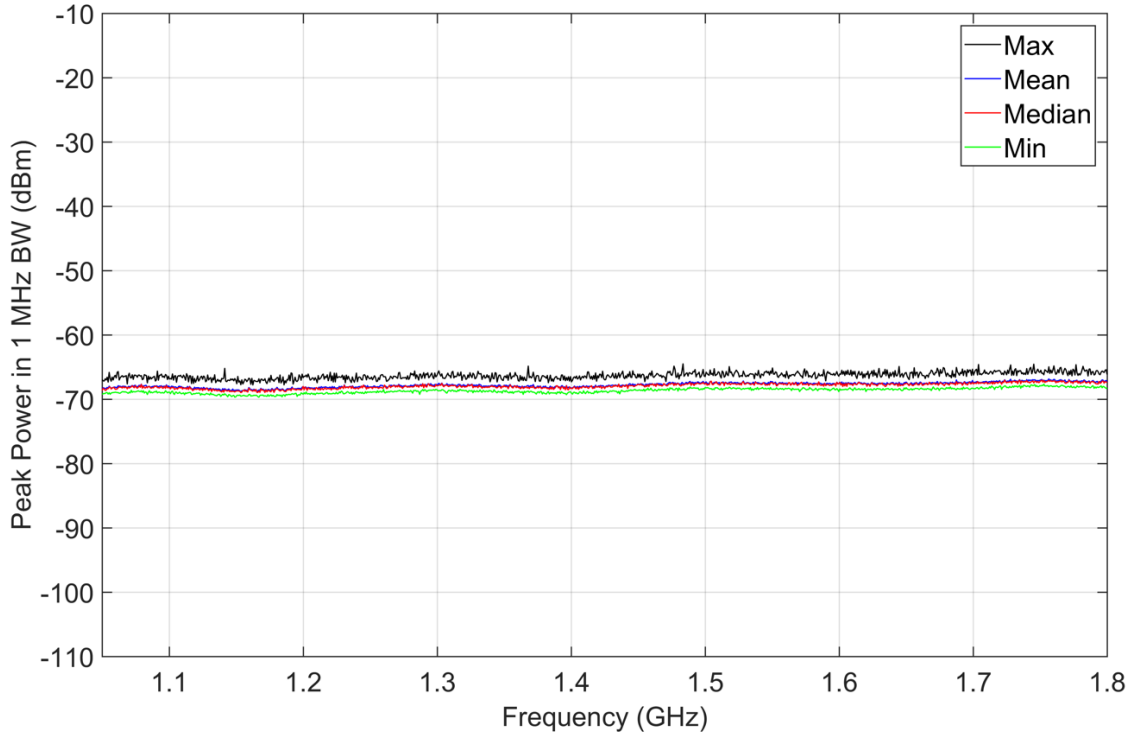


Figure 36. M4 statistics, peak detection, jammer off, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

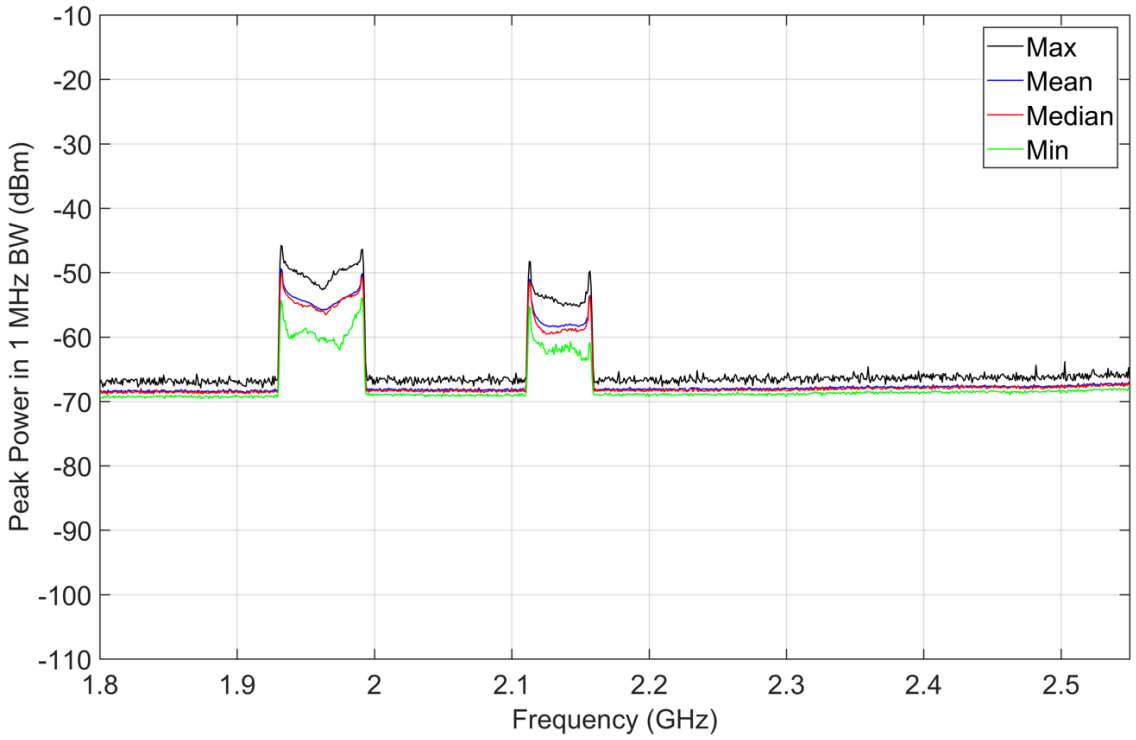


Figure 37. M4 statistics, peak detection, jammer on, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

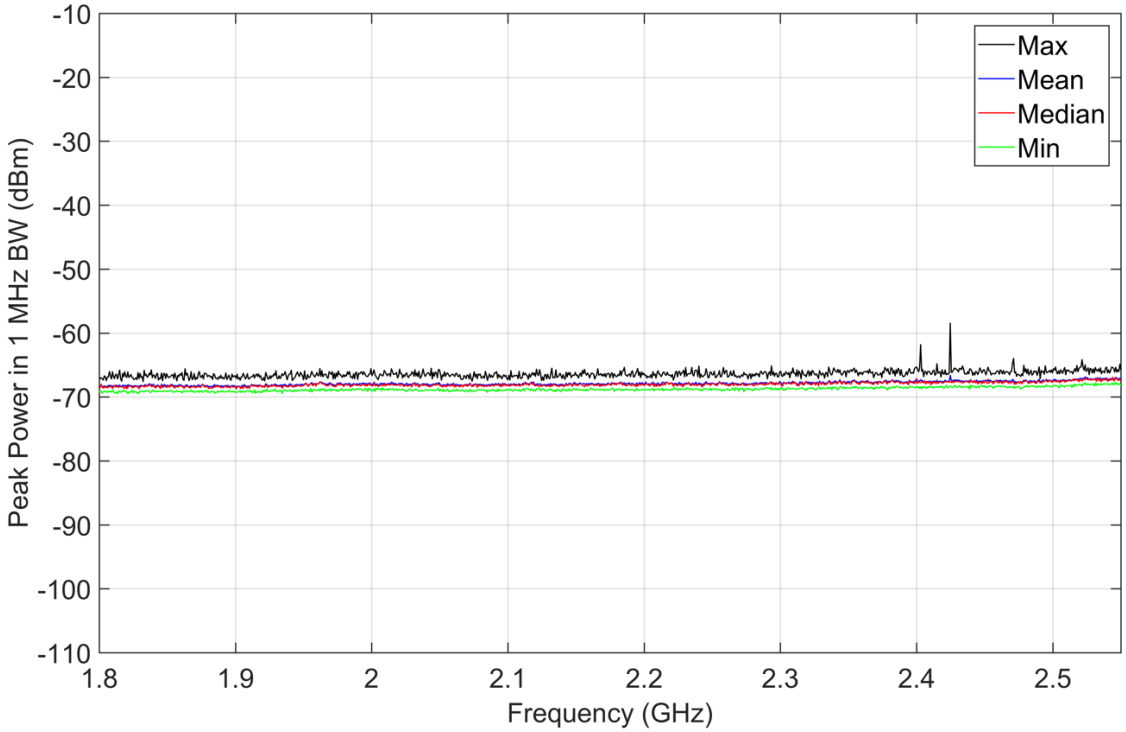


Figure 38. M4 statistics, peak detection, jammer off, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

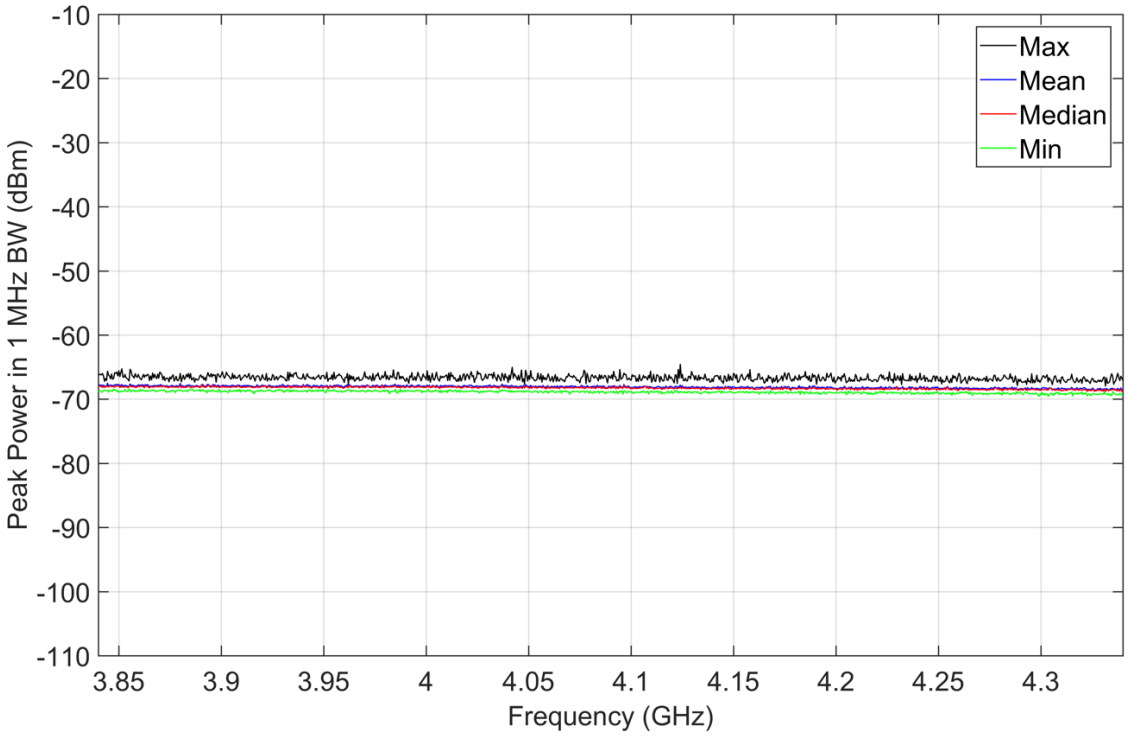


Figure 39. M4 statistics, peak detection, jammer on, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

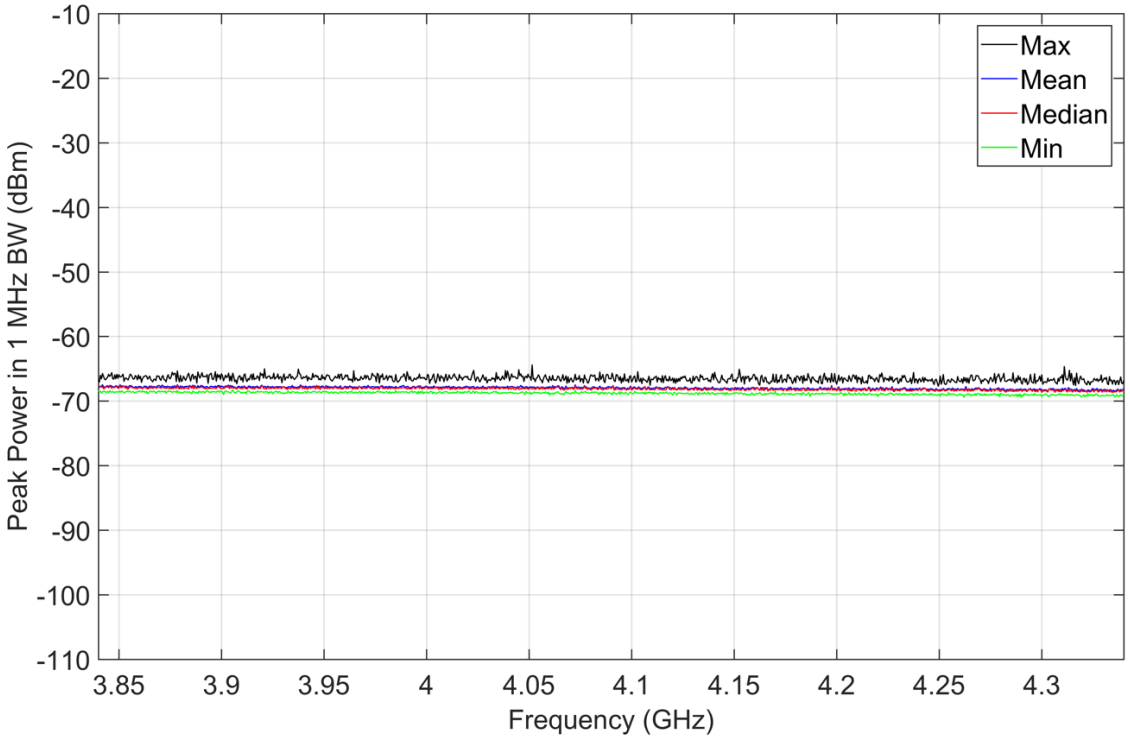


Figure 40. M4 statistics, peak detection, jammer off, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

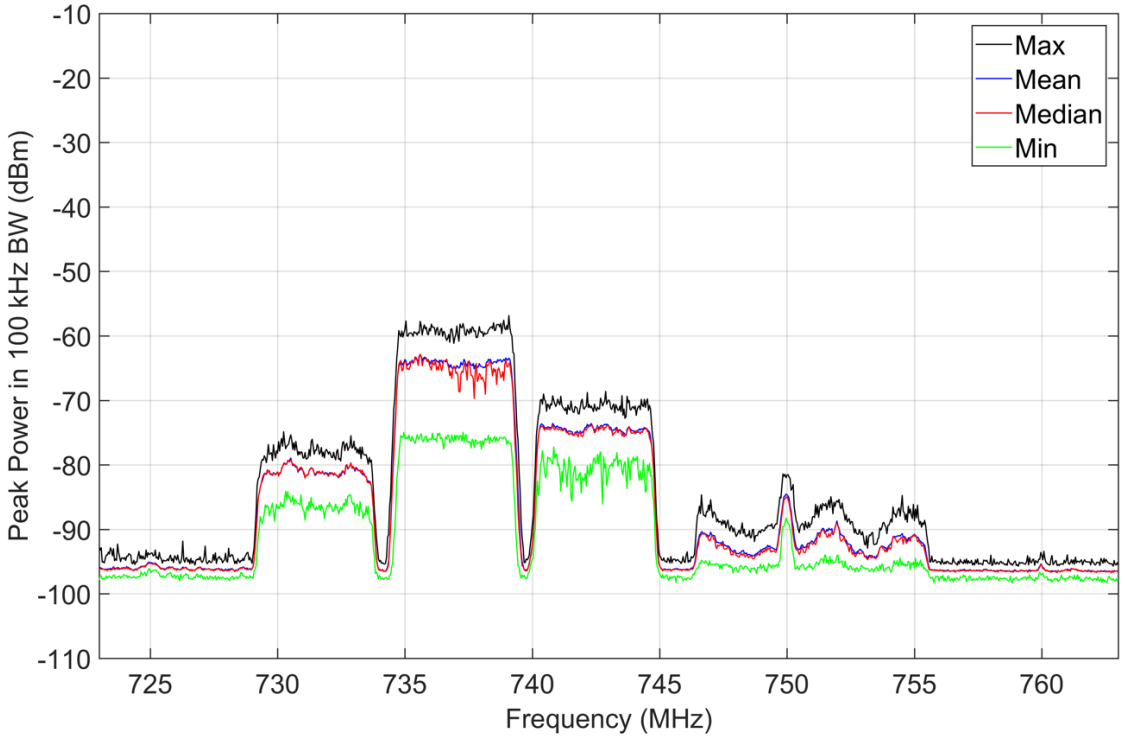


Figure 41. M4 statistics, peak detection, jammer off, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location I-1 inside targeted prison cell.

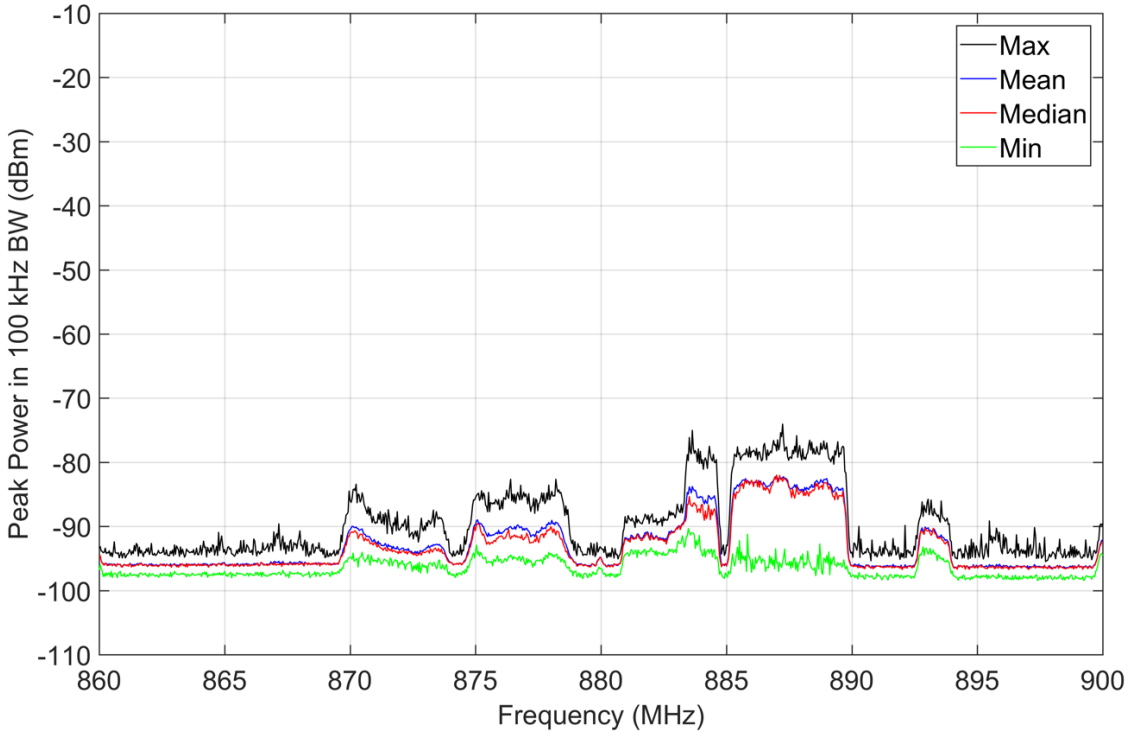


Figure 42. M4 statistics, peak detection, jammer off, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location I-1 inside targeted prison cell.

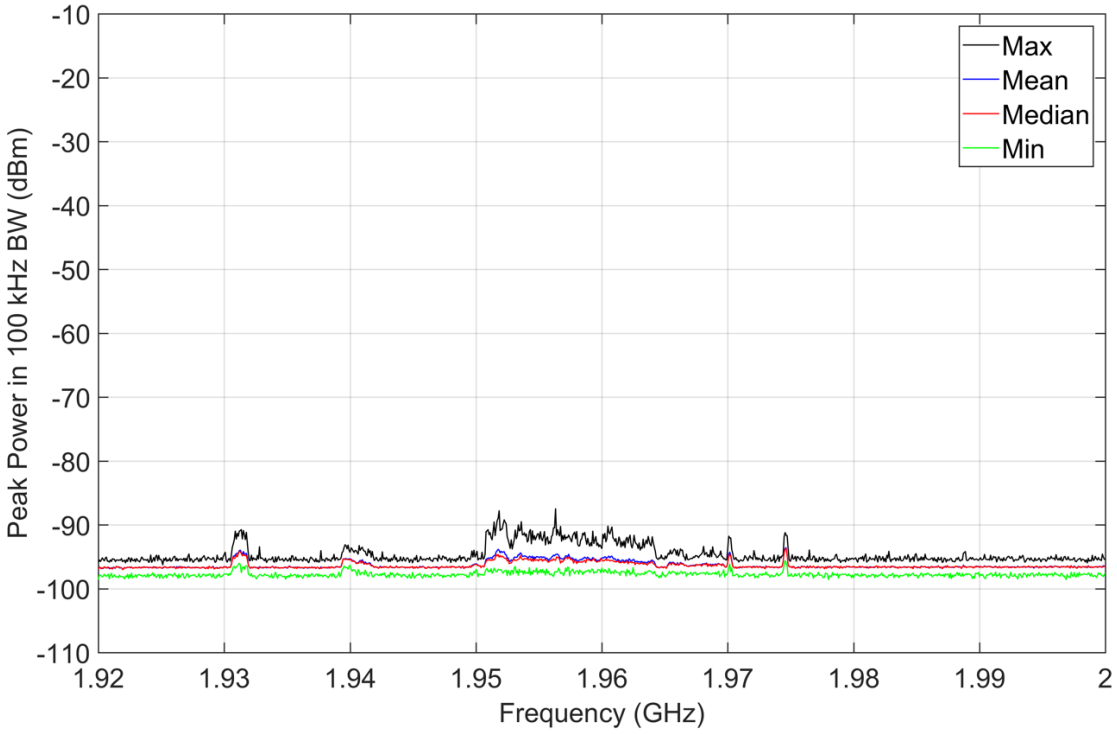


Figure 43. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location I-1 inside targeted prison cell.

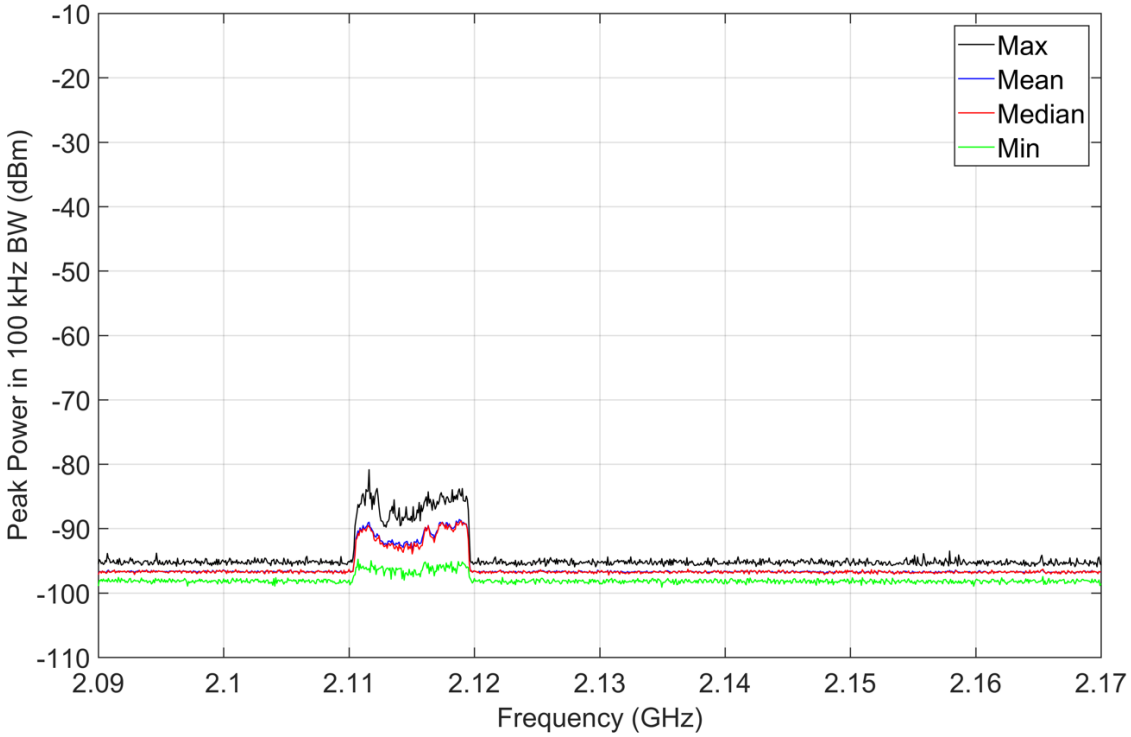


Figure 44. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location I-1 inside targeted prison cell.

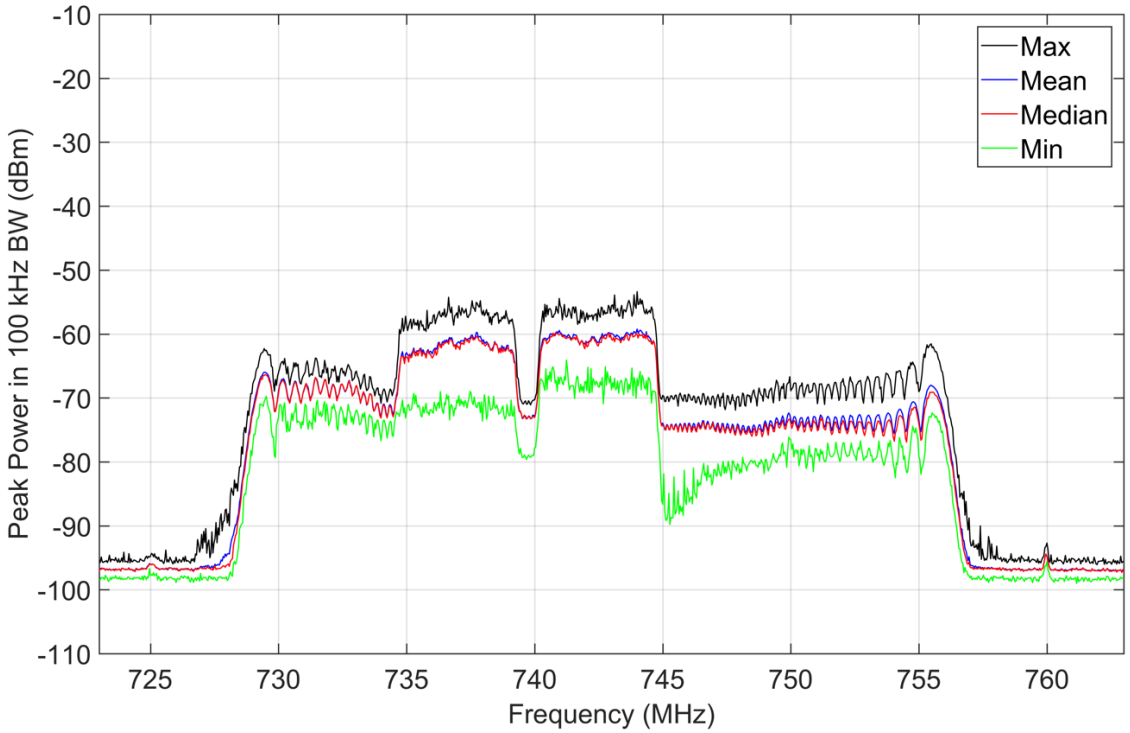


Figure 45. M4 statistics, peak detection, jammer on, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

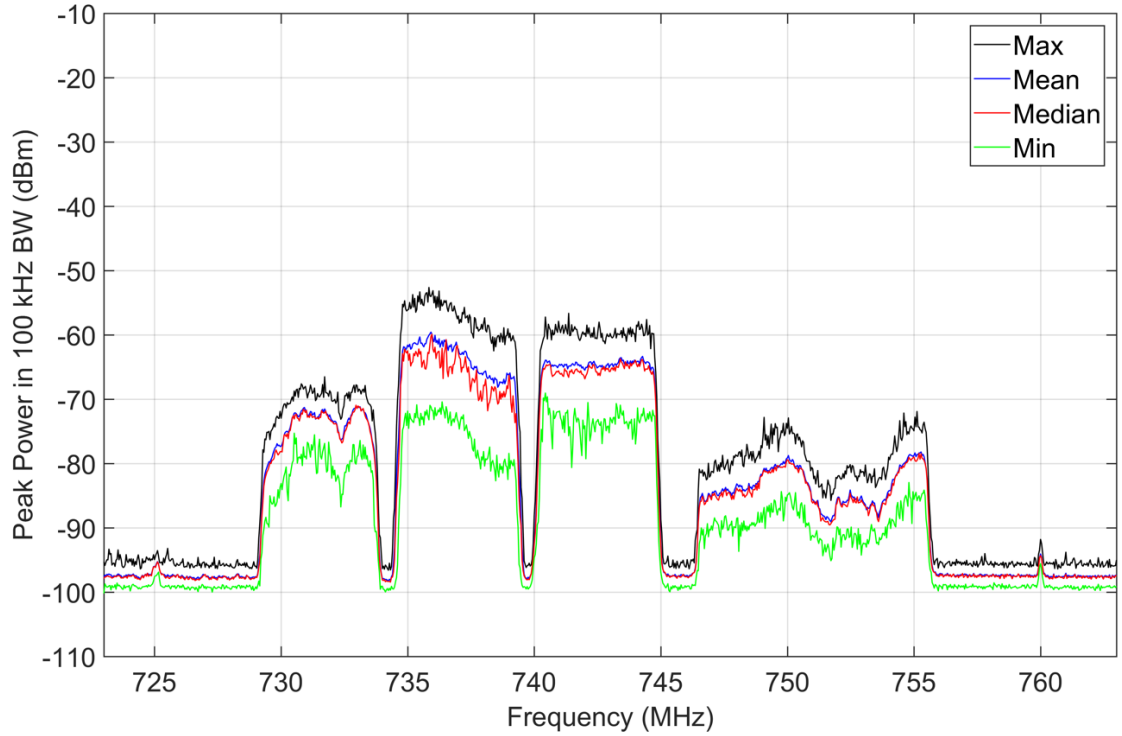


Figure 46. M4 statistics, peak detection, jammer off, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

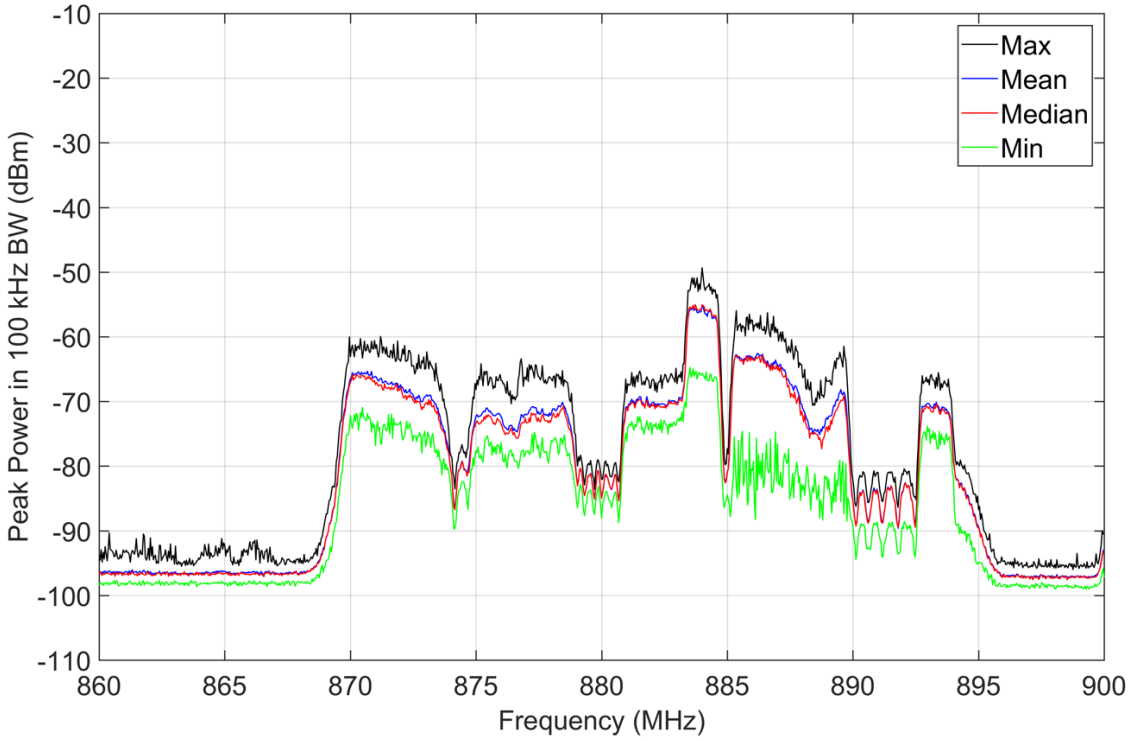


Figure 47. M4 statistics, peak detection, jammer on, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

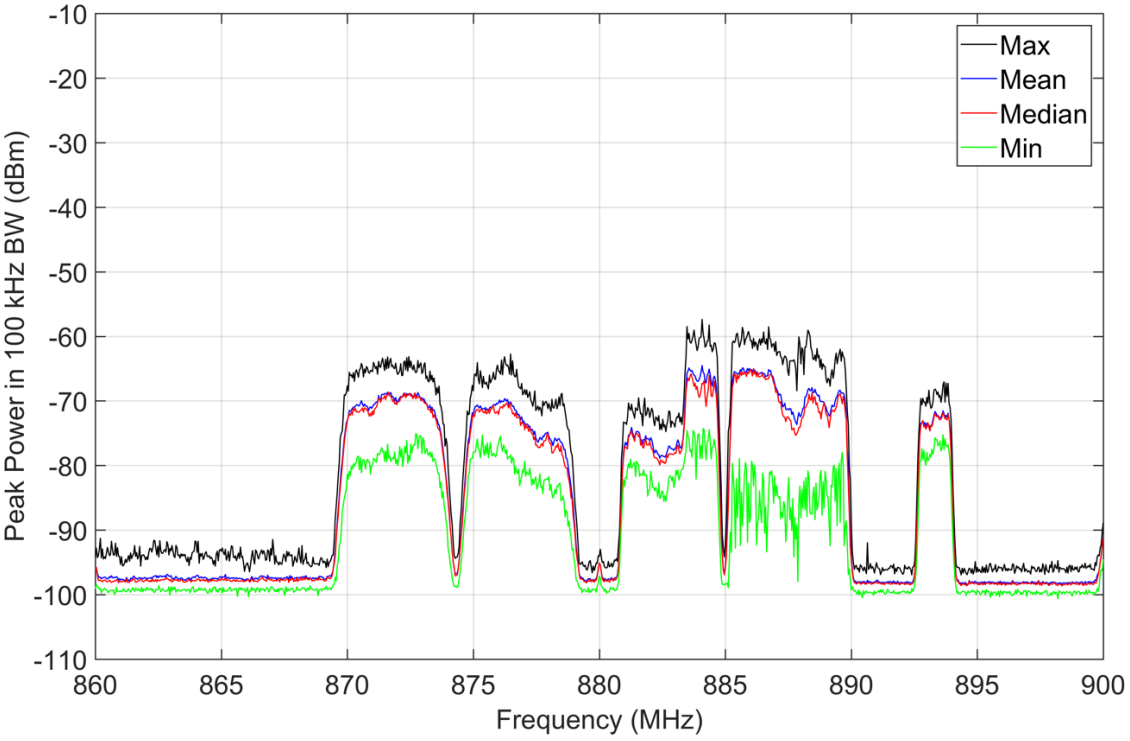


Figure 48. M4 statistics, peak detection, jammer off, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

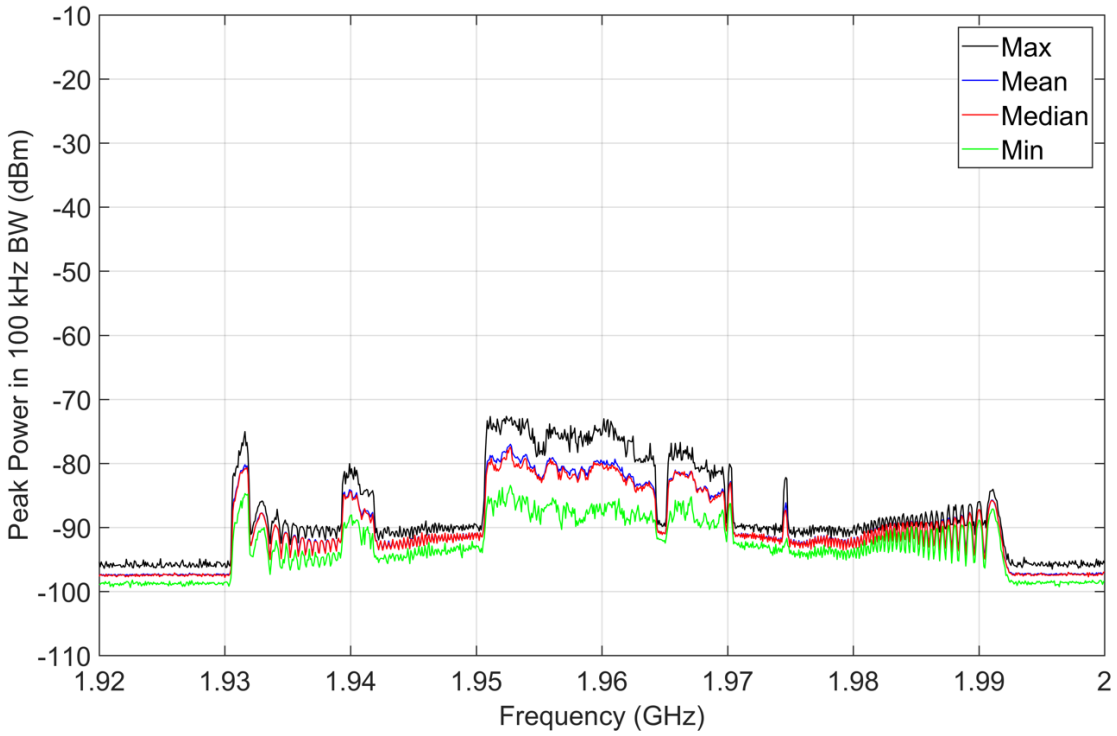


Figure 49. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on location O-1 outside targeted prison cell.

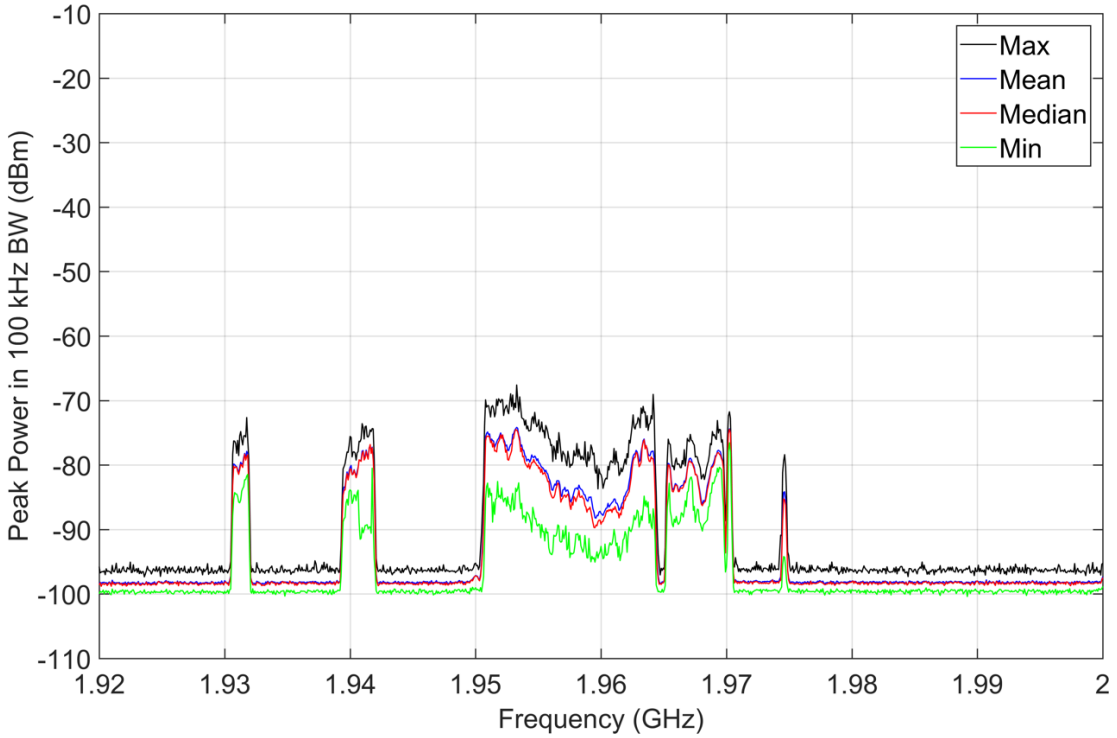


Figure 50. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

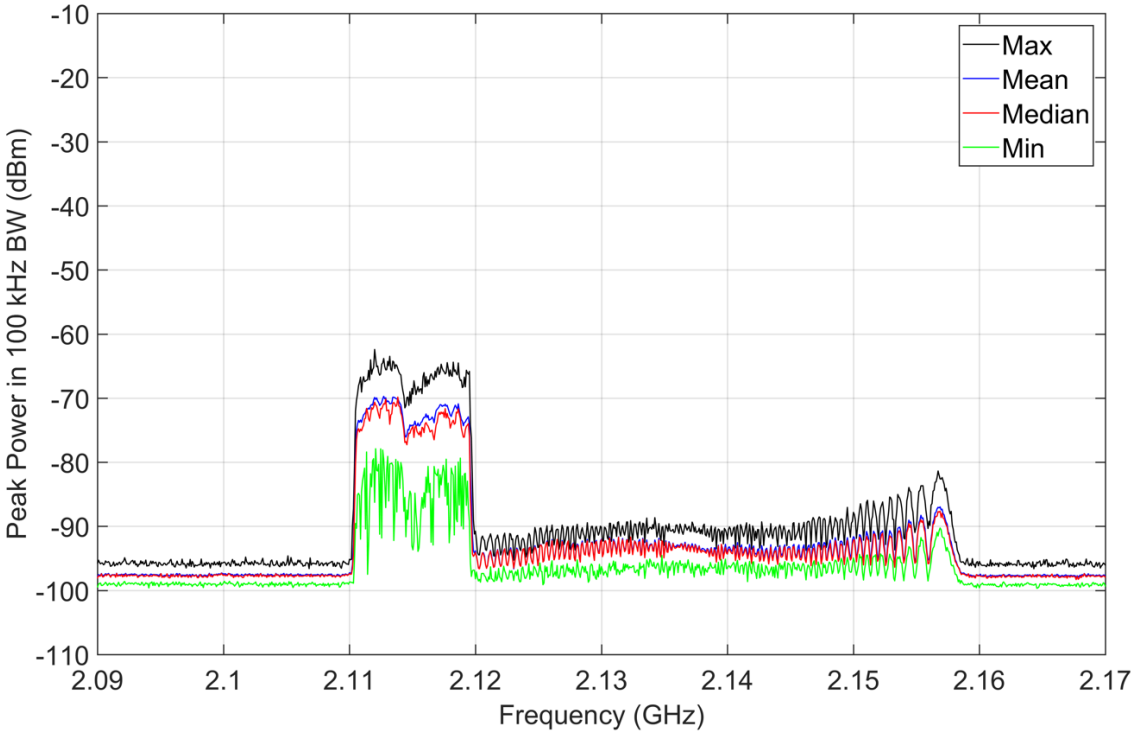


Figure 51. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

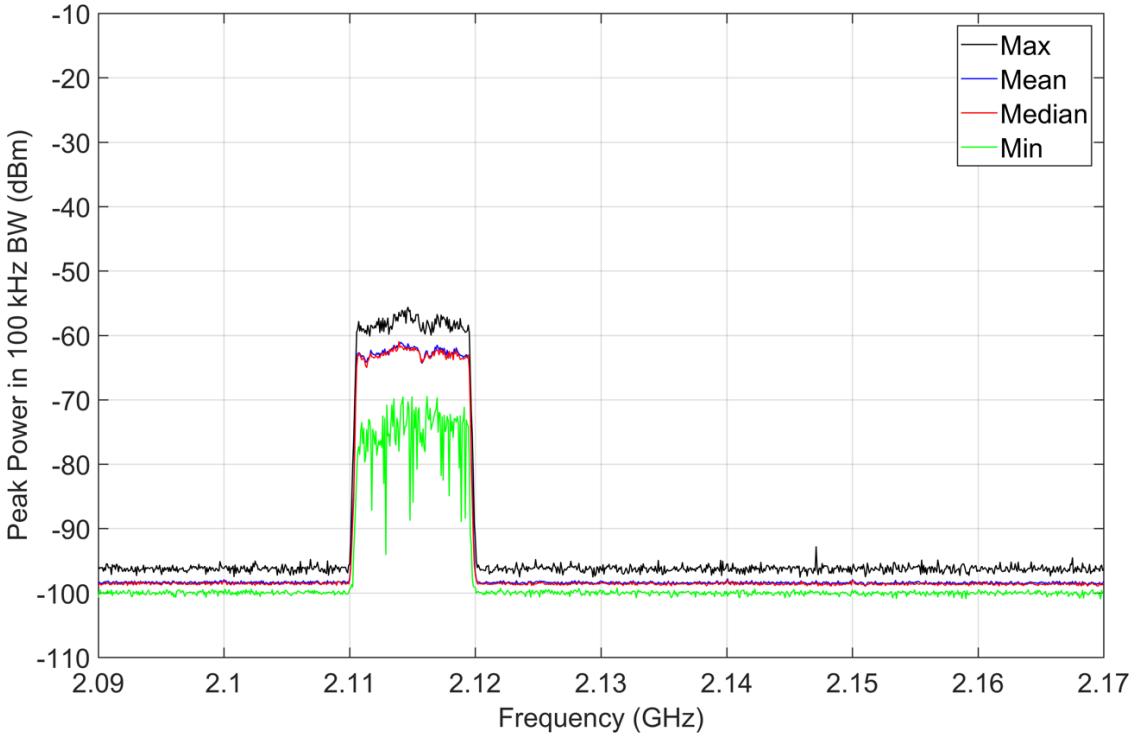


Figure 52. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

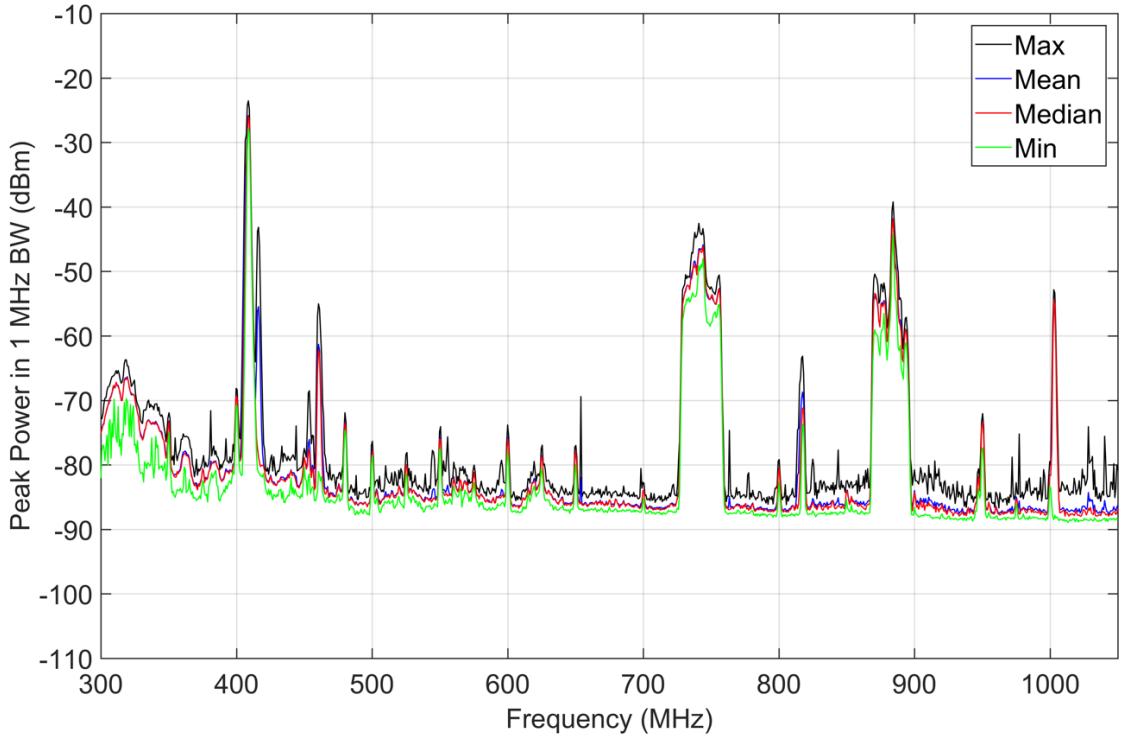


Figure 53. M4 statistics, peak detection, jammer on, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

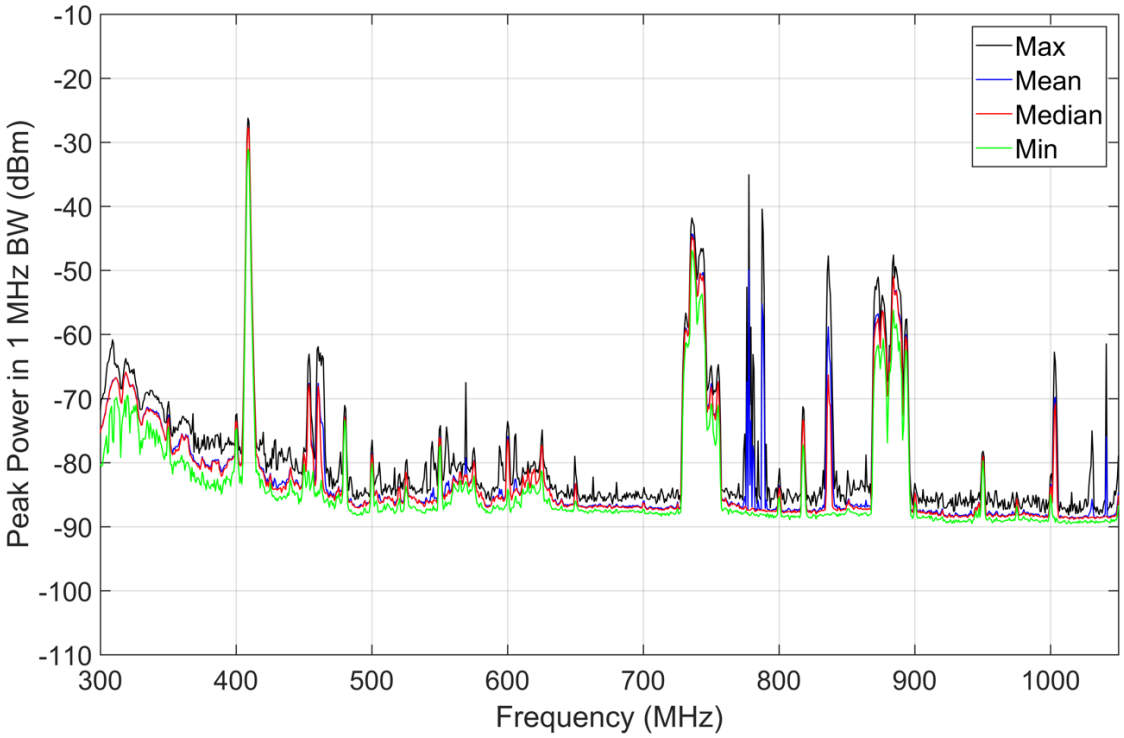


Figure 54. M4 statistics, peak detection, jammer off, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

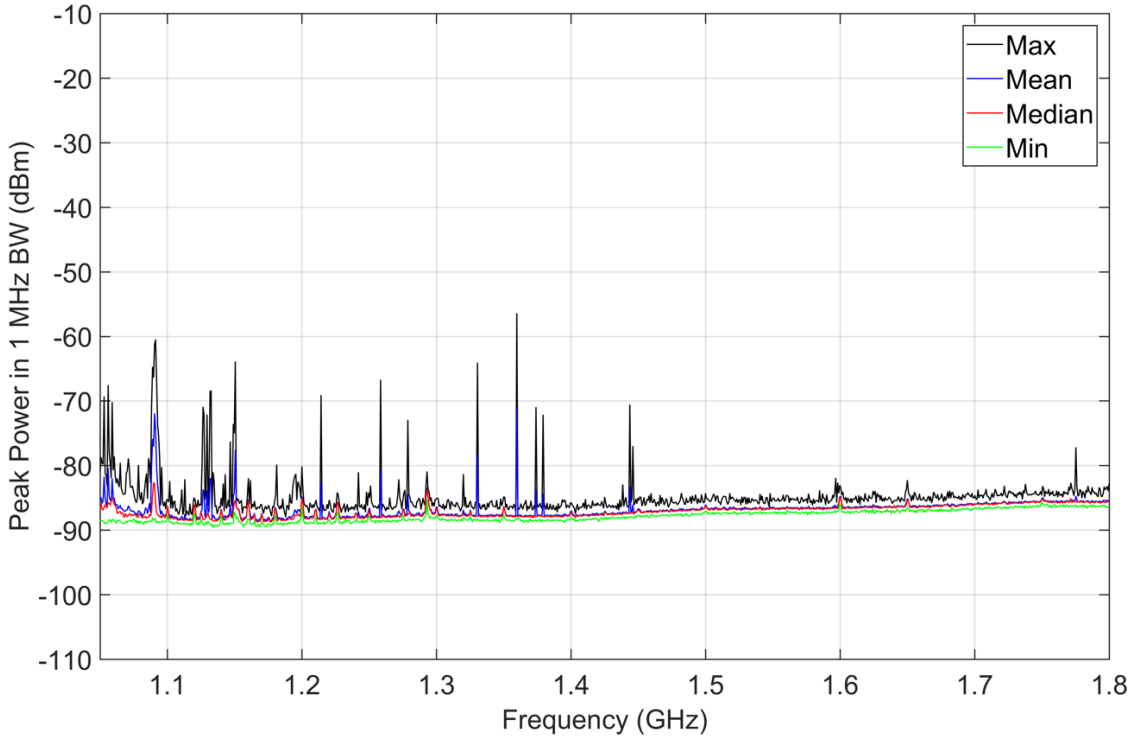


Figure 55. M4 statistics, peak detection, jammer on, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

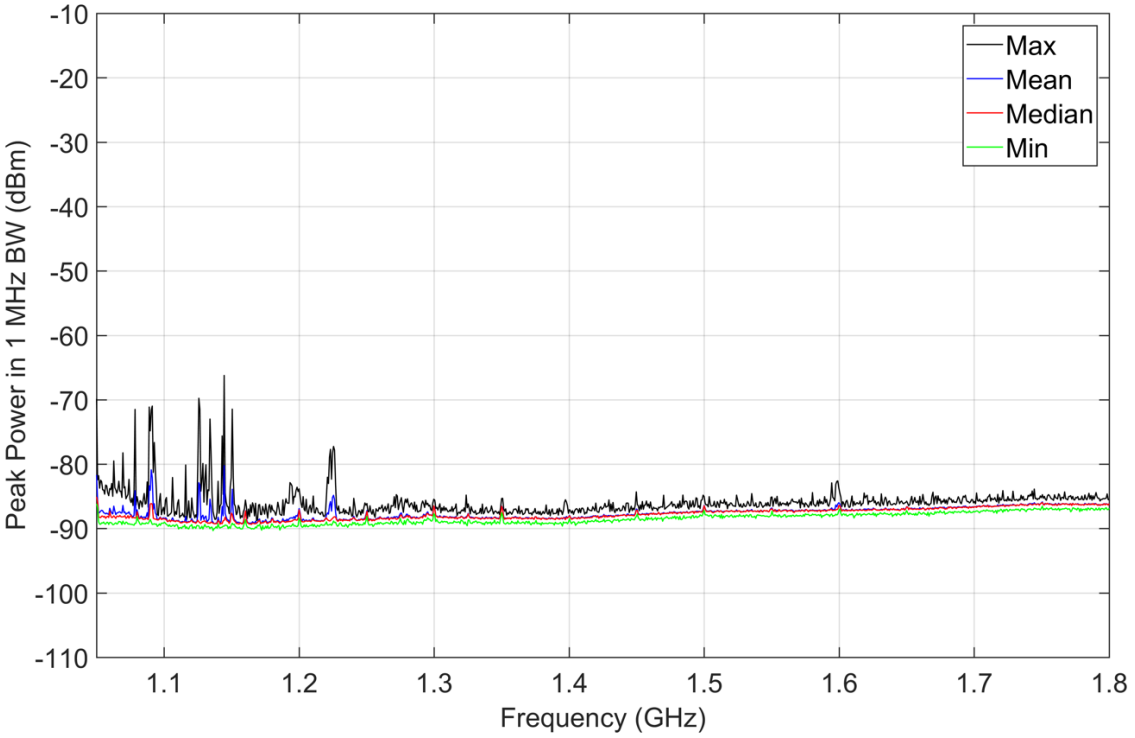


Figure 56. M4 statistics, peak detection, jammer off, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

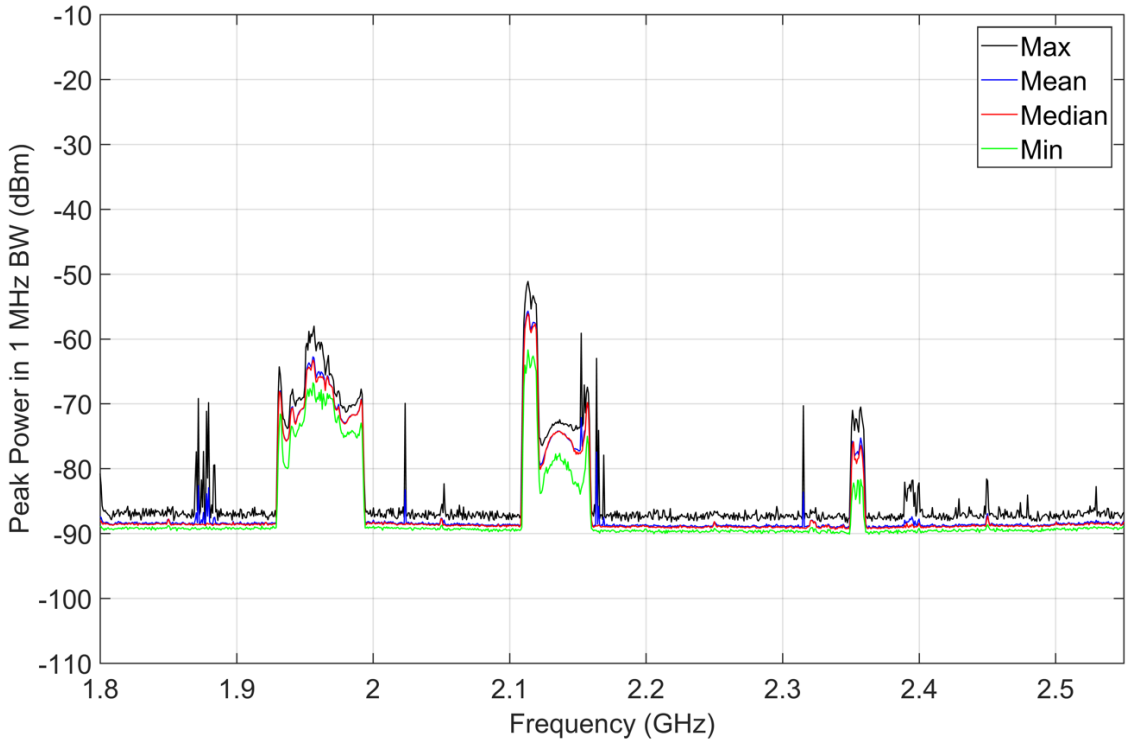


Figure 57. M4 statistics, peak detection, jammer on, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

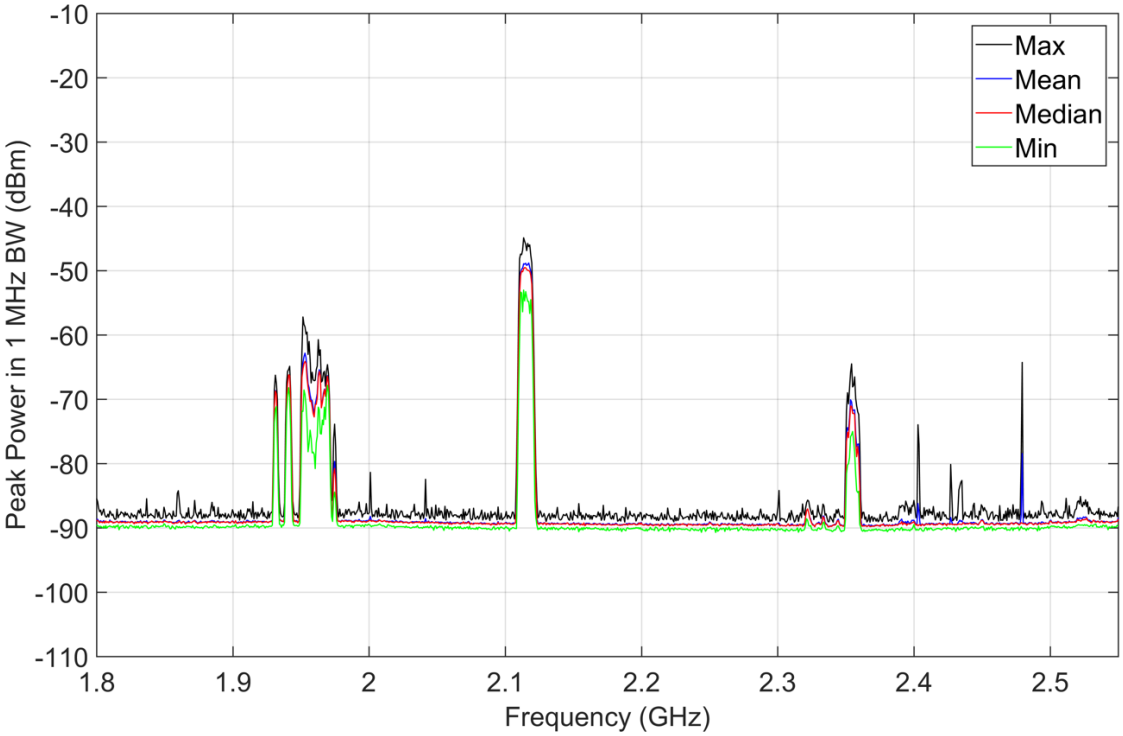


Figure 58. M4 statistics, peak detection, jammer off, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

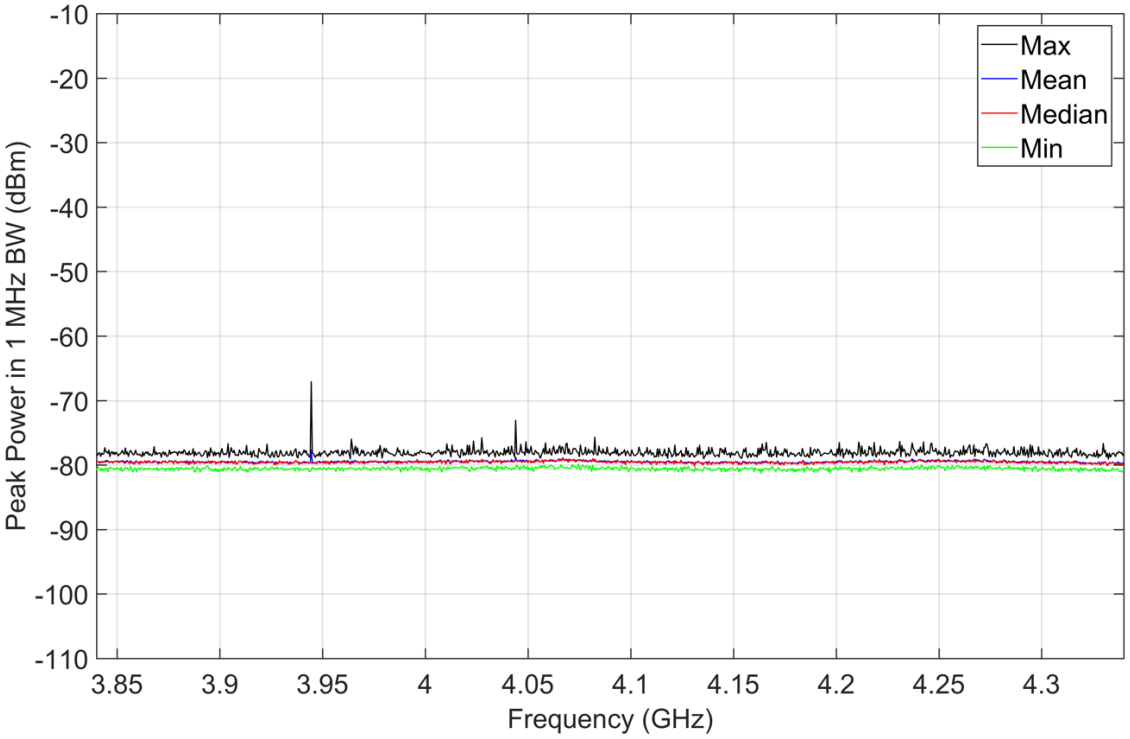


Figure 59. M4 statistics, peak detection, jammer on, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

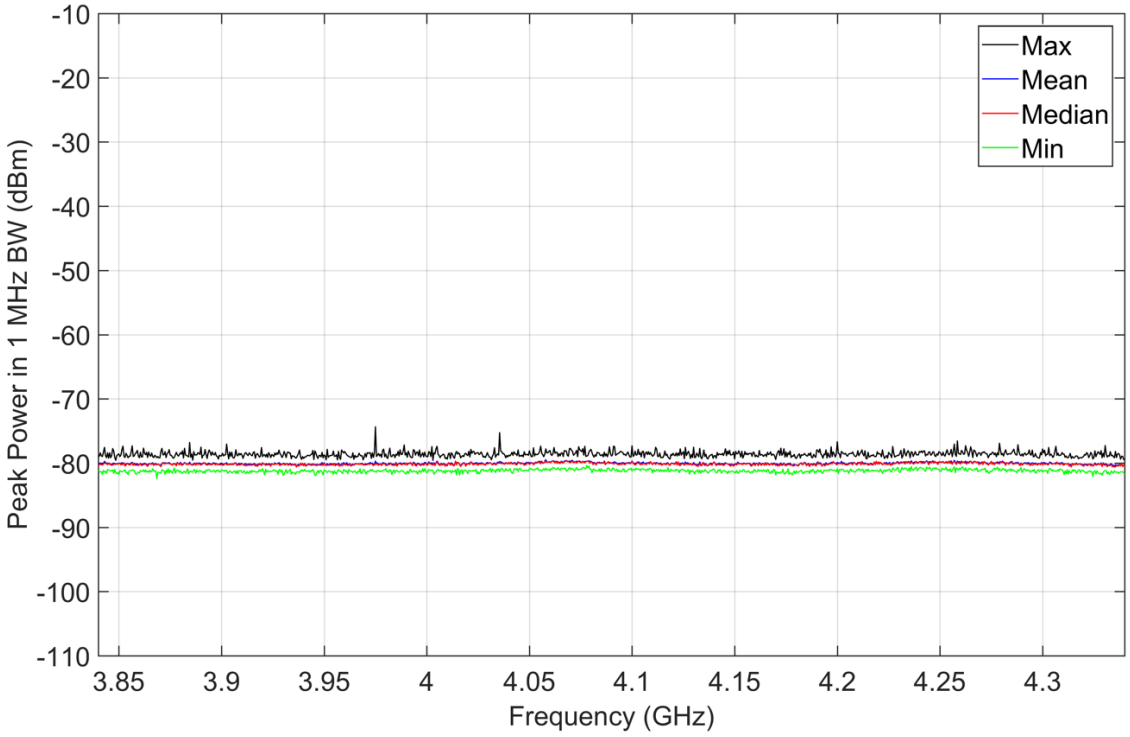


Figure 60. M4 statistics, peak detection, jammer off, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

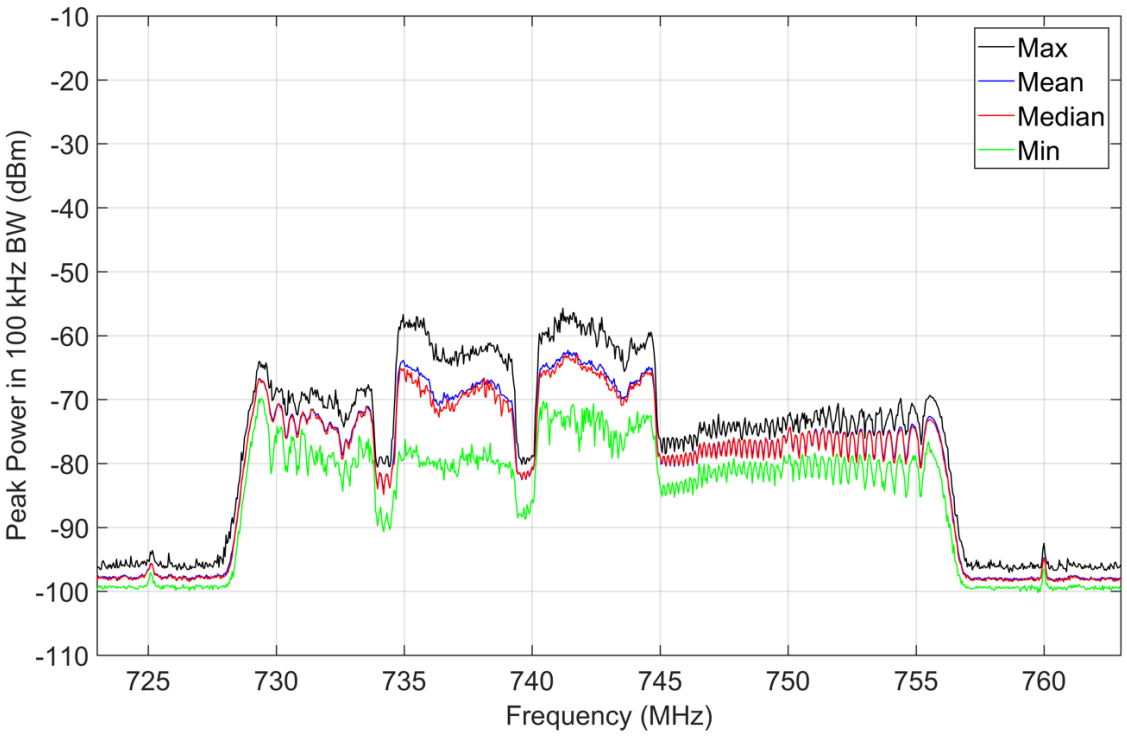


Figure 61. M4 statistics, peak detection, jammer on, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

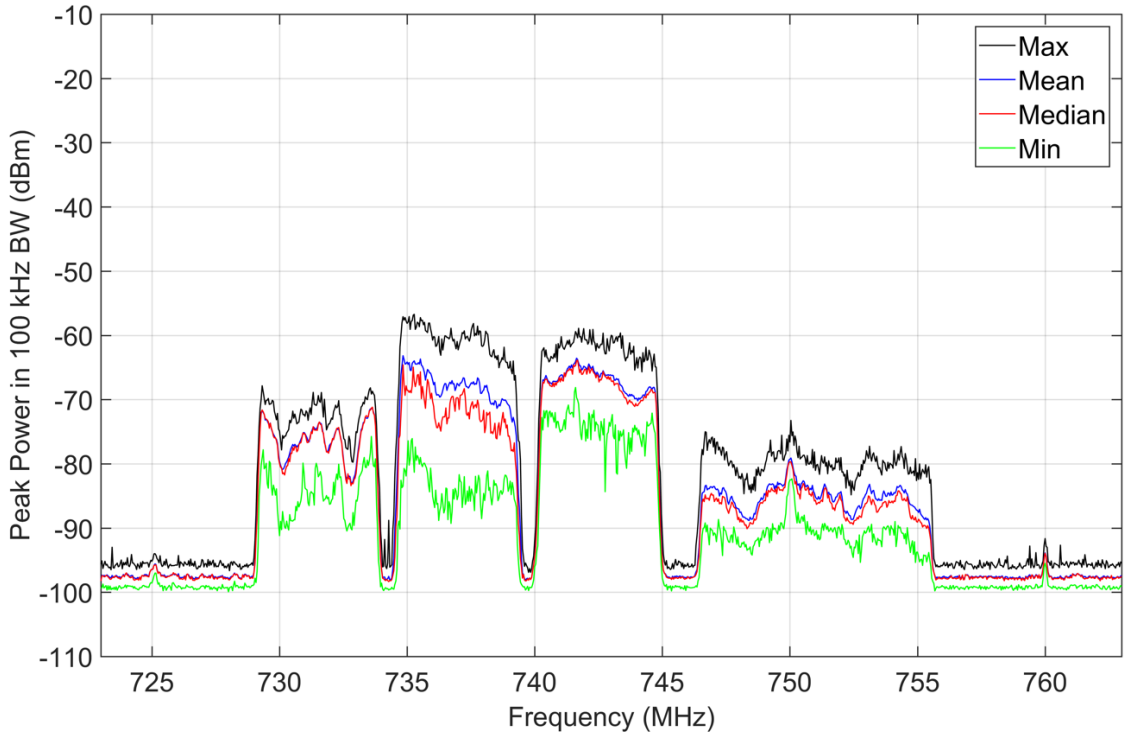


Figure 62. M4 statistics, peak detection, jammer off, 723–763 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

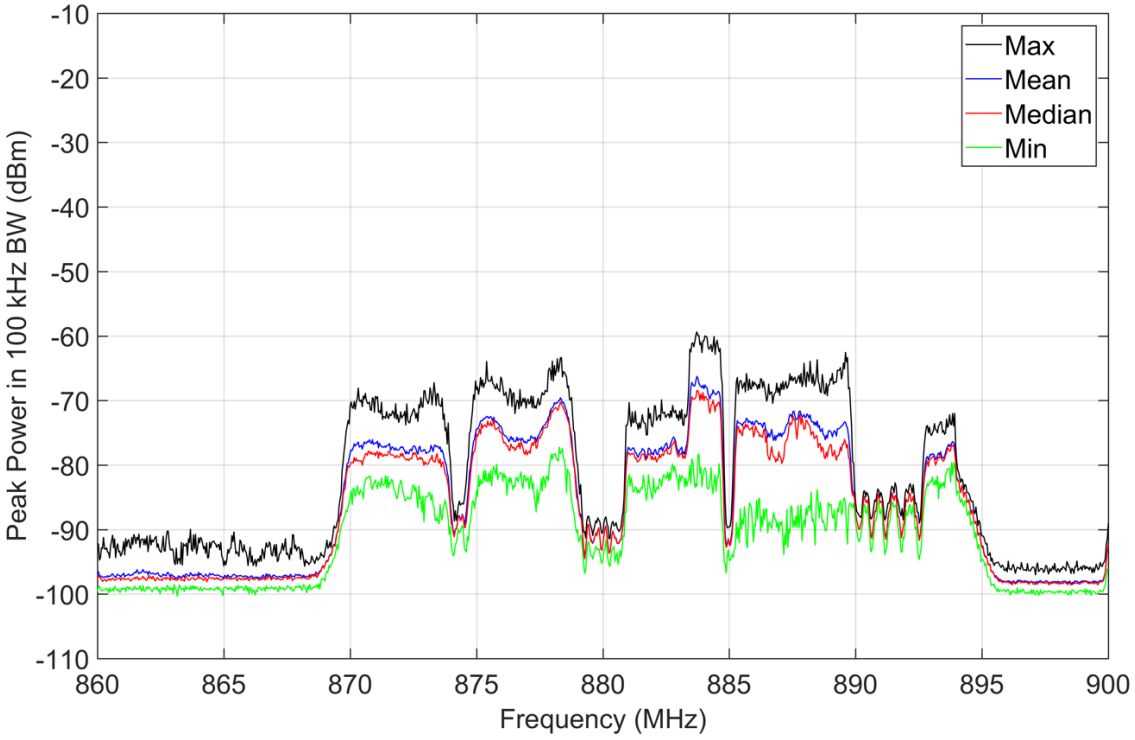


Figure 63. M4 statistics, peak detection, jammer on, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

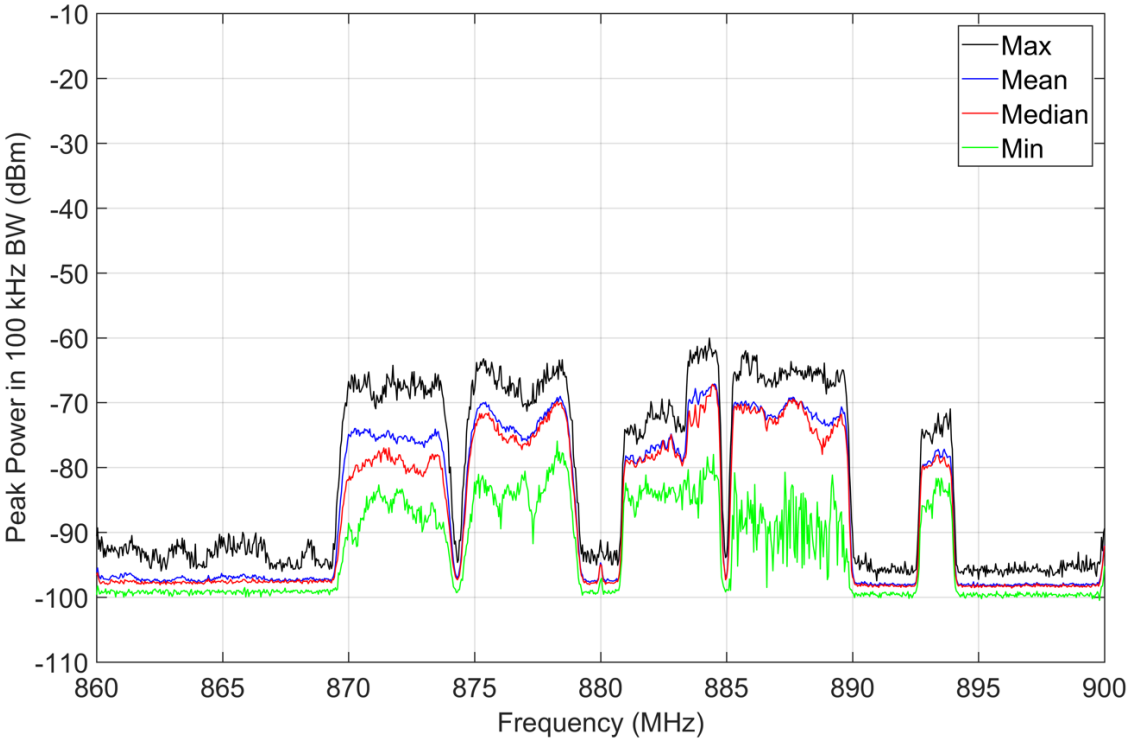


Figure 64. M4 statistics, peak detection, jammer off, 860–900 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside inside targeted prison cell.

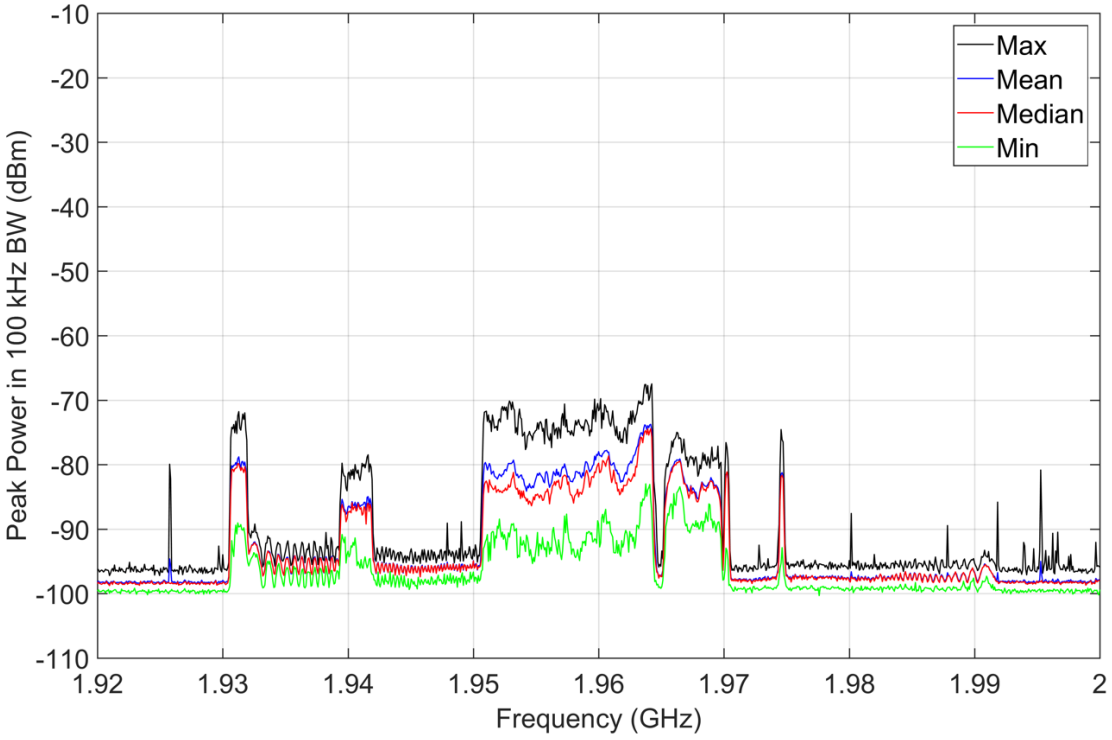


Figure 65. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

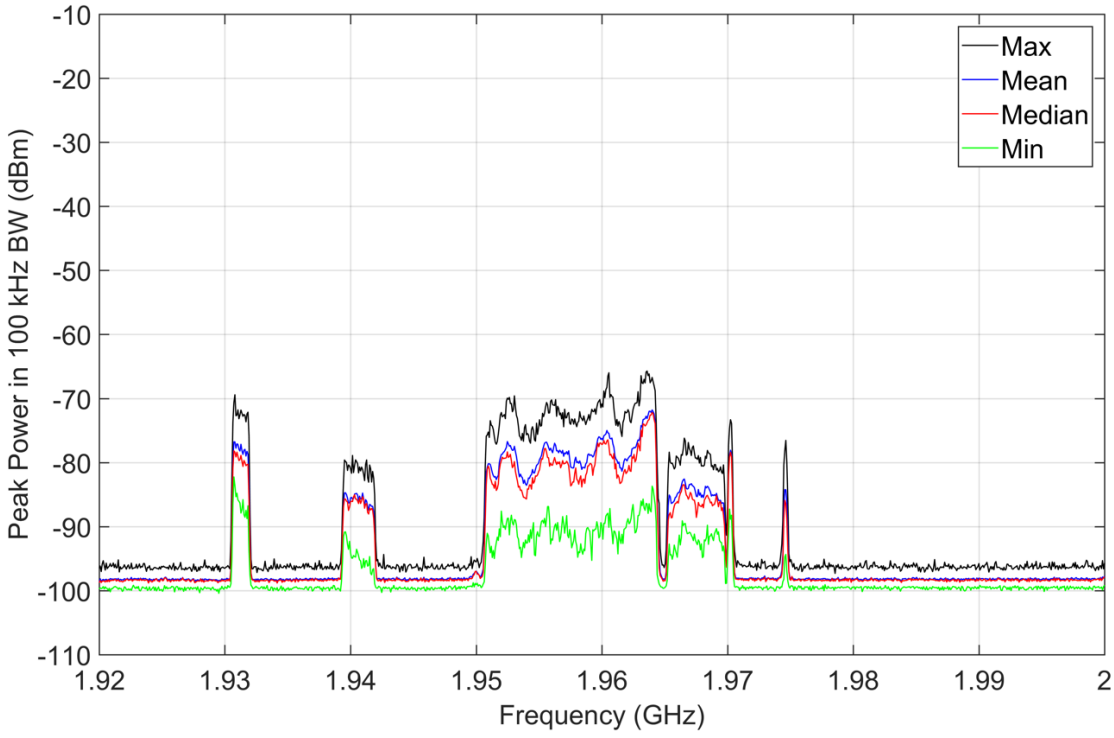


Figure 66. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

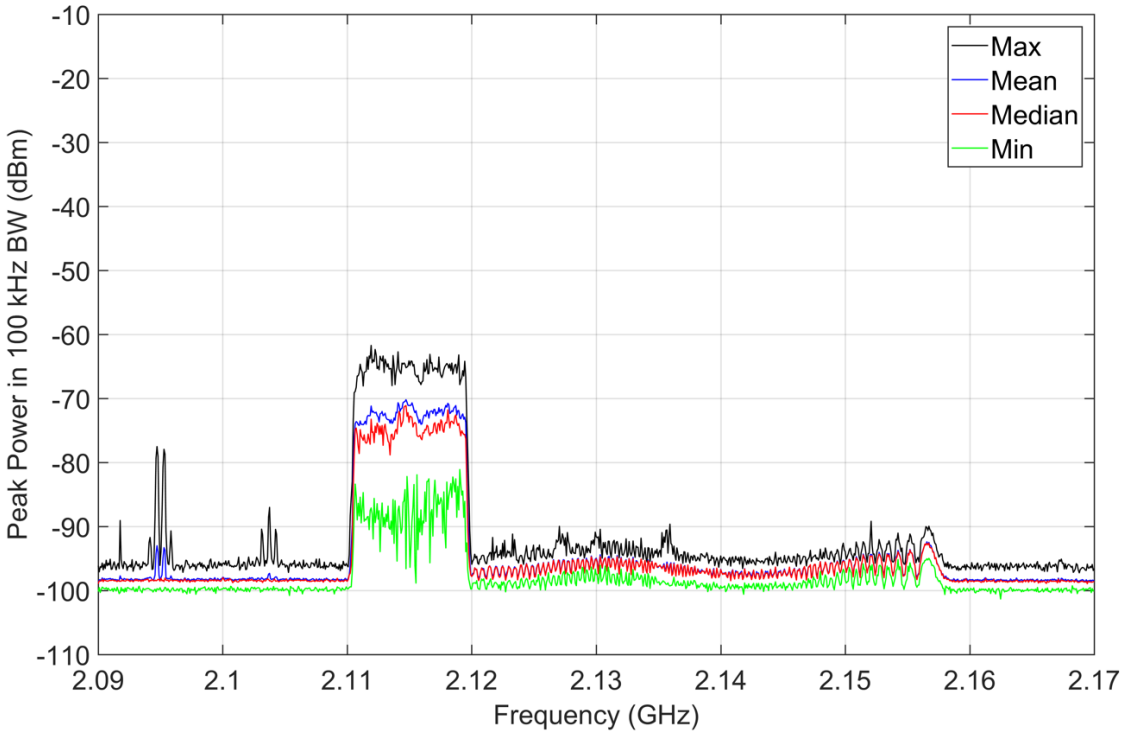


Figure 67. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

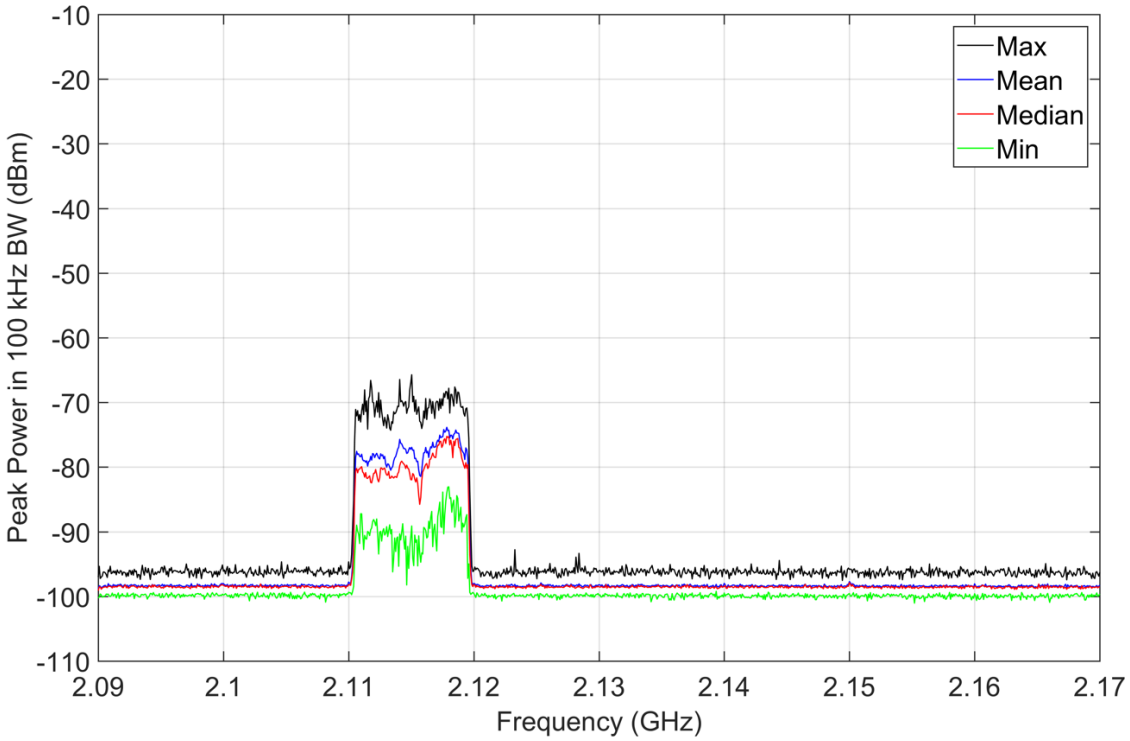


Figure 68. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

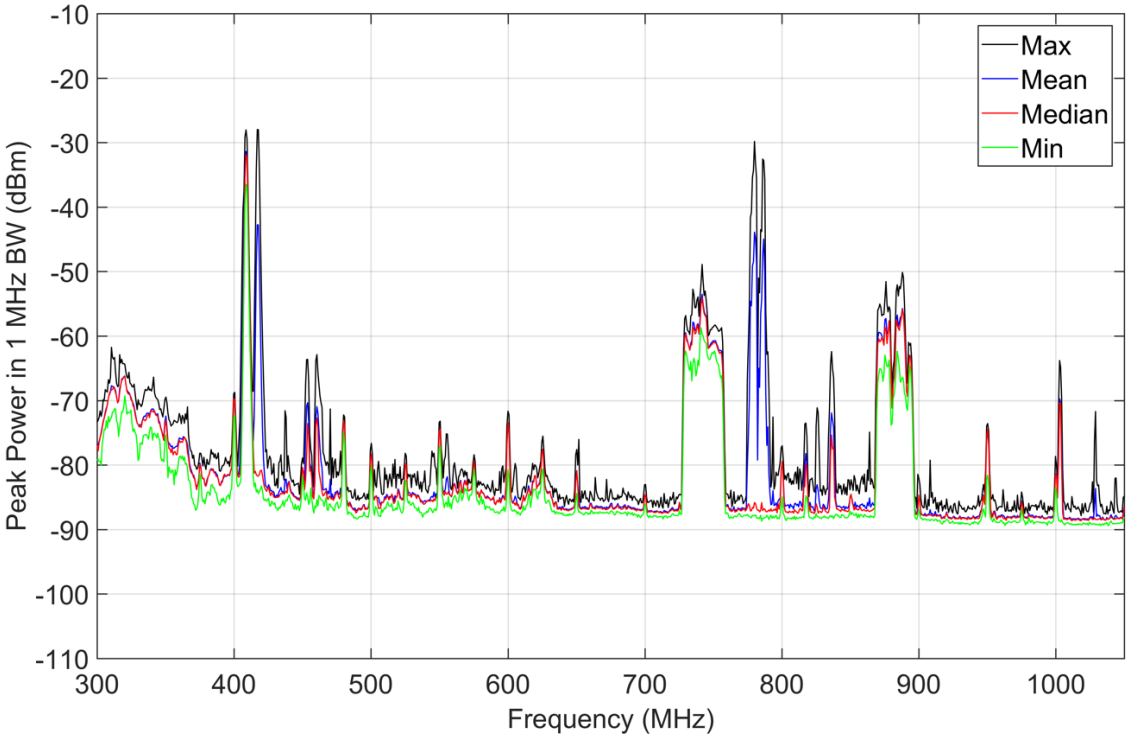


Figure 69. M4 statistics, peak detection, jammer on, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

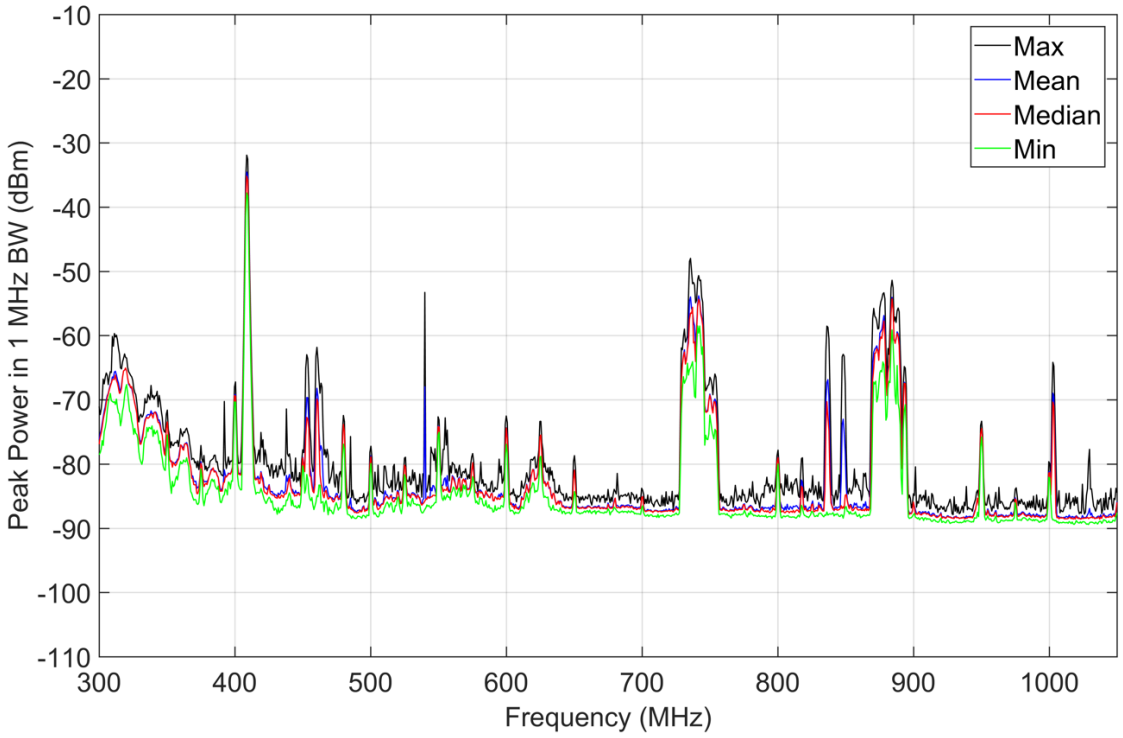


Figure 70. M4 statistics, peak detection, jammer off, 300–1050 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

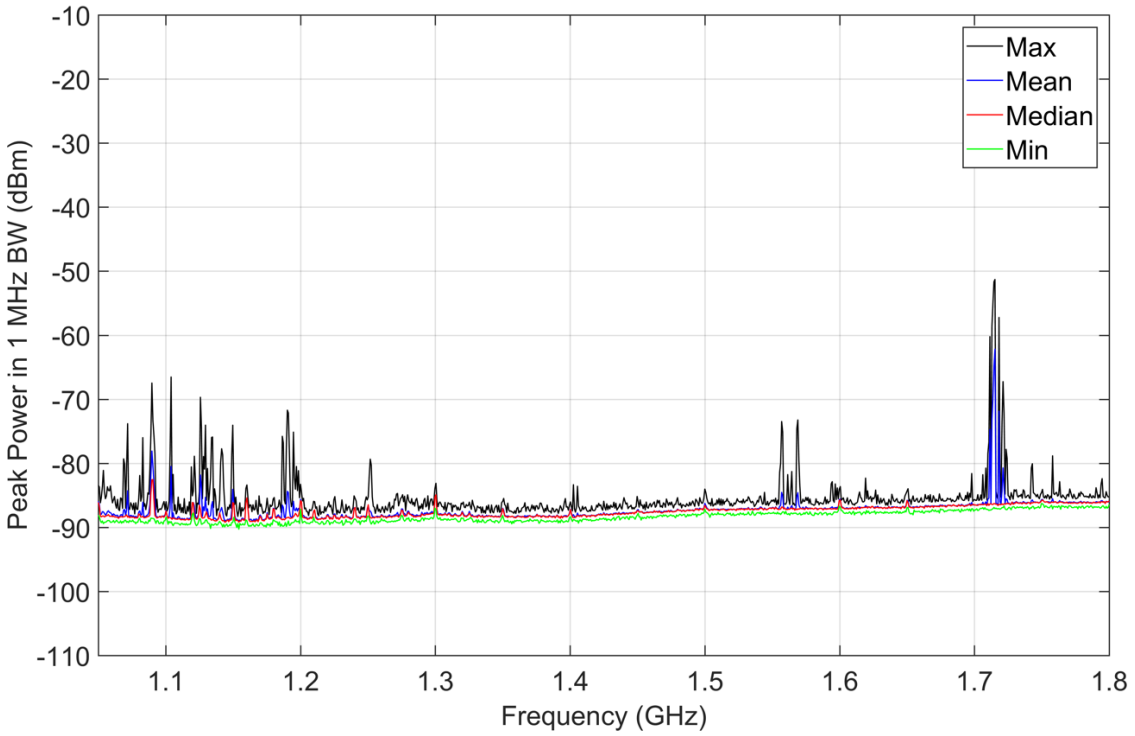


Figure 71. M4 statistics, peak detection, jammer on, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

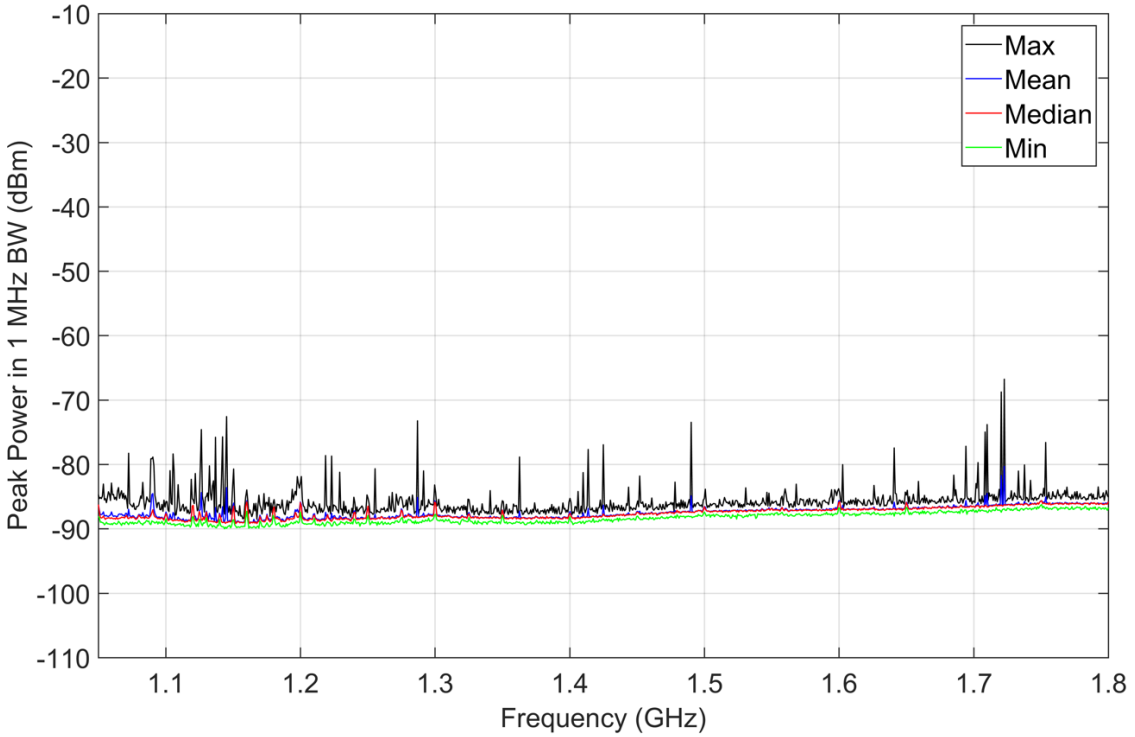


Figure 72. M4 statistics, peak detection, jammer off, 1050–1800 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

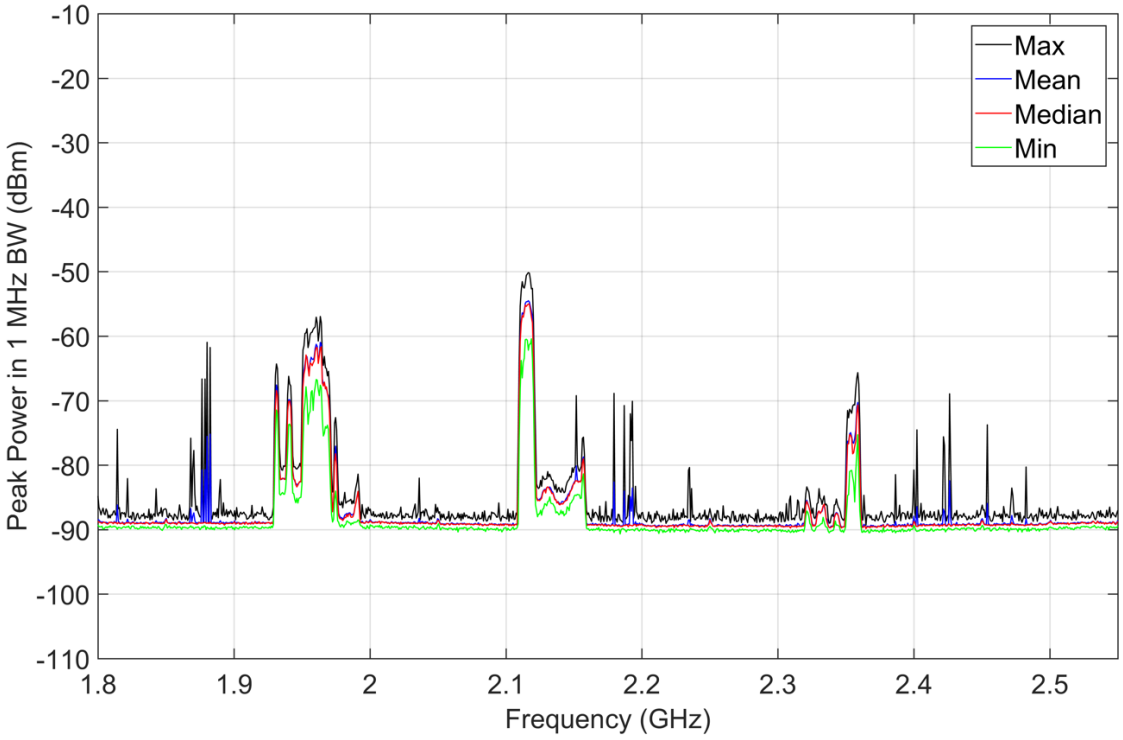


Figure 73. M4 statistics, peak detection, jammer on, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

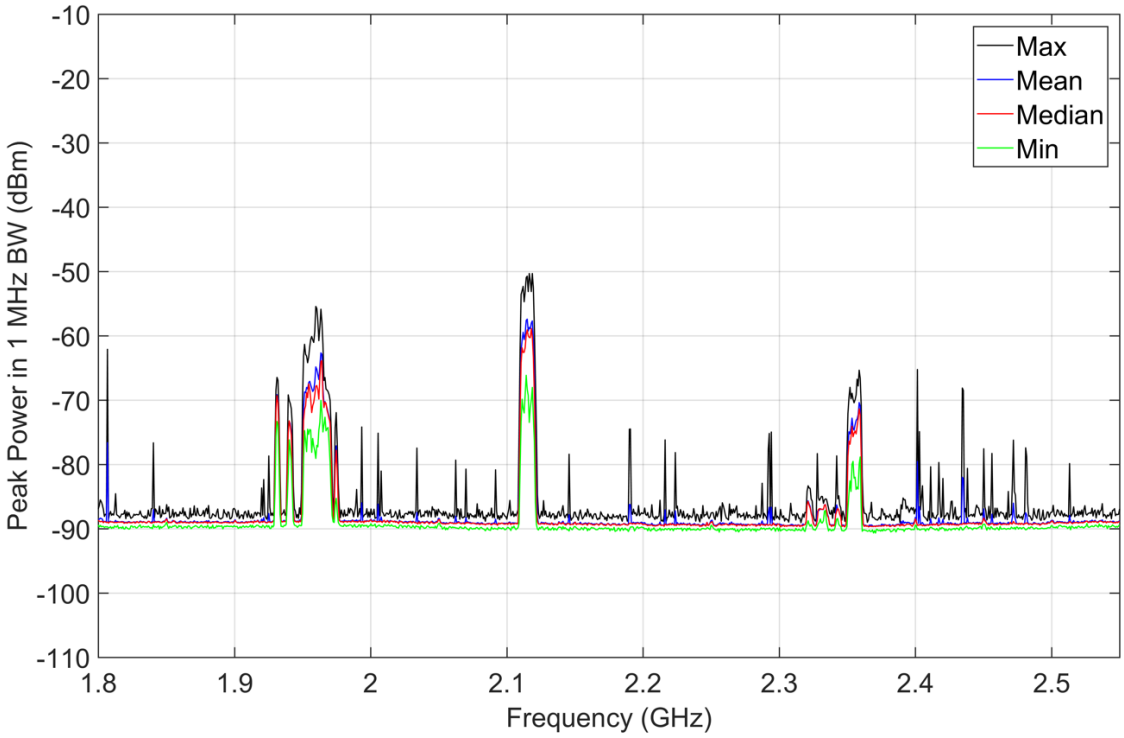


Figure 74. M4 statistics, peak detection, jammer off, 1800–2550 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

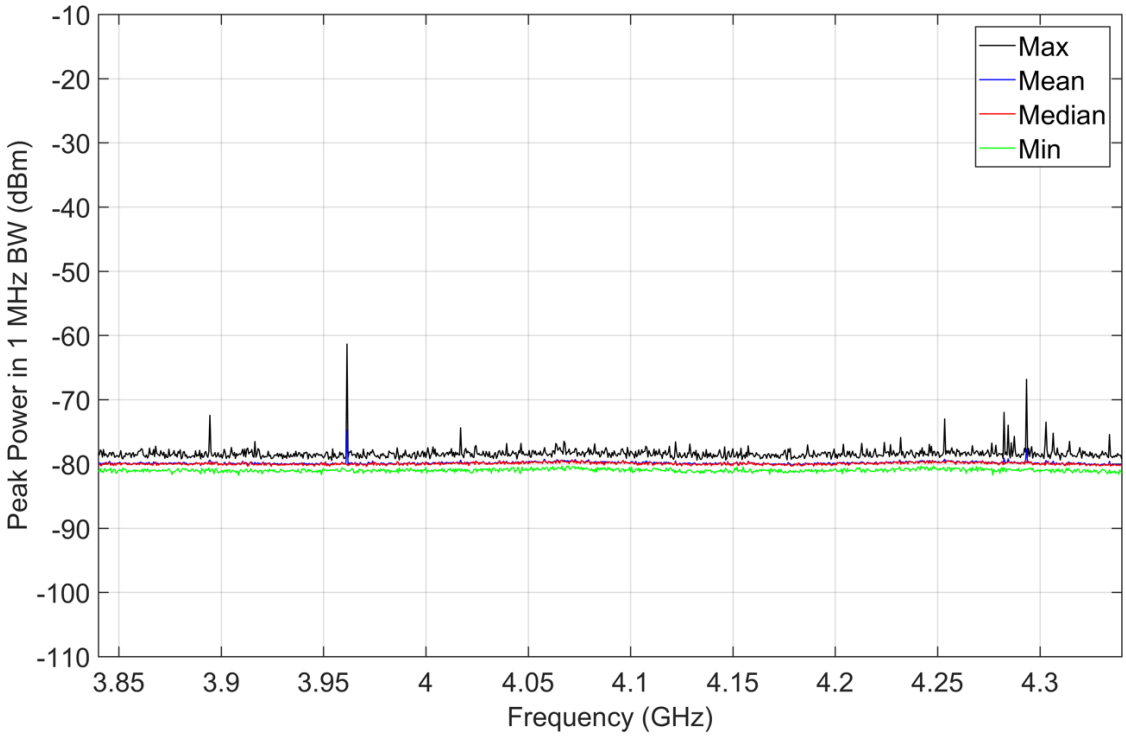


Figure 75. M4 statistics, peak detection, jammer on, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

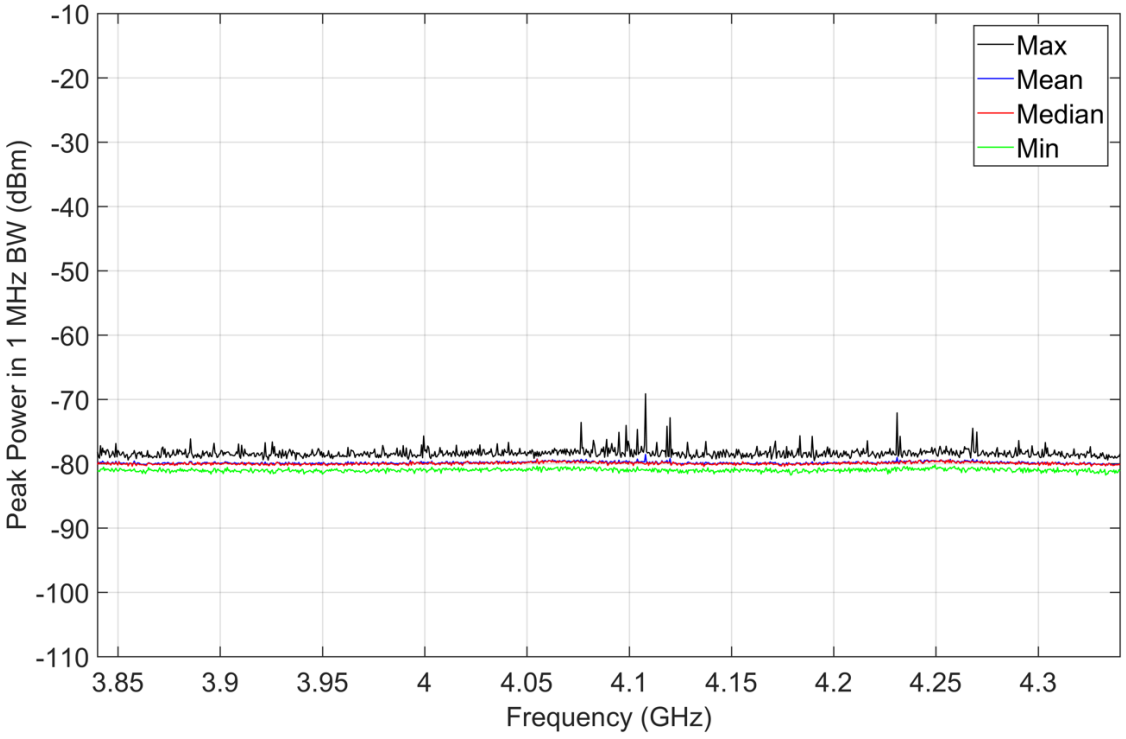


Figure 76. M4 statistics, peak detection, jammer off, 3840–4340 MHz, 1 MHz bandwidth, 30 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

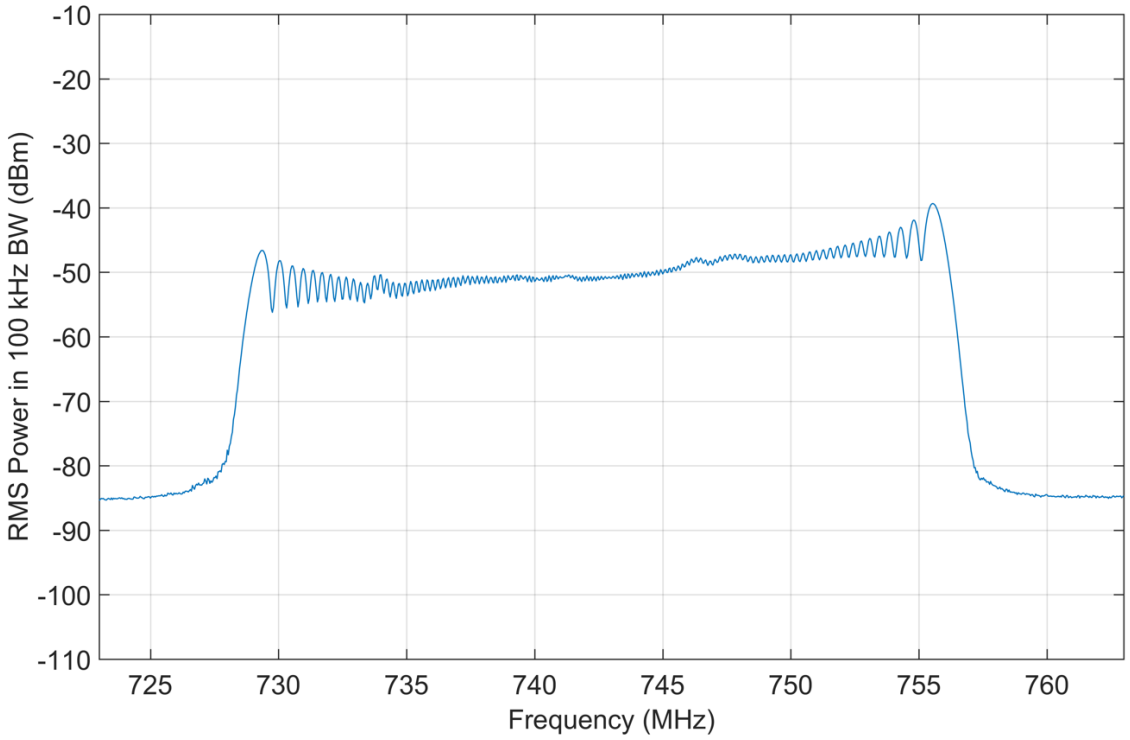


Figure 77. RMS average detection, jammer on, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-1 inside targeted prison cell.

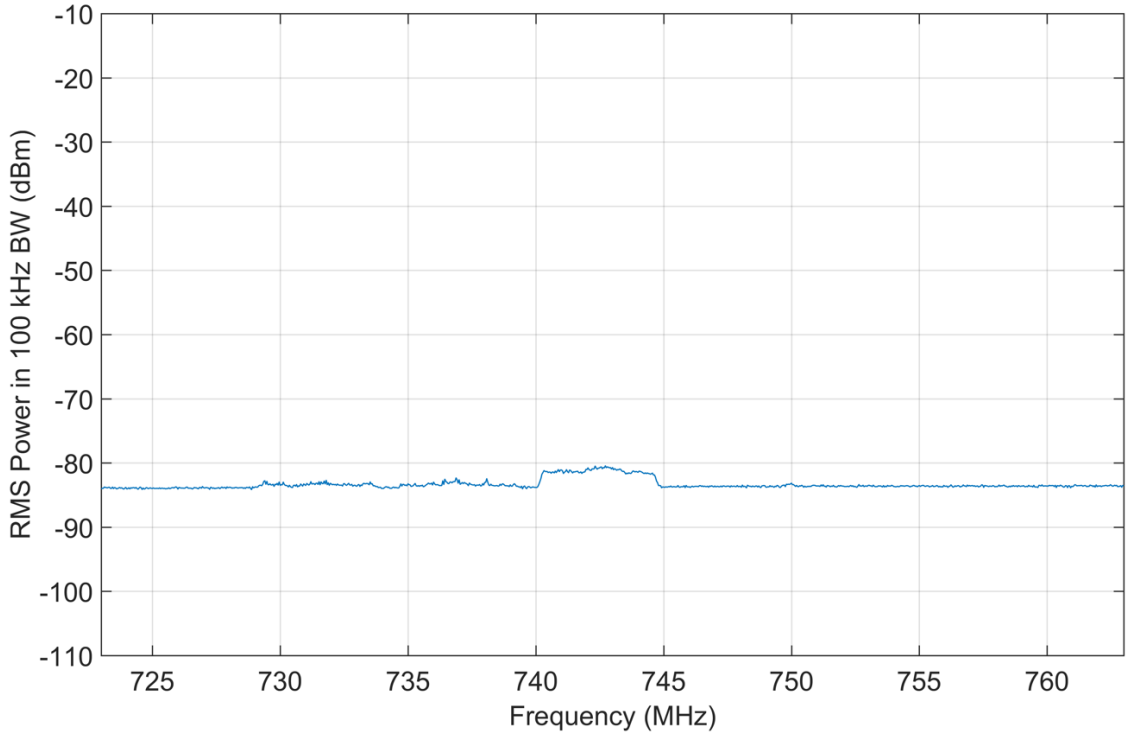


Figure 78. RMS average detection, jammer off, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-1 inside targeted prison cell.

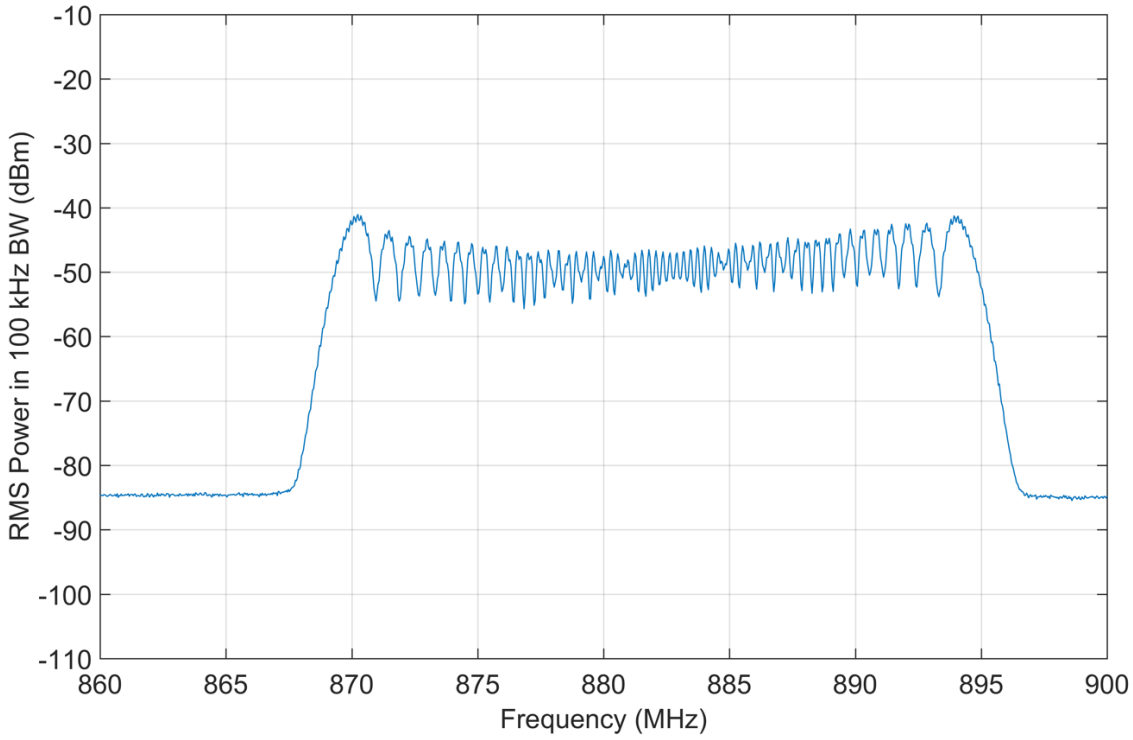


Figure 79. RMS average detection, jammer on, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-1 inside targeted prison cell.

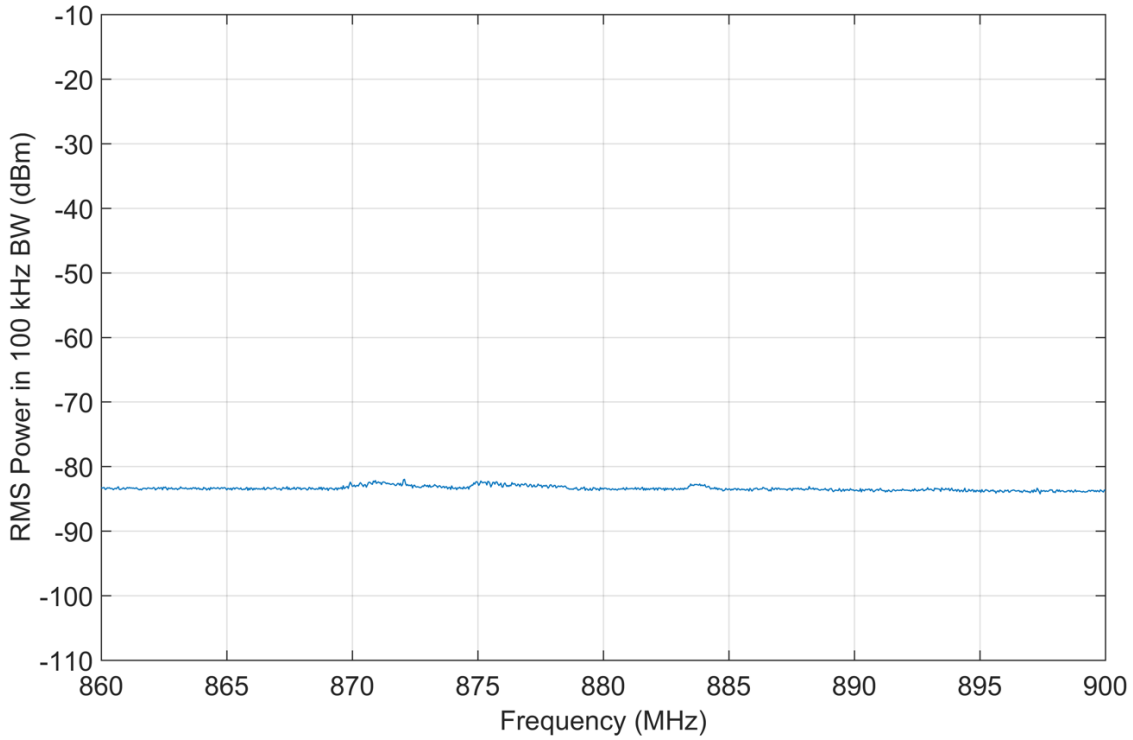


Figure 80. RMS average detection, jammer off, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-1 inside targeted prison cell.

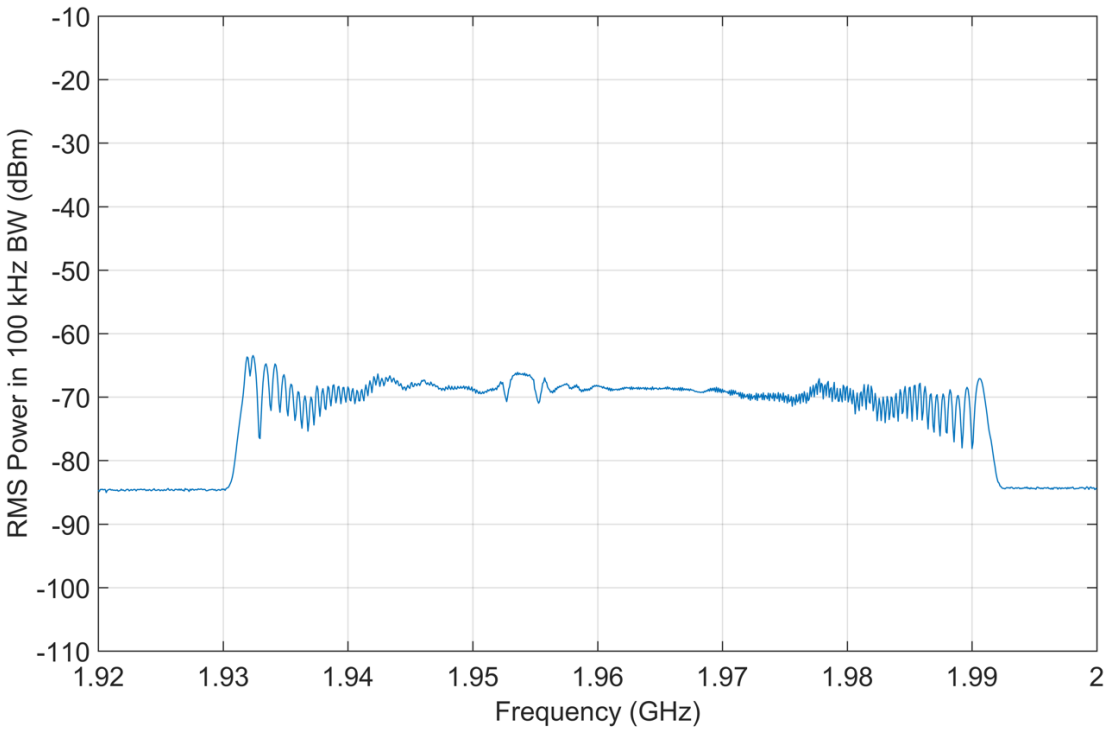


Figure 81. RMS average detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-1 inside targeted prison cell.

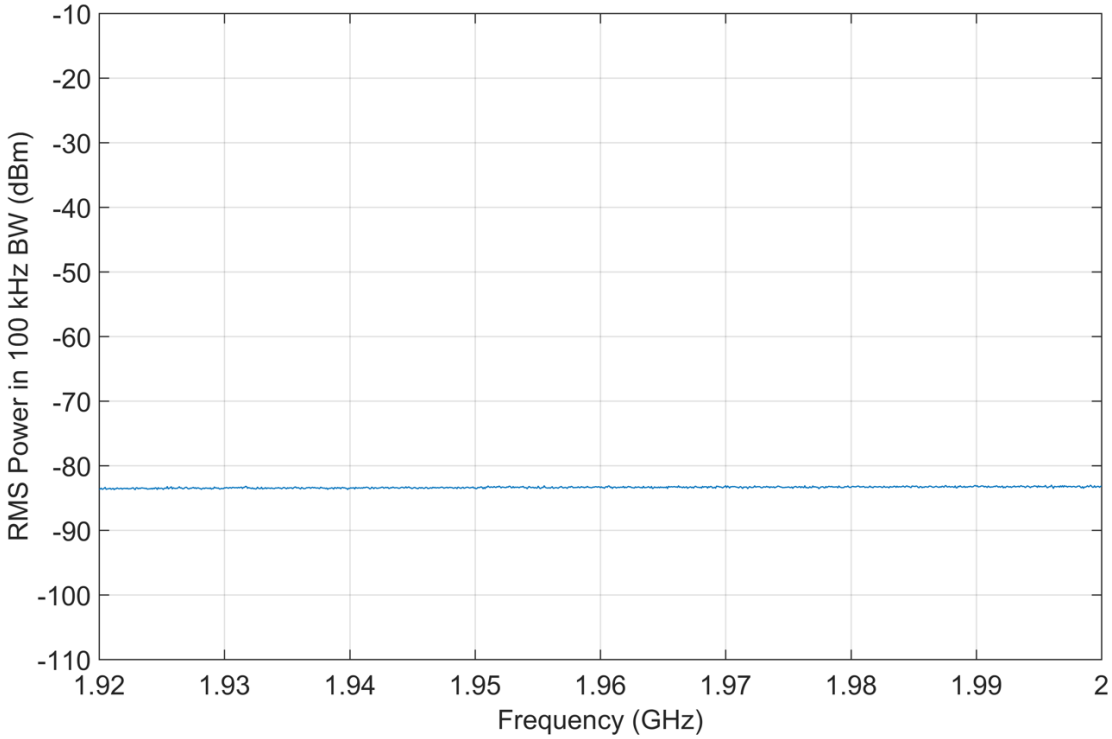


Figure 82. RMS average detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-1 inside targeted prison cell.

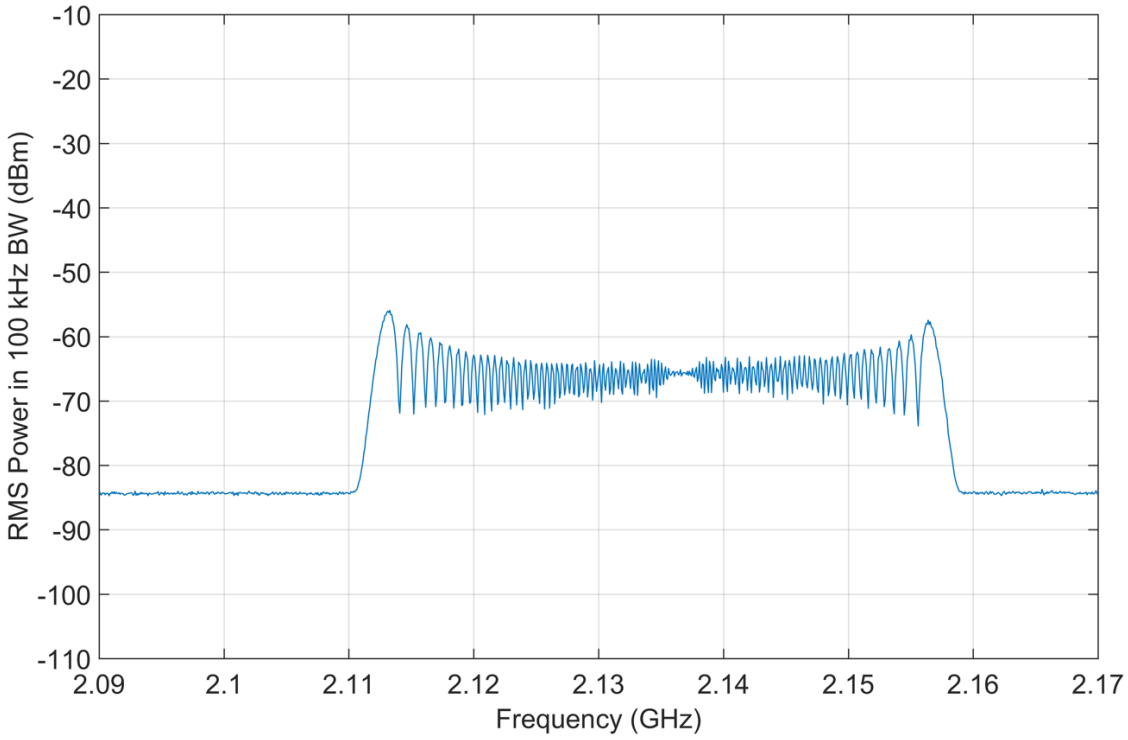


Figure 83. RMS average detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-1 inside targeted prison cell.

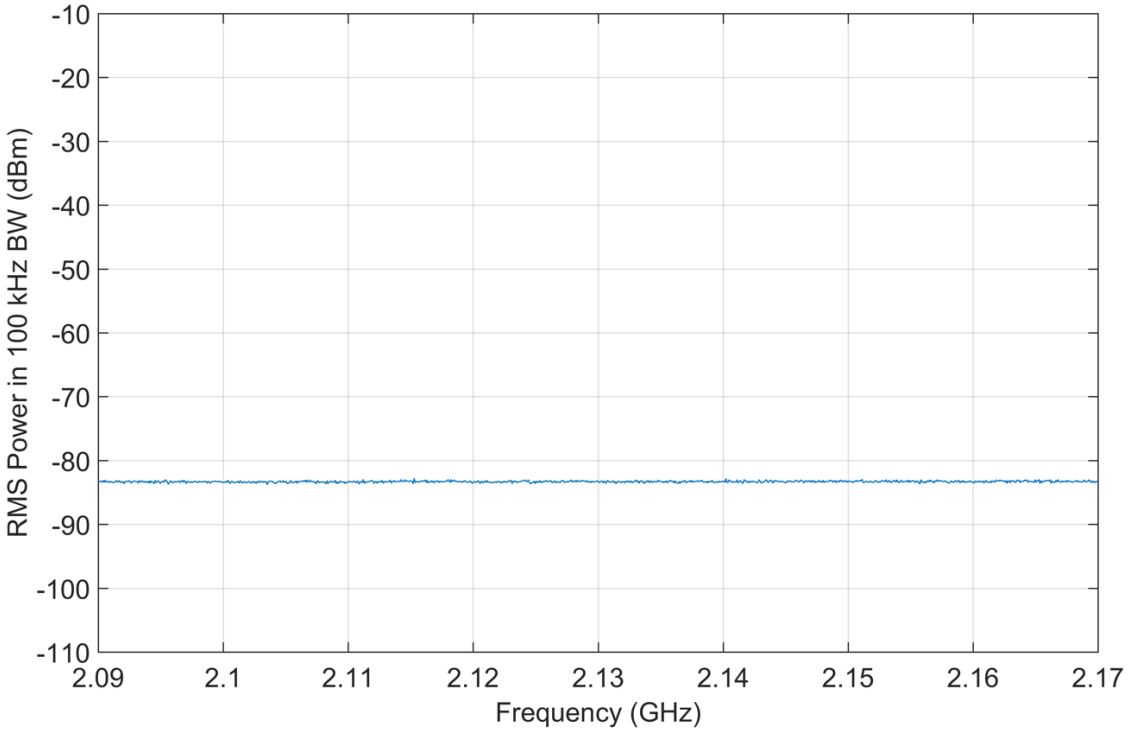


Figure 84. RMS average detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-1 inside targeted prison cell.

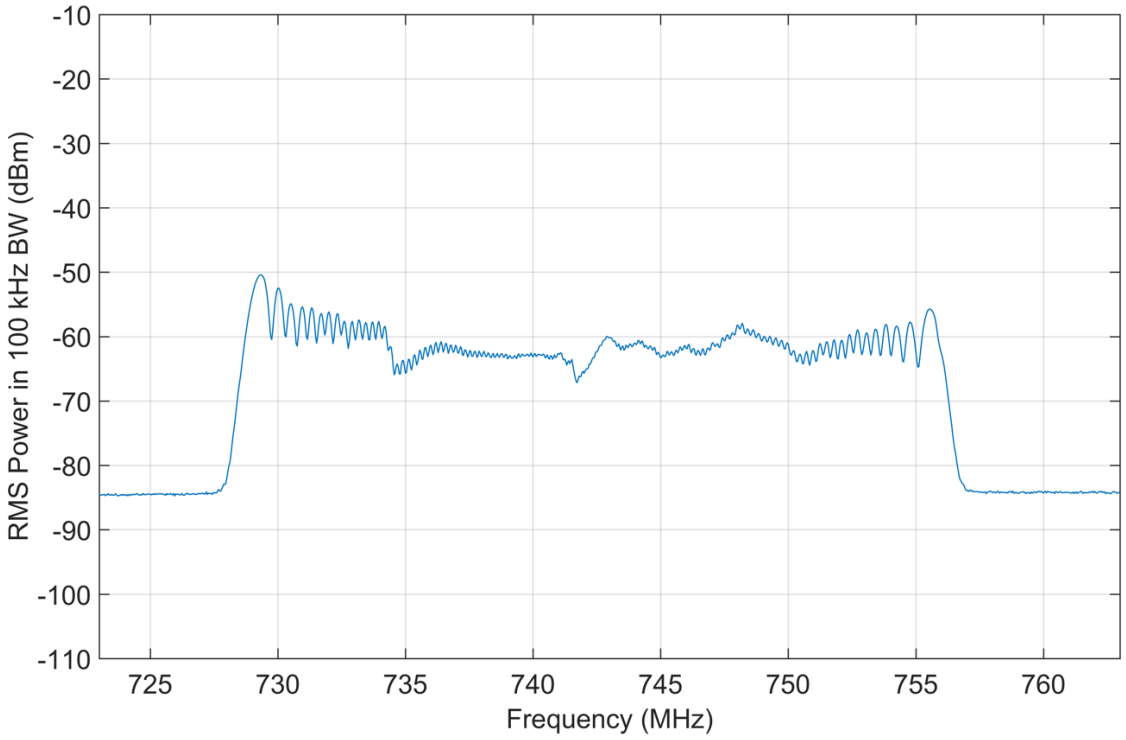


Figure 85. RMS average detection, jammer on, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-2 inside targeted prison cell.

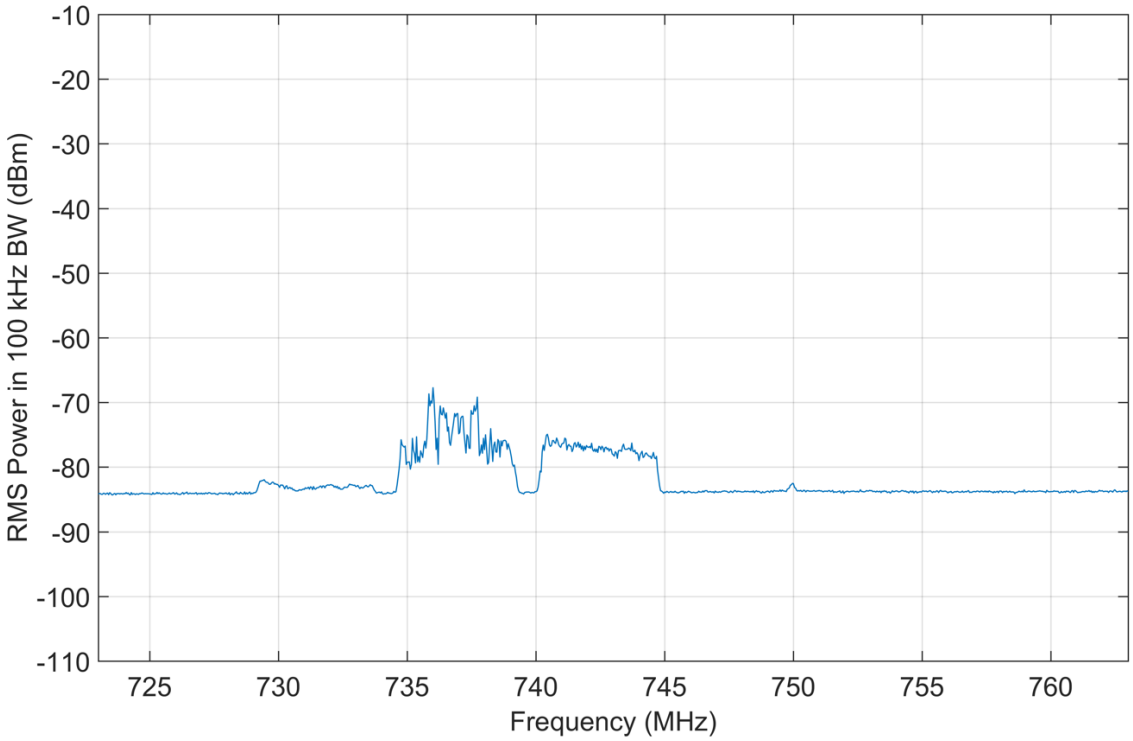


Figure 86. RMS average detection, jammer off, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-2 inside targeted prison cell.

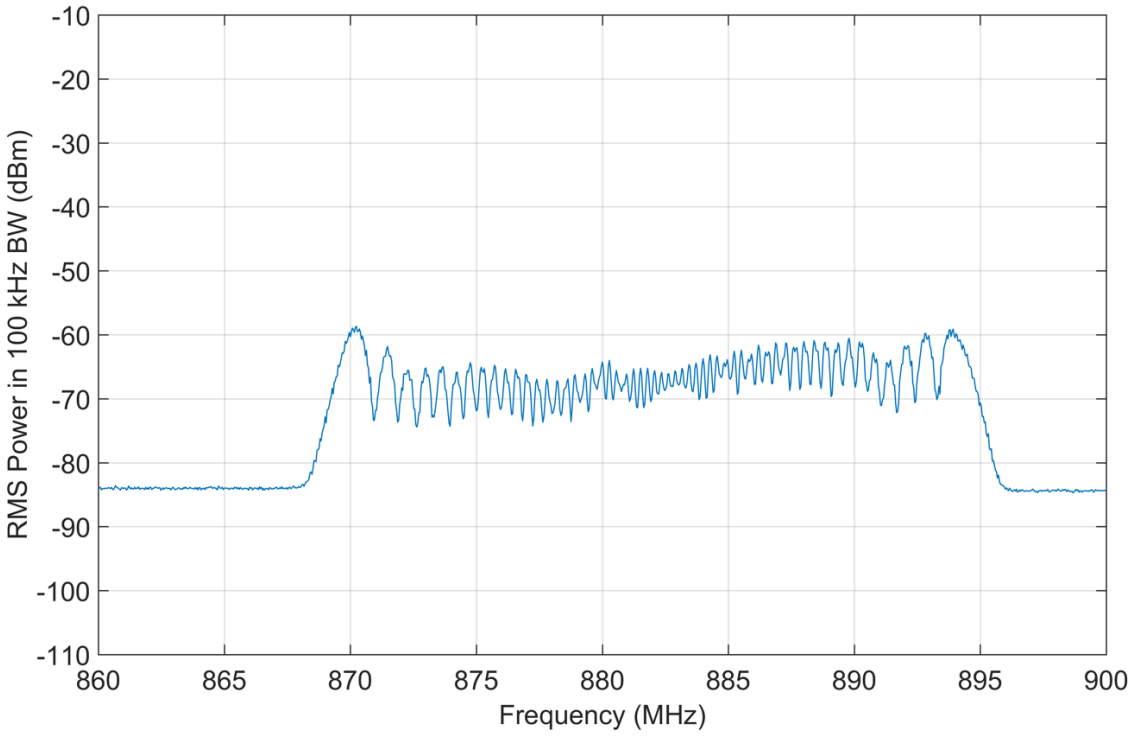


Figure 87. RMS average detection, jammer on, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-2 inside targeted prison cell.

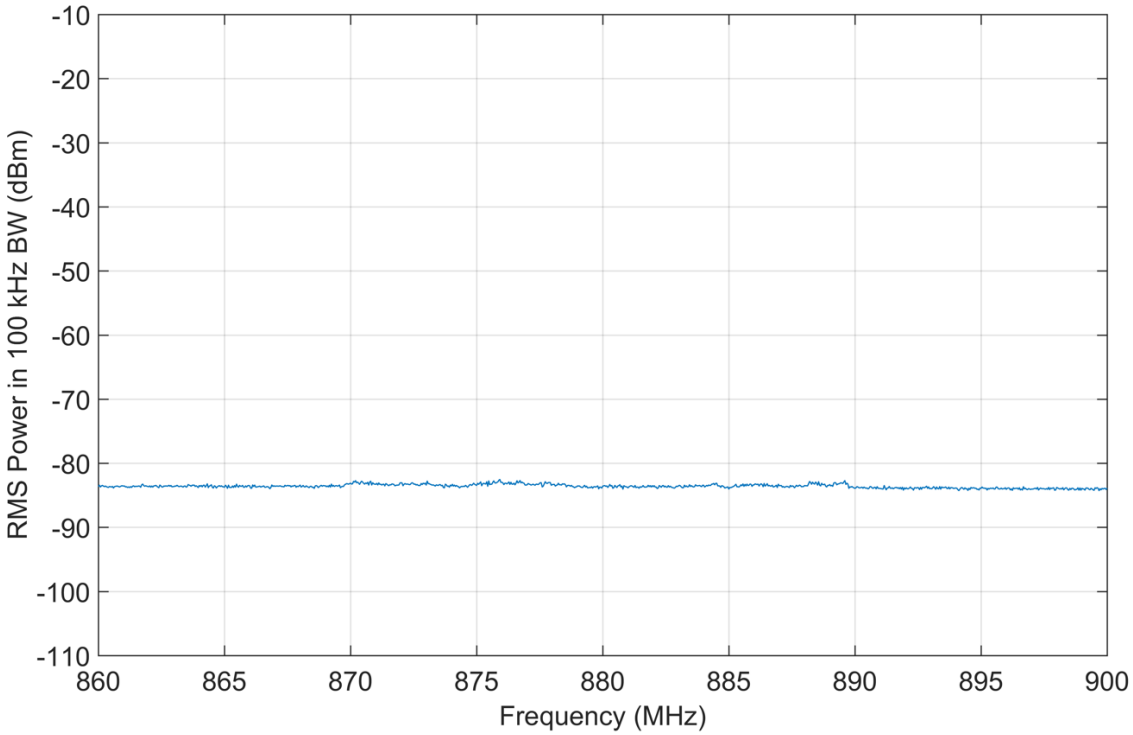


Figure 88. RMS average detection, jammer off, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-2 inside targeted prison cell.

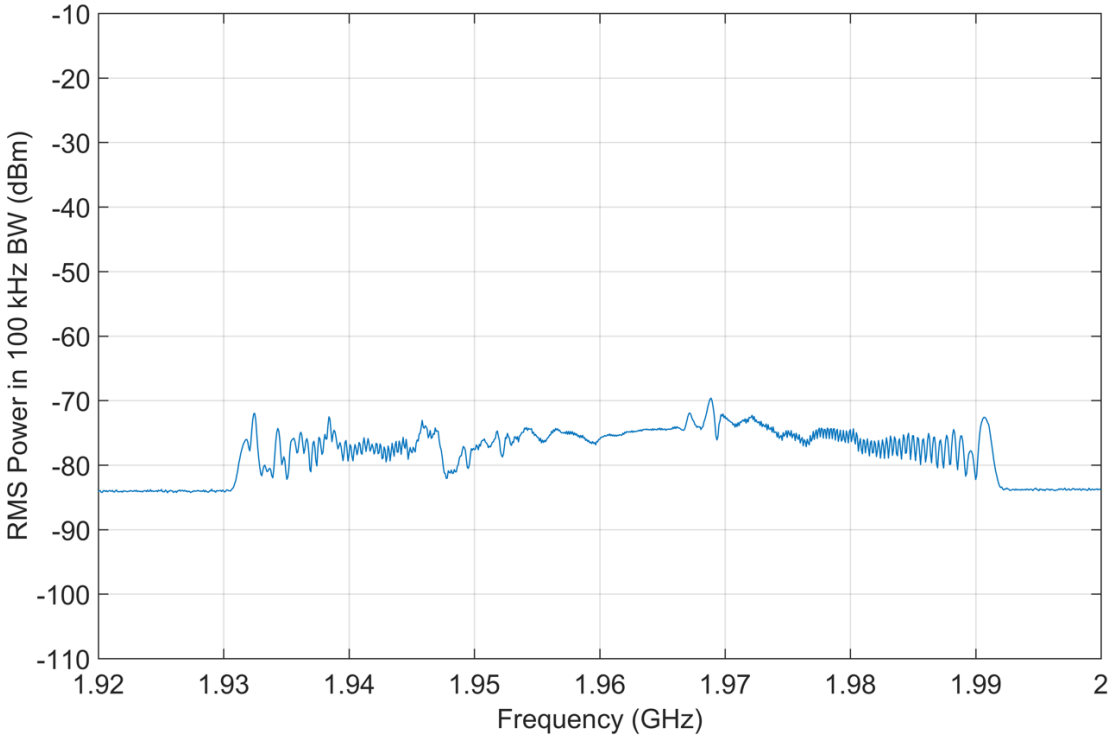


Figure 89. RMS average detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-2 inside targeted prison cell.

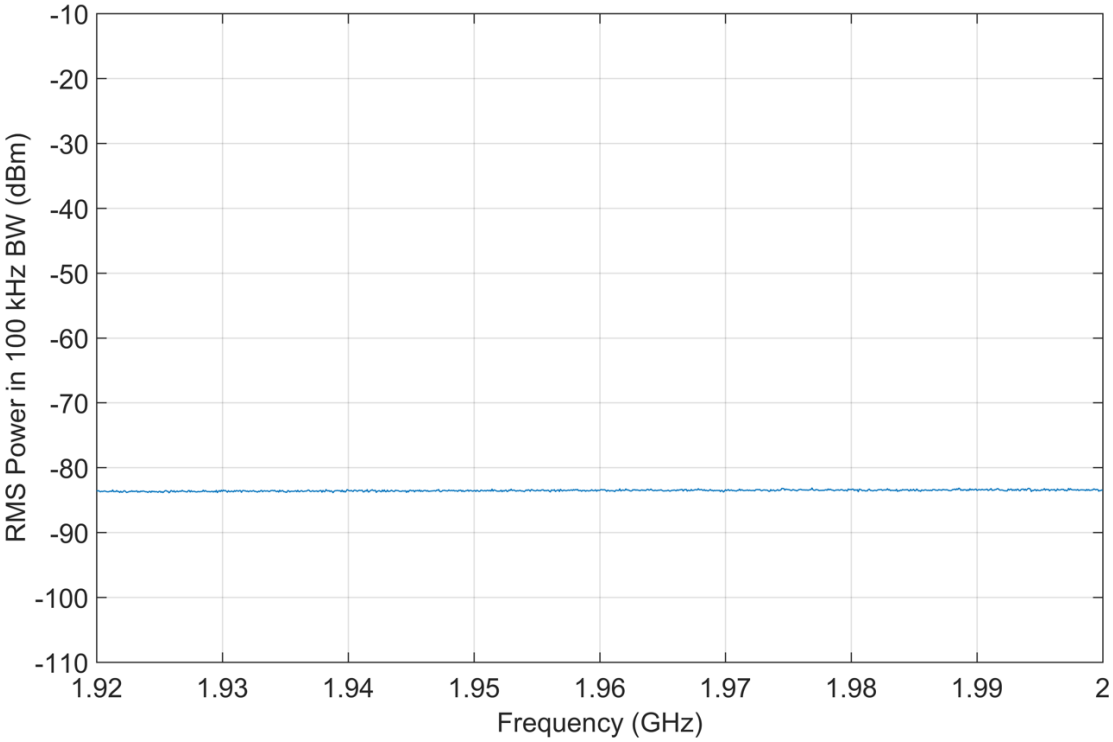


Figure 90. RMS average detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp off, location I-2 inside targeted prison cell.

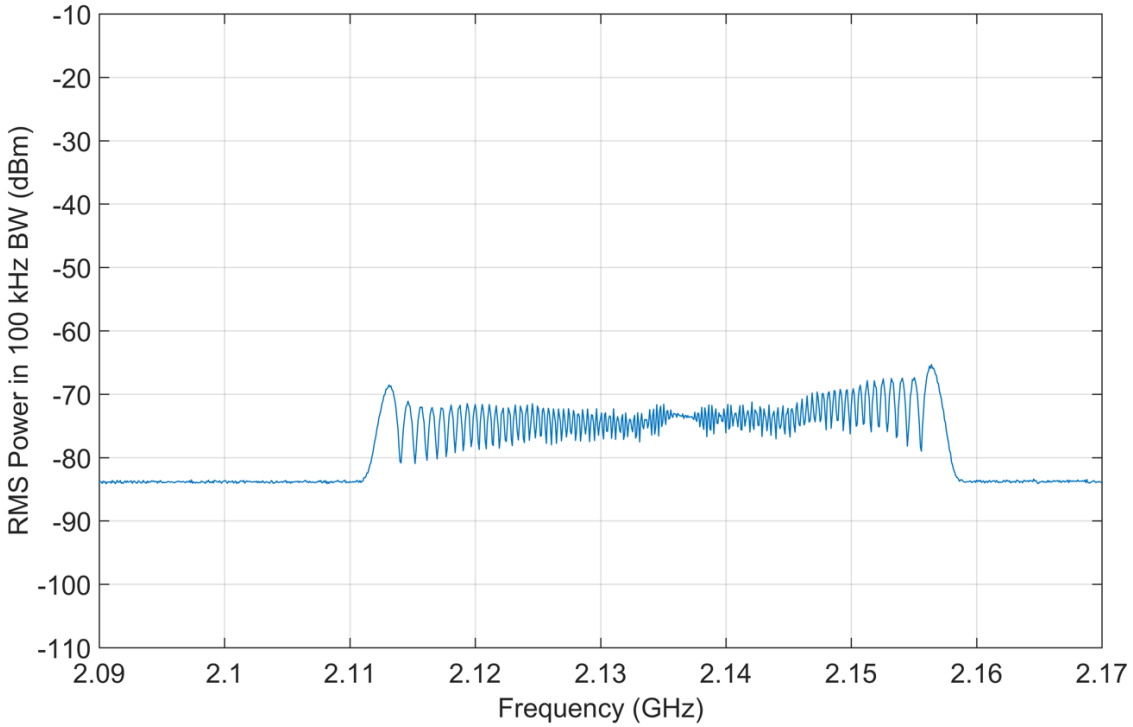


Figure 91. RMS average detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-2 inside targeted prison cell.

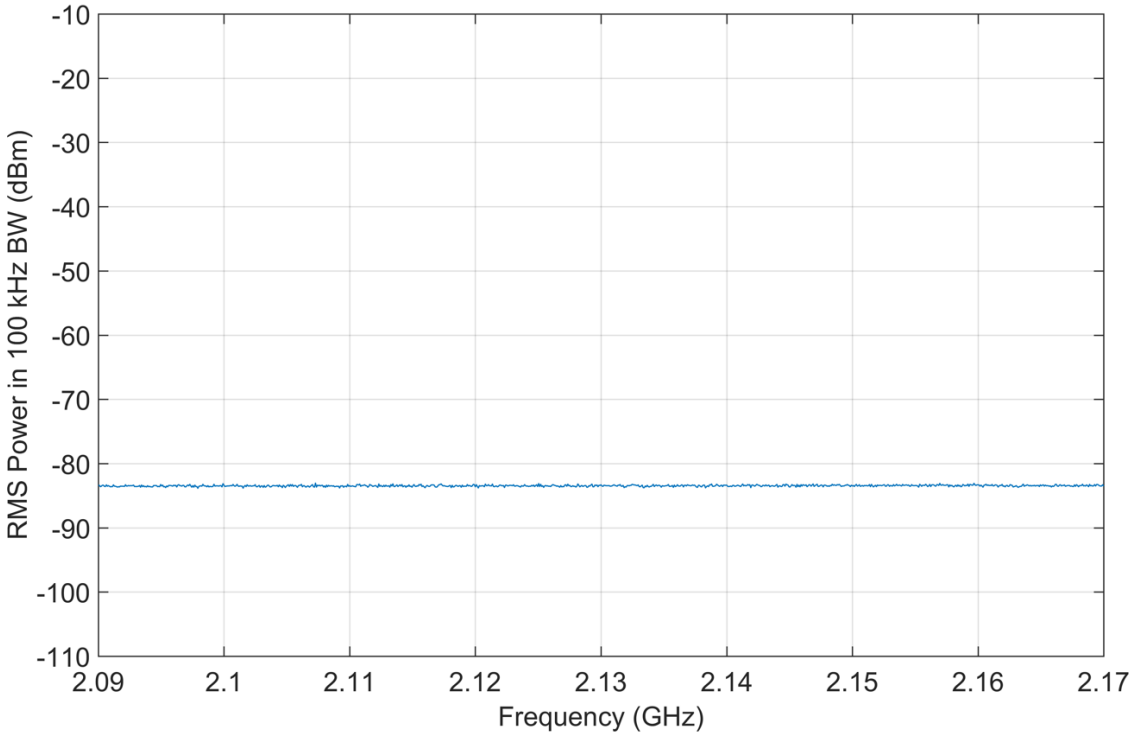


Figure 92. RMS average detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp off, location I-2 inside targeted prison cell.

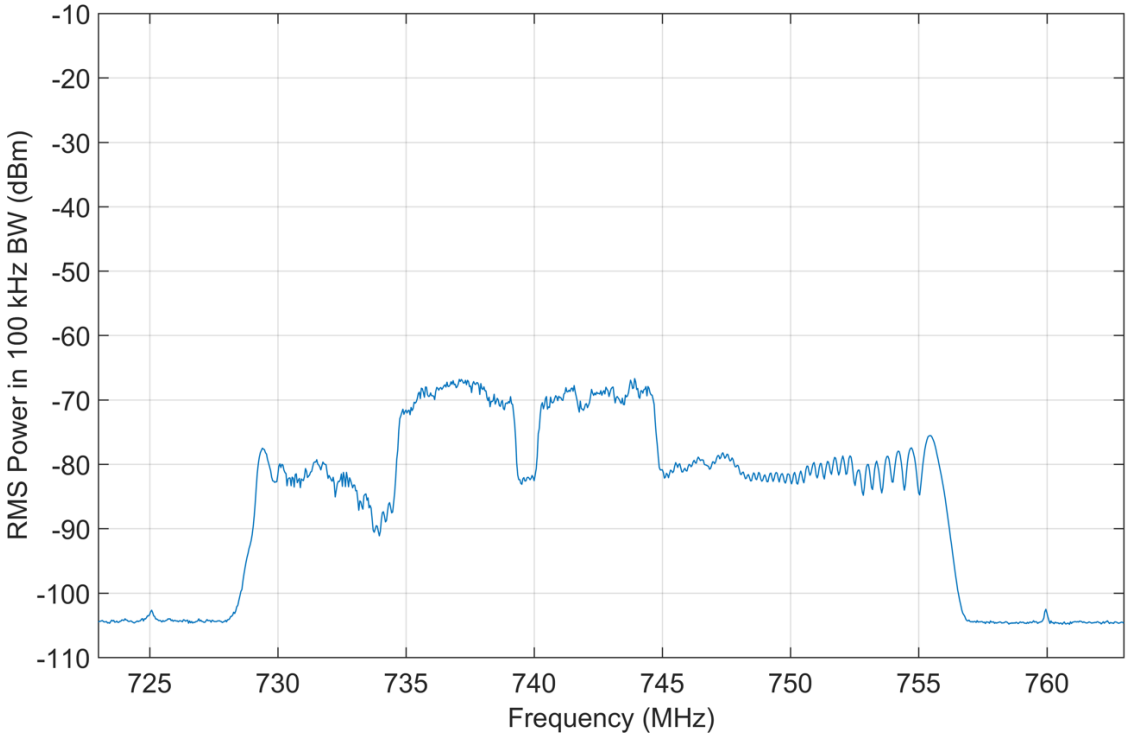


Figure 93. RMS average detection, jammer on, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-1 outside targeted prison cell.

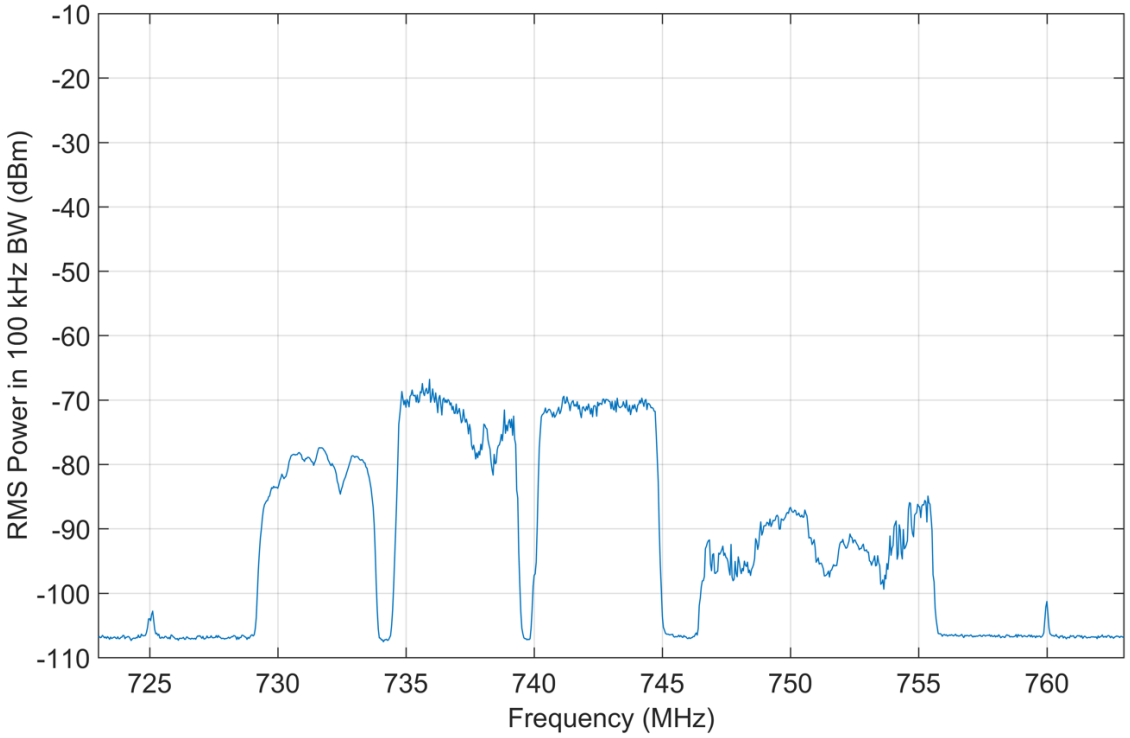


Figure 94. RMS average detection, jammer off, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-1 outside targeted prison cell.

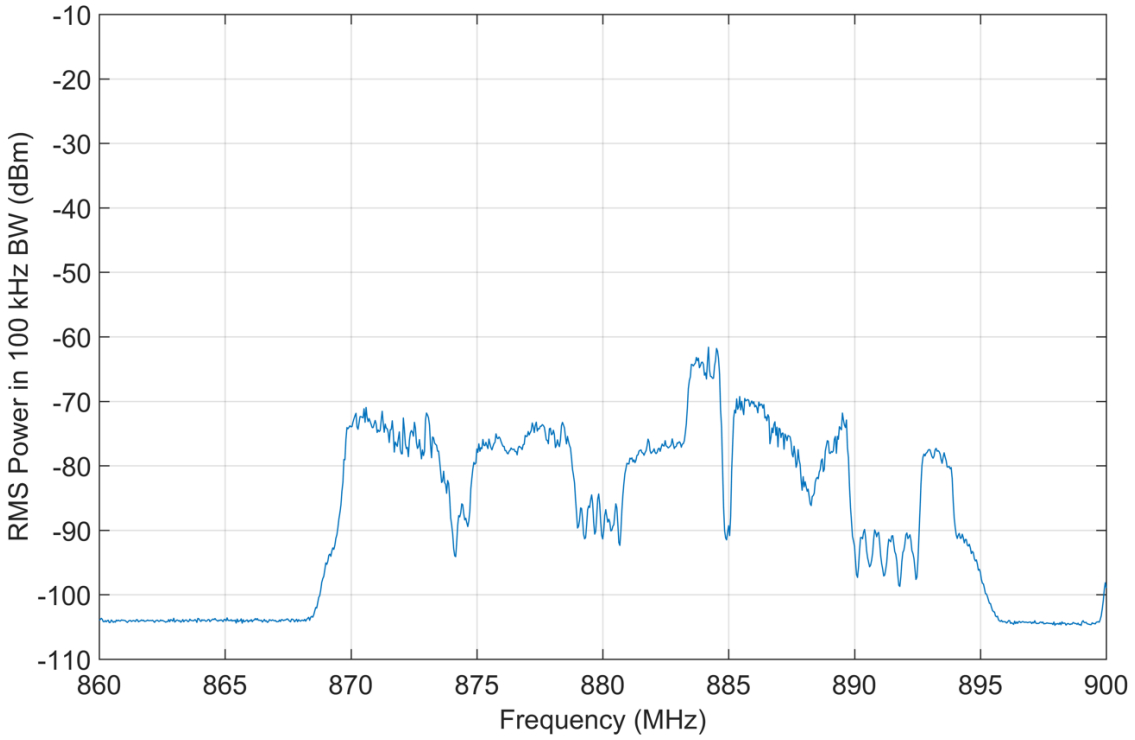


Figure 95. RMS average detection, jammer on, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-1 outside targeted prison cell.

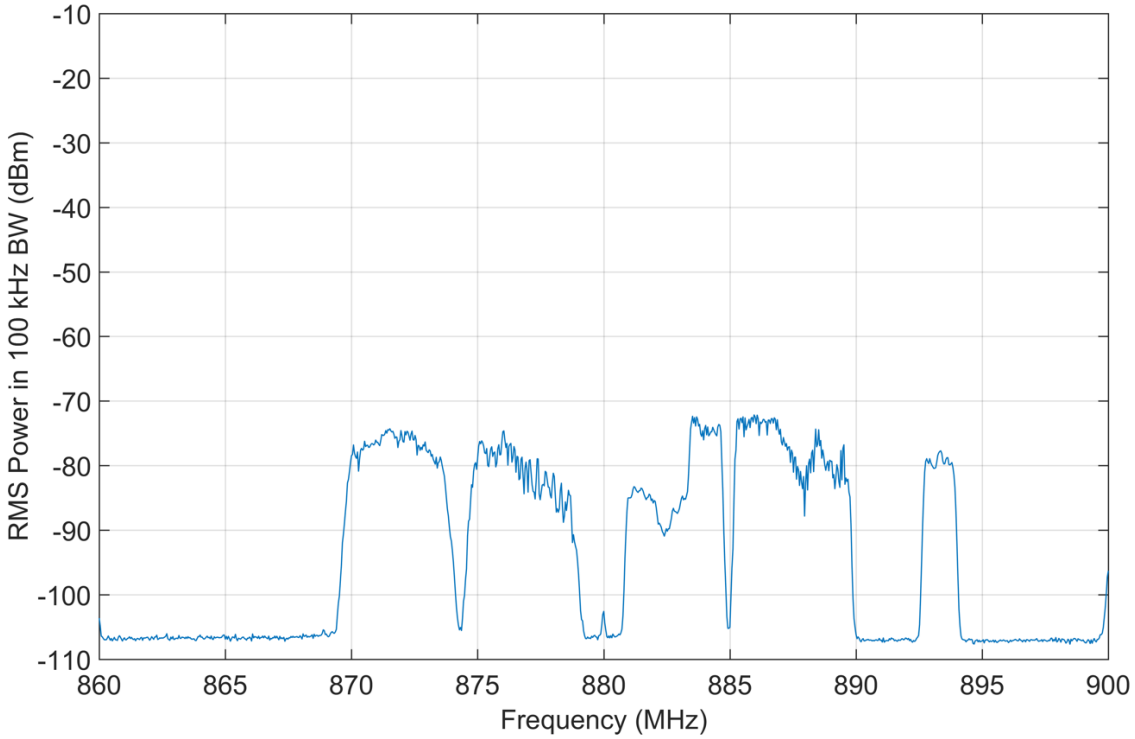


Figure 96. RMS average detection, jammer off, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-1 outside targeted prison cell.

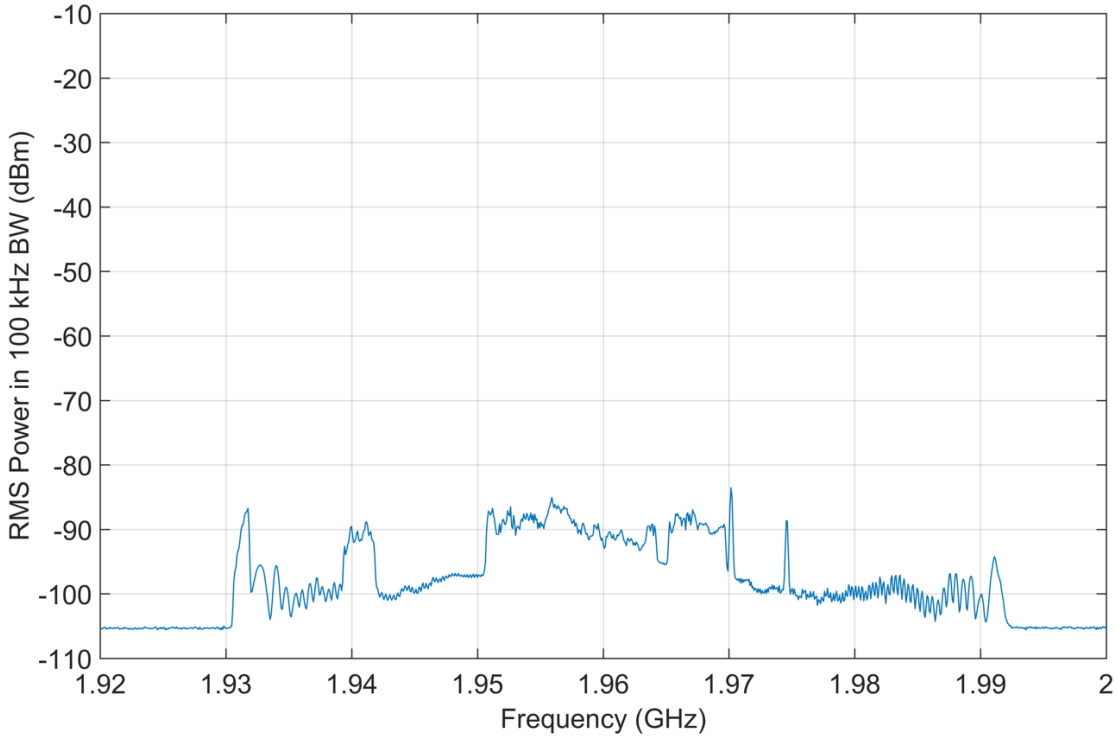


Figure 97. RMS average detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-1 outside targeted prison cell.

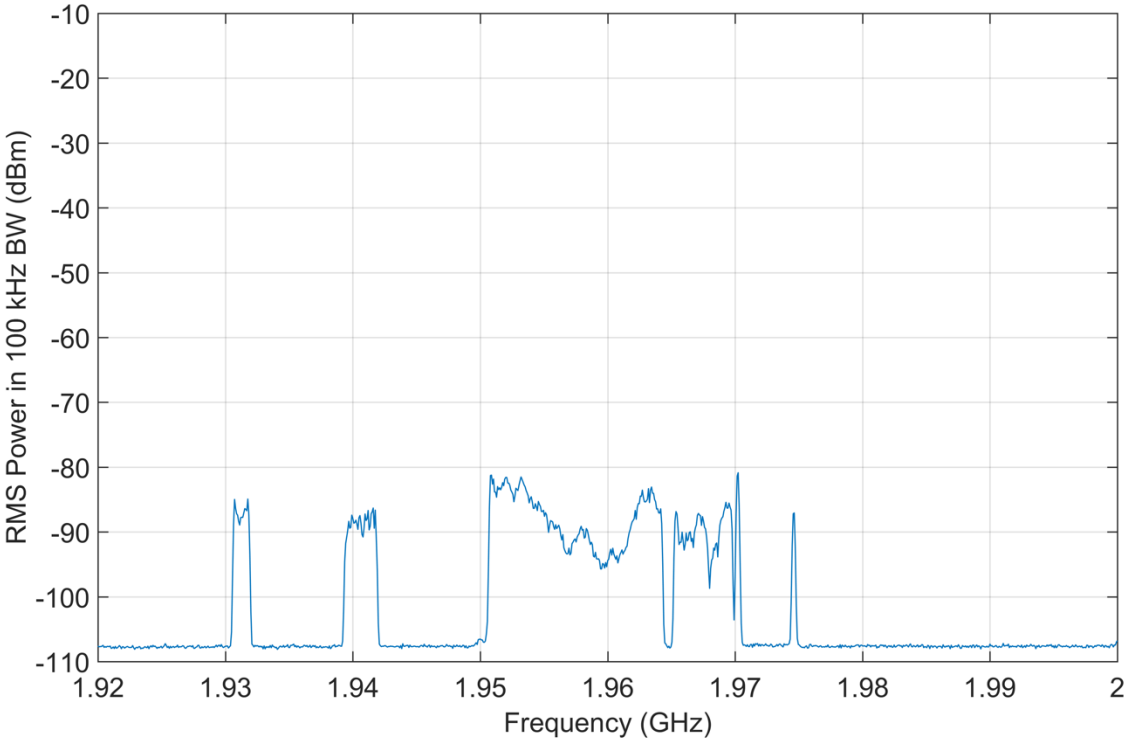


Figure 98. RMS average detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-1 outside targeted prison cell.

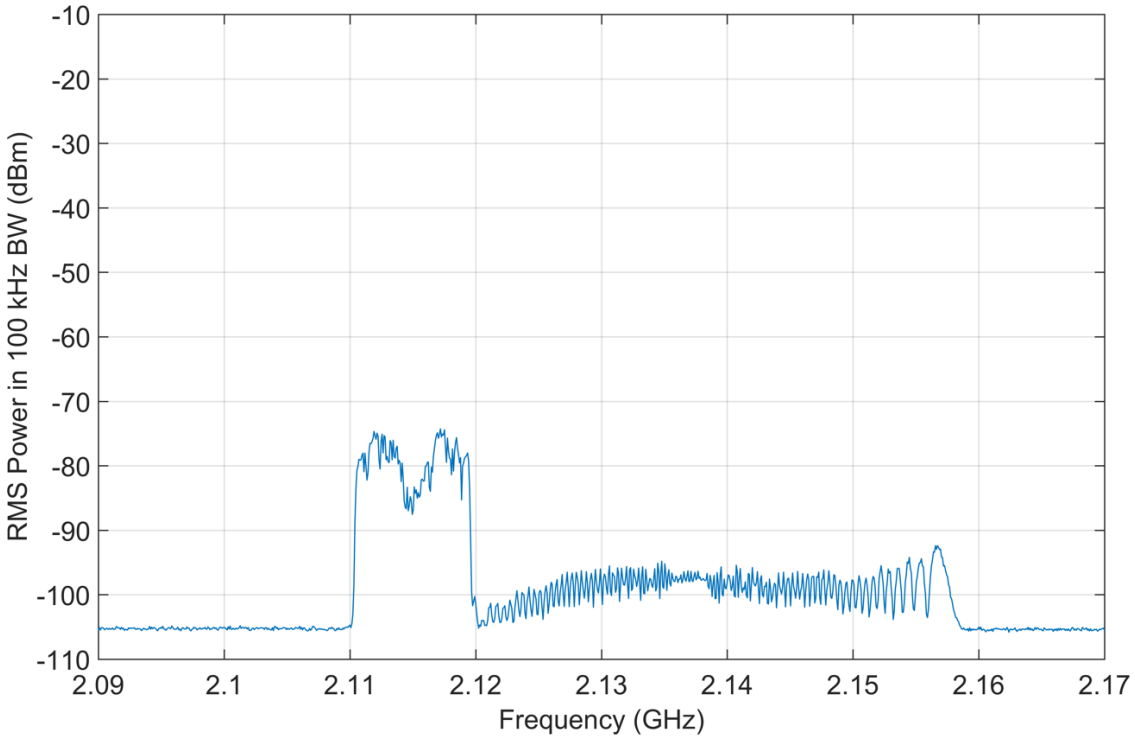


Figure 99. RMS average detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-1 outside targeted prison cell.

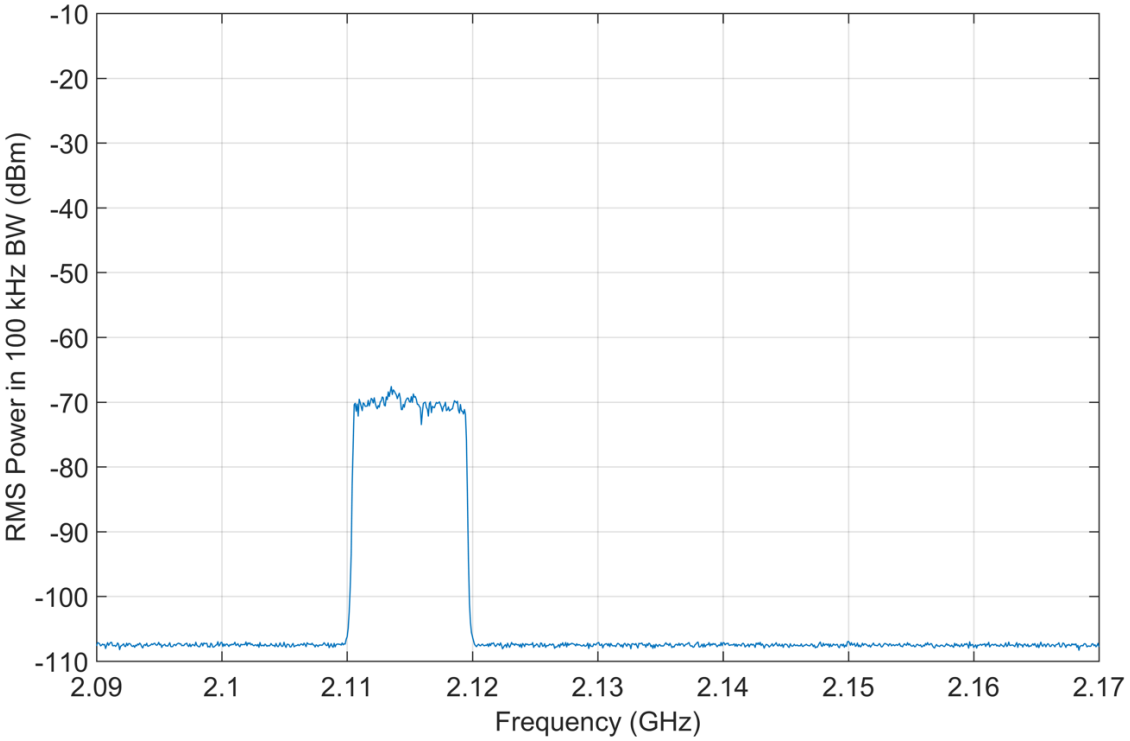


Figure 100. RMS average detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-1 outside targeted prison cell.

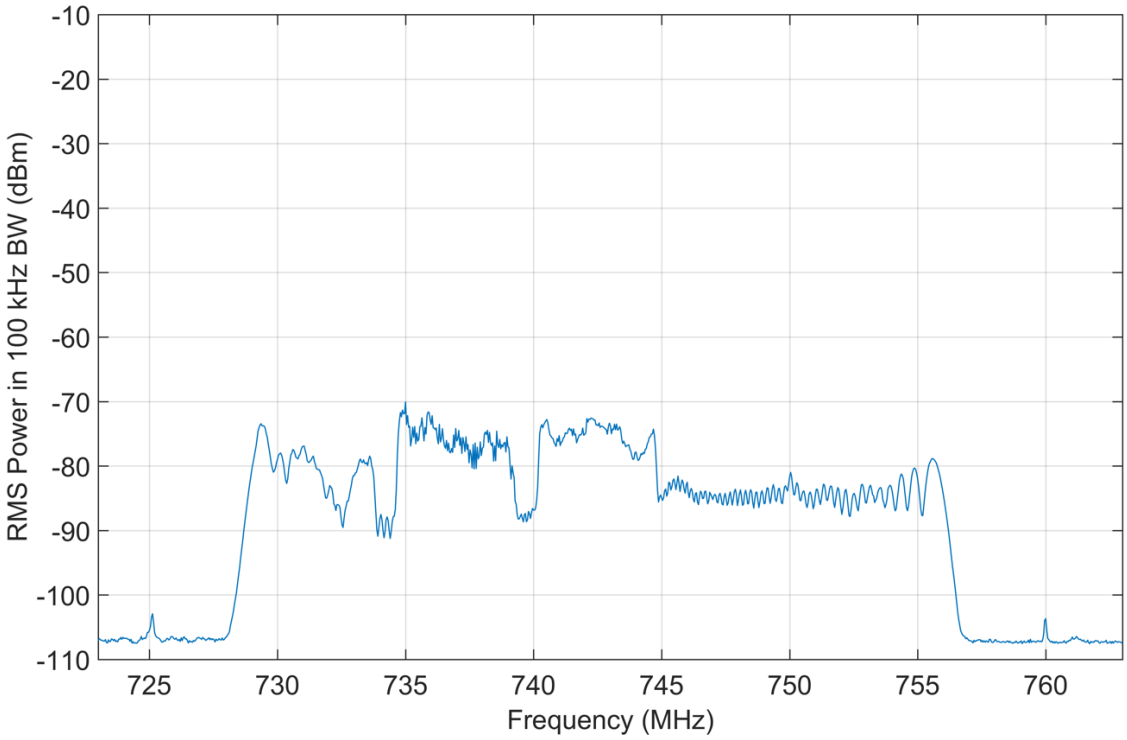


Figure 101. RMS average detection, jammer on, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-2 outside targeted prison cell.

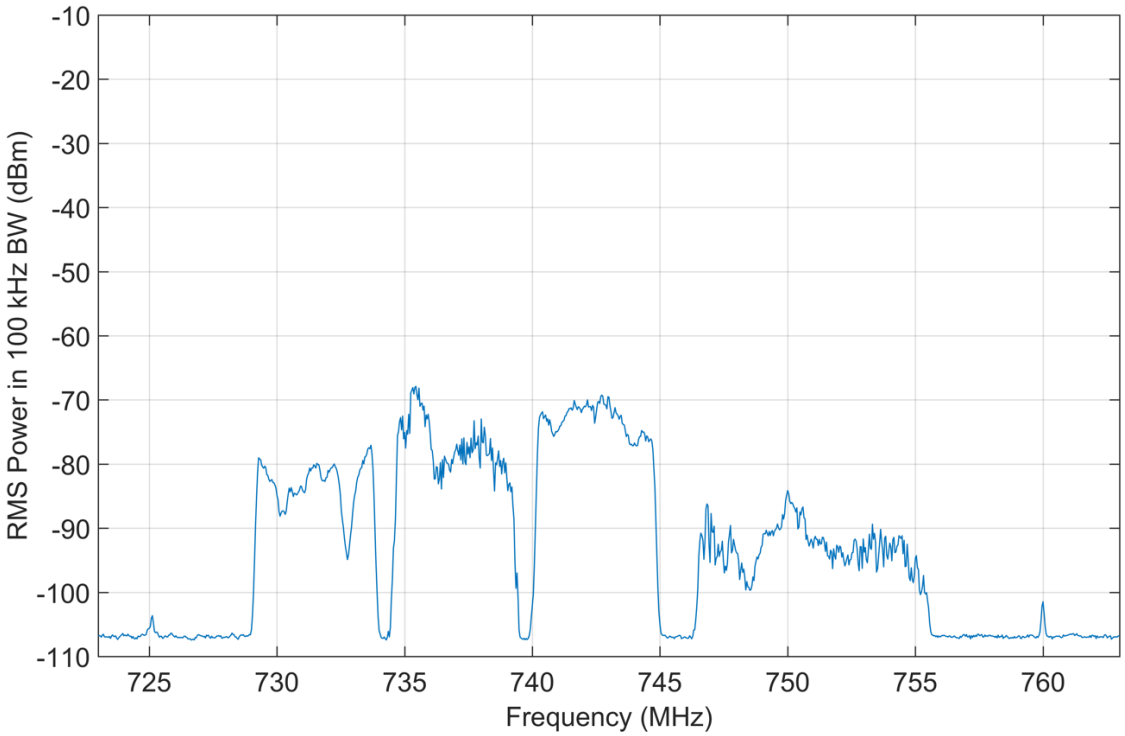


Figure 102. RMS average detection, jammer off, 723–763 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-2 outside targeted prison cell.

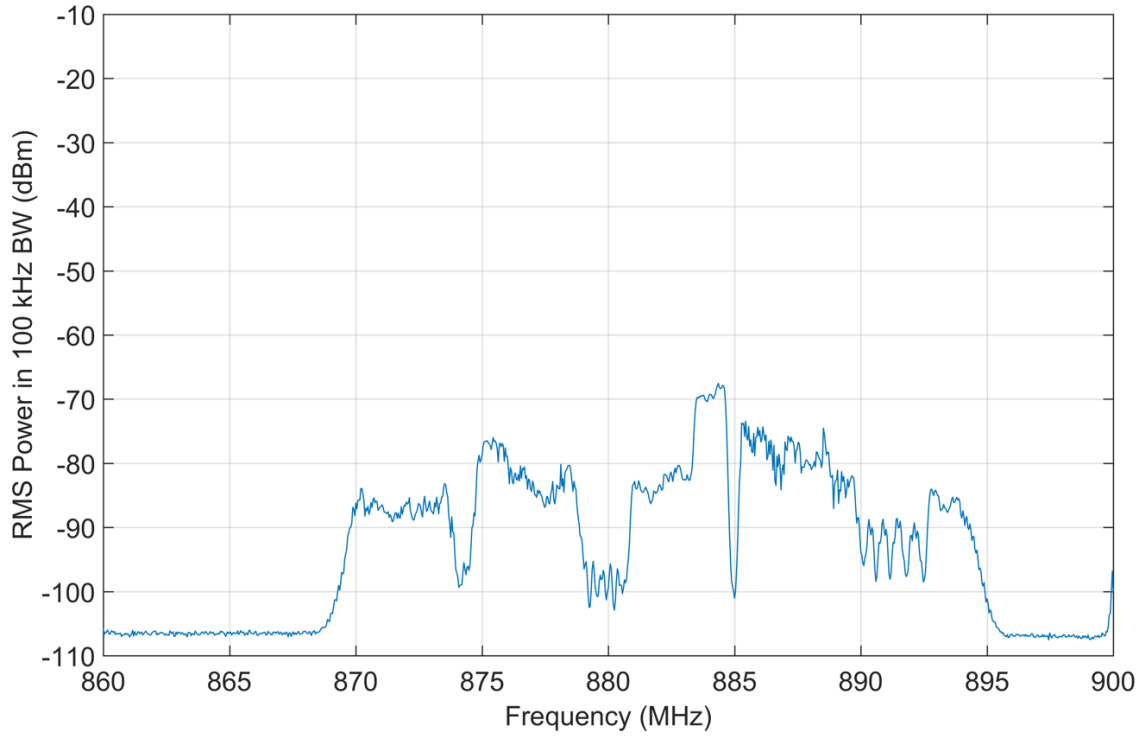


Figure 103. RMS average detection, jammer on, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-2 outside targeted prison cell.

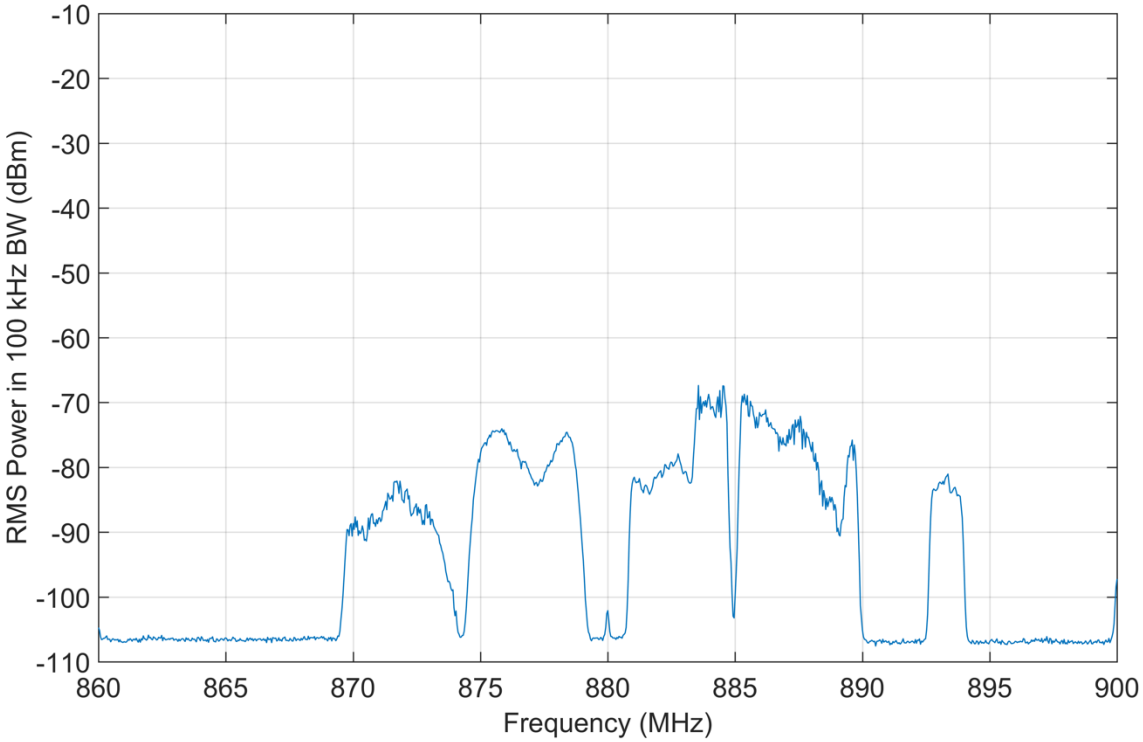


Figure 104. RMS average detection, jammer off, 860–900 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-2 outside targeted prison cell.

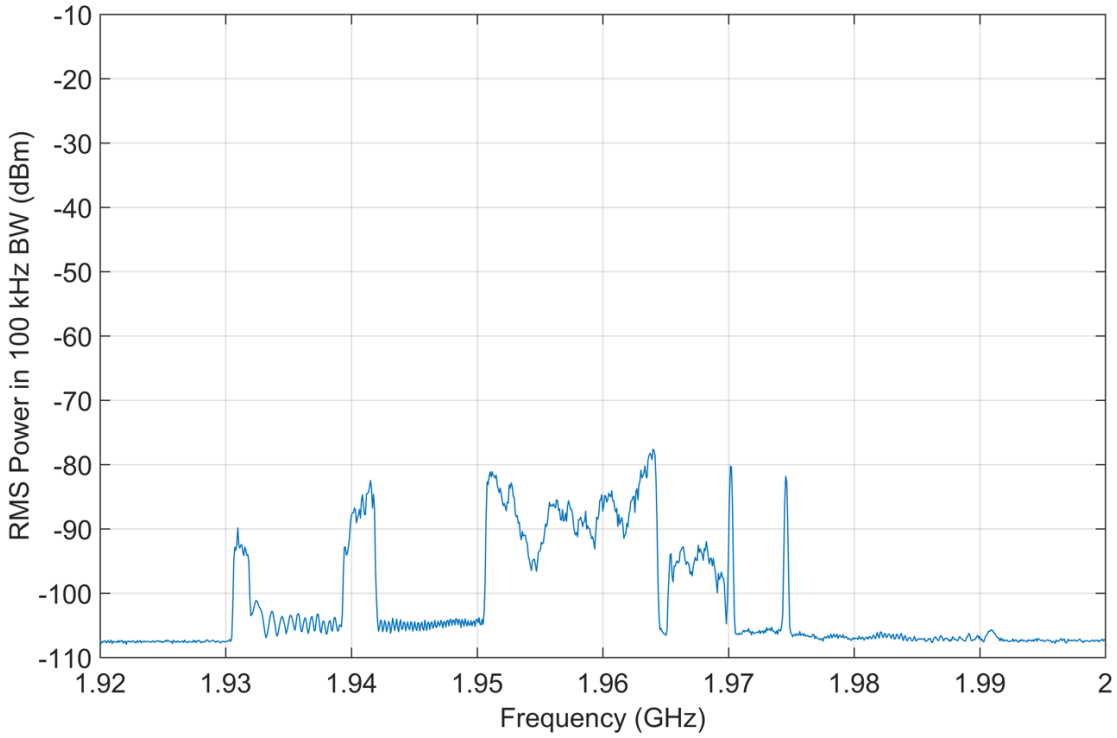


Figure 105. RMS average detection, jammer on, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-2 outside targeted prison cell.

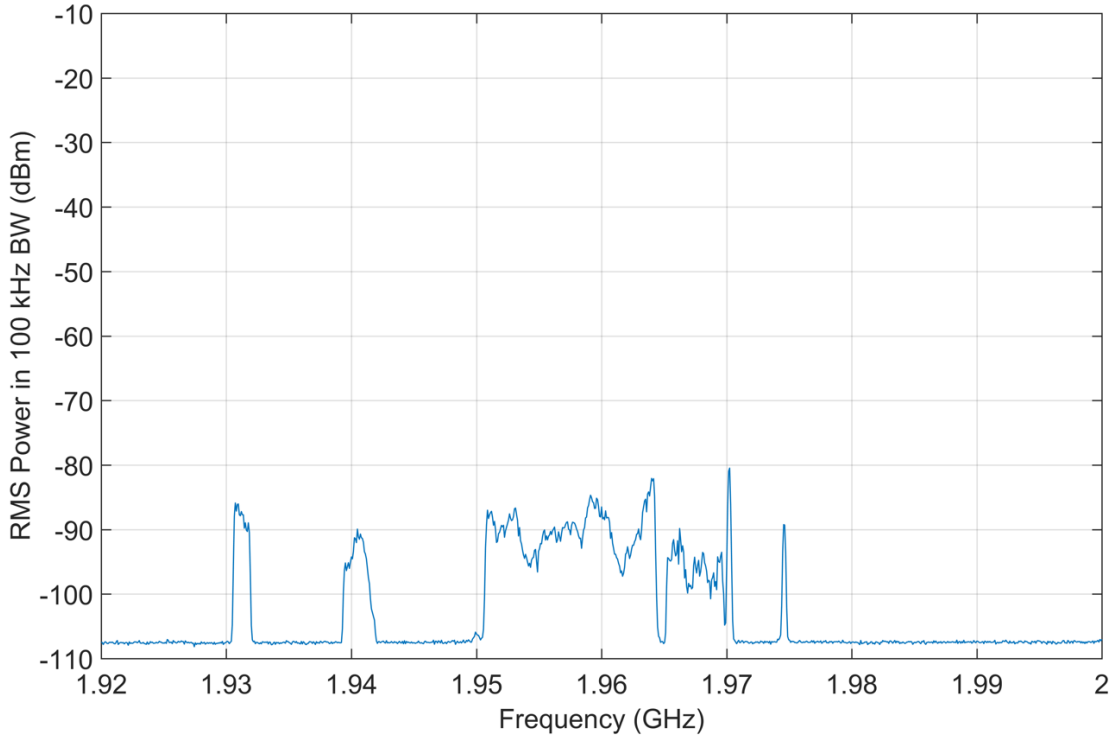


Figure 106. RMS average detection, jammer off, 1920–2000 MHz, 100 kHz bandwidth, single long (28 second) sweep, preamp on, location O-2 outside targeted prison cell.

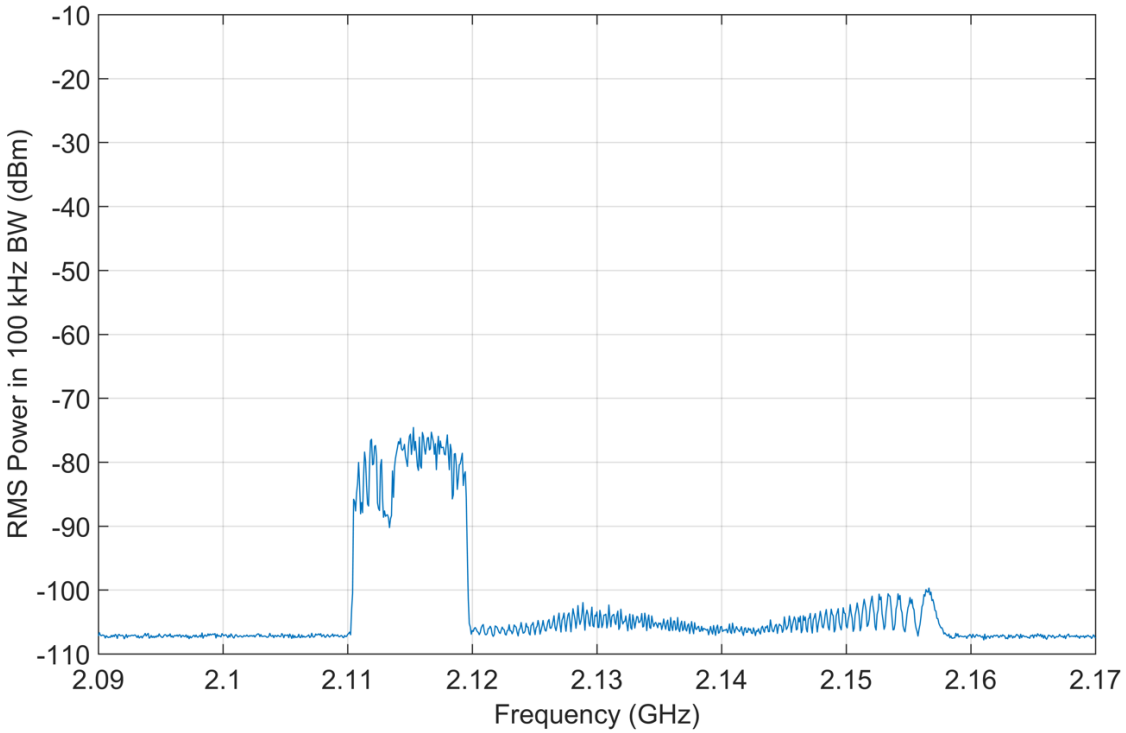


Figure 107. RMS average detection, jammer on, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-2 outside targeted prison cell.

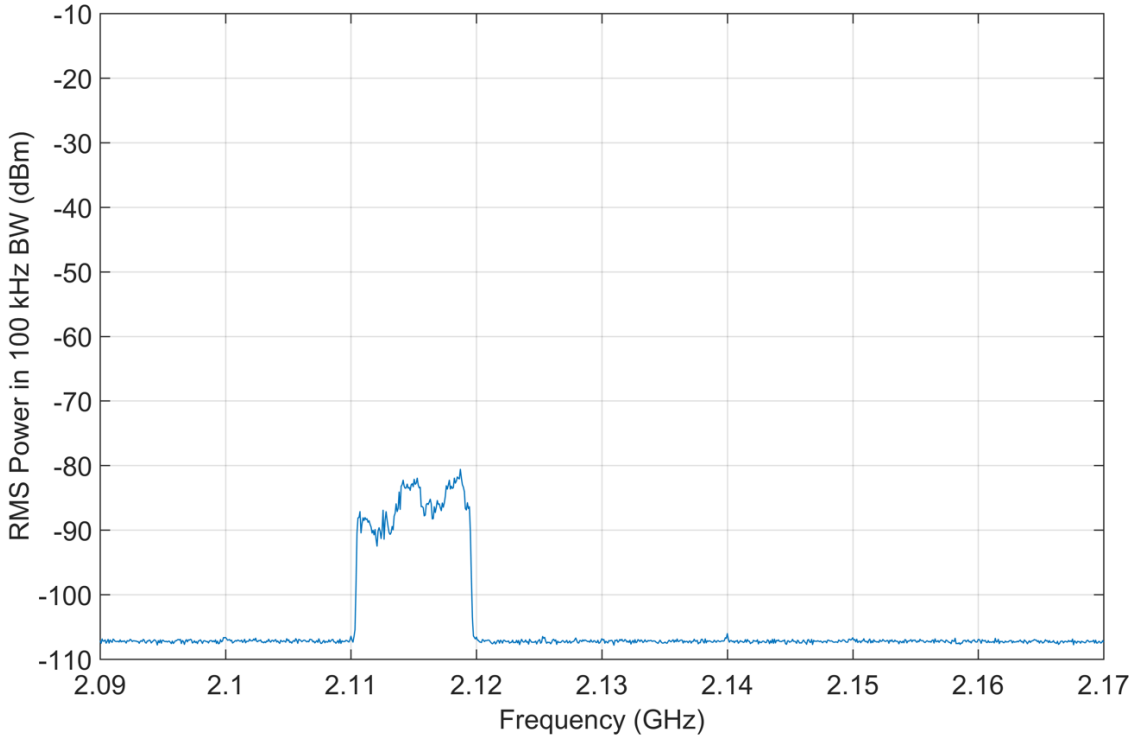


Figure 108. RMS average detection, jammer off, 2090–2170 MHz, 100 kHz bandwidth, single long (14 second) sweep, preamp on, location O-2 outside targeted prison cell.

# 5. DATA ANALYSIS

## 5.1 Time Domain Data Analysis

Figures 5–8 show the appearance of the jammer signal in each of the four CMRS bands when that signal is observed on a single frequency in time. Because the jammer sweeps through frequencies as time progresses (Figure 1), the jammer's signal is only present on any given frequency for a limited interval during each of the jammer's sweeps. This interval between the pulses will be uniform (equal from one to the next) only at the *center* of its chirping range in each operational band. At off-center frequencies in any chirping range, the pulses will occur at two unequal intervals: short, long, short, long, and so on. The ratio between these two intervals will go as the ratio of the frequency offset from the center of the chirping range divided by the chirping range itself. In Figure 5, the tuned frequency was 750 MHz, an offset of 7 MHz from the band's center frequency of 743 MHz. The total chirp range was (757 MHz – 729 MHz) = 28 MHz. The ratio of the offset to the chirping range was (7 MHz)/(28 MHz) = ¼. This causes the interval ratio (long:short) to go as ¾ to ¼, or 3:1 at this frequency, just as seen in Figure 5.

The *length* of that momentary appearance (a pulse width, effectively) is equal to the frequency sweep rate divided by the receiver's (in the case of this report, the spectrum analyzer's) IF bandwidth. For example, in the 750 MHz CMRS band, where the jammer sweeps across 28 MHz in 7.1 microseconds (μs), the rate of sweeping is 3.94 megahertz per microsecond, or 254 nanoseconds (ns) per megahertz.

In a 100 kHz ($^1\!/_{10}$ of a megahertz) bandwidth such as was used for many of this report's jammer measurements, this will create pulses that are 25.4 ns long. In the 180 kHz of an LTE RB, this pulse width would be 45.6 ns. But the shortest time response that any filter can generate is equal to the inverse of the filter's bandwidth. Therefore, for 100 kilohertz the jamming pulses would be seen to be no shorter than 10 μs long; in the 180 kilohertz width of an LTE RB the jamming pulses can be no shorter than (1/180 kHz) = 5.6 μs long. In a 1 MHz reference bandwidth, such as we used for our time domain measurements, these pulses will appear to be 1/(1 MHz) = 1 μs long. This is consistet with the observed 3 dB pulse widths of 1 μs in Figure 5.

In Table 6, the jammer pulse characteristics are compared to the bandwidth-limited responses of receivers using 180 kHz IF bandwidths (such as LTE RBs).[22] Since an LTE receiver's response to the 45.6 ns-duration chirped jamming pulses is bandwidth-limited to 5.6 μs, and since the intervals *between* jamming pulses will be about the same as that (a maximum interval of either 7.1 or 14.2 μs between pulses at the ends of a band and a minimum interval of 3.6 or 7.1 μs between pulses in the middle of the band), this means that such receivers will see the chirped-jamming pulses as nearly (but sometimes not quite) running together and thus looking like a nearly continuous signal in their bandwidth-limited IF stages. The blurring effect is demonstrated by the overlaps between the values of the two right-most columns in this table.

[22] LTE systems operate with clock intervals and signal-burst intervals of 10 ms, as observed by the authors in the course of other, unrelated LTE signal measurements. This is about 1800 times longer than the bandwidth-limited LTE interval of (1/180 kHz) = 5.6 μs.

Table 6. Jammer chirp-pulse characteristics *versus* effective pulse widths and intervals in 180 kHz bandwidth.

| CMRS Band (MHz) | CMRS Band Width (MHz) | Jammer One-Way Chirp Interval (μs) | Jammer Pulse Width Computed in 180 kHz (ns) | Bandwidth-Limited Pulse Width in 180 kHz IF (μs) | Pulse Interval in 180 kHz IF (μs) |
|---|---|---|---|---|---|
| 729–757 | 28 | 7.1 | 46 | 5.6 | 7.1–14.2 |
| 869–894 | 25 | 3.57 | 26 | 5.6 | 3.57– 7.14 |
| 1930–1990 | 60 | 7.1 | 21 | 5.6 | 7.1– 14.2 |
| 2110–2155 | 45 | 3.57 | 14 | 5.6 | 3.57–7.14 |

This behavior is exemplified in Figures 6–8. Here, the graphing time scale has been enlarged from the 140 μs of Figure 5 to a longer interval of 1000 μs. The IF bandwidth of the receiver (the spectrum analyzer) is still 1 MHz. The inverse of this measurement bandwidth, 1000 ns, is more than an order of magnitude longer than the tens of nanosecond intervals that are seen in the fourth column of Table 6. We expect to see the individual jammer pulses blur together to approach something like a continuous carrier wave in these figures. And that is exactly what those figures show. This smearing-out in the time domain, and the consequent approach to a carrier wave characteristic for the jammer signal, will be even more pronounced in a narrower 180 kHz RB bandwidth. This approach to continuous energy in a receiver bandwidth would be expected to enhance the jammer's effectiveness.

## 5.2 Spectrum Data Analysis

### 5.2.1 Lobed Appearance of Jammer Spectra

Inspection of the spectrum data graphs (jammer-on Figures 9 through A-31) shows that the jammer spectra have a distinctly lobed appearance. The power level of the lobes is highest at the band edges; power levels are lower in the center of each chirp range. This spectrum shape is consistent with the jammer's chirped modulation. Chirped-carrier wave modulations in the time domain Fourier-transform into the frequency domain (via Fresnel integrals) into such spectra.

We do not analyze these lobed structures in this report. But we do note that such structures are determined, ultimately, by the dimensionless time-bandwidth products of the chirping. The time-bandwidth products of the jammer in each of the CMRS bands are shown in Table 7.

Table 7. Time-bandwidth products of the jammer in each CMRS band.

| CMRS Band (MHz) | Bandwidth (MHz) | Chirp Intervals (μs) | Time-Bandwidth Products (Dimensionless) |
|---|---|---|---|
| 729–757 | 28 | Half = 7.1; Full = 14.2 | Half = 199; Full = 398 |
| 869–894 | 25 | Half = 3.57; Full = 7.14 | Half = 89; Full = 179 |
| 1930–1990 | 60 | Half = 7.1; Full = 14.2 | Half = 426; Full = 852 |
| 2110–2155 | 45 | Half = 3.57; Full = 7.14 | Half = 161; Full = 321 |

### 5.2.2 Jammer Signal Relative to CMRS Signals

As shown in Figures 5–16, 25–32, 45–52, and 61–68 (100 kHz peak data); A-1 to A-32 (1 MHz peak data); and 77–108 (100 kHz RMS average data), the jammer signal had the following characteristics in the CMRS bands at the four measurement locations. Within the targeted prison cell, the jammer signal was substantially stronger than the ambient CMRS signals. Outdoors, the jammer signal power was reduced compared to the ambient CMRS signals. Tables 8 and 9 show the relative power levels of CMRS and jammer signals at all measurement locations for both mean peak and RMS average in 100 kHz bandwidth.

Table 8. Jammer power levels, relative to CMRS signals, mean peak statistics, 100 kHz bandwidth.

| | **I-1 power, dBm** | | **I-2 power, dBm** | | **O-1 power, dBm** | | **O-2 power, dBm** | |
|---|---|---|---|---|---|---|---|---|
| **CMRS Band** | CMRS | Jammer | CMRS | Jammer | CMRS | Jammer | CMRS | Jammer |
| 729–757 | -65 to -90 | -36 to -44 | -65 to -90 | -45 to -55 | -65 to -85 | -70 to -75 | -65 to -85 | -70 to -80 |
| 869–894 | -85 to -90 | -35 to -43 | -85 to -90 | -54 to -60 | -65 to -80 | -80 to -85 | -70 to -80 | -82 to -90 |
| 1930–1990 | -95 | -54 to -60 | -95 | -67 to -73 | -75 to -90 | -85 to -90 | -75 to -86 | -97 |
| 2110–2155 | -91 | -50 to -61 | -95 | -59 to -68 | -63 | -89 to -95 | -80 | -97 |

Table 9. Jammer power levels, relative to CMRS signals, RMS average, 100 kHz bandwidth.

| | **I-1 power, dBm** | | **I-2 power, dBm** | | **O-1 power, dBm** | | **O-2 power, dBm** | |
|---|---|---|---|---|---|---|---|---|
| **CMRS Band** | CMRS | Jammer | CMRS | Jammer | CMRS | Jammer | CMRS | Jammer |
| 729–757 | -81 | -40 to -50 | -78 | -50 to -65 | -70 to -95 | -80 to -75 | -70 to -95 | -85 |
| 869–894 | < -83 | -40 to -50 | < -83 | -60 to -70 | -72 to -90 | -90 | -80 | -95 |
| 1930–1990 | < -83 | -70 | < -83 | -75 | -90 | -100 | -85 to -100 | -105 |
| 2110–2155 | < -83 | -59 to -65 | < -83 | -65 to -80 | -70 | -100 | -85 | -105 |

### 5.2.3 Jammer Signals Observed Outside CMRS Bands

Figures 17–24, 33–40, 53–60, and 69–76 were used to determine the extent to which jammer signals were observed at any of the measurement locations outside the operational (intentional) jamming bands. Table 10 summarizes these observations.

Jammer signals were identified outside the CMRS bands based on their known bands of intentional operation and their chirped fundamental-frequency bandwidths.

Table 10. Jammer signals observed in other bands.

| **Source Figure** | **Location** | **Frequencies (MHz)** | **Power Relative to Jammer $f_0$ in CMRS Band (dB)** | **Comments** |
|---|---|---|---|---|
| 19 | I-1 | 1458–1514 | -24 | 2nd harmonic of 729–757 MHz |
| 23 | I-1 | 4220–4310 | -7 | 2nd harmonic of 2110–2155 MHz |
| 75 | O-2 | 4260–4310 | -12 | 2nd harmonic of 2110–2155 MHz |

The frequency range 1458–1514 MHz is used by mobile aeronautical telemetry. The frequency range 4220–4310 is used by airborne radio altimeters (the allocated band for altimeters being 4200–4400 MHz).

A few other signals of interest were noted in the non-CMRS bands, but they were not produced by the jammer. These were: Figure 55, location O-1, 1215–1440 MHz, local long range radar (either a Common Air Route Surveillance Radar or an Air Route Surveillance Radar); Figure 69, location O-2, 780–800 MHz, possible local Public Safety communications; and Figure 75, location O-2, 1715 MHz, a probable local repeater or other terrestrial mobile-network communication signal.

### 5.2.4 Aggregated Jammer Emission Considerations

The micro-jammer that was measured was a single unit. Many such micro-jammer transmitter units, on the order of a fifty to a hundred per housing unit,[23] would be required to effectively deny wireless service throughout any given facility such as Cumberland FCI. When multiple transmitters operate together, the sum total of all of their radio emission power will combine (aggregate) together as radiation into space. The way that the signals from the individual jammer transmitters will sum at locations within a facility will be complex and will vary considerably within each facility. With increasing distance from the boundaries of a facility, however, the facility itself will look increasingly like a point source to receivers that look in its direction. In that limiting case, the aggregate power of all of the deployed jammer transmitters will tend to sum in direct proportion to the total number of transmitters within the facility boundaries. Assessment of the aggregation effects of multiple jammer transmitters is beyond the scope of this report. Such assessment would require either measurements of a deployed aggregate at a facility (within one or more housing units), or else detailed theoretical modeling and analysis of a proposed deployment at a facility (again, within one or more housing units).

### 5.2.5 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, but with all other measurement factors being held constant (see Figures 9, 11, 13, 15, 25, 27, 29, and 31 for these 100 kHz data and Figures A-1, A-5, A-7, A-9, A-11, A-13, and A-15 for the comparative 1 MHz data) can be used to determine the rate at which peak-detected jammer power varies as a function of receiver bandwidth, as discussed above in Section 3.2.2. Table 11 shows these differences between the 100 kHz and 1 MHz spectra.

[23] There are, for example, eight medium security housing units at Cumberland FCI.

Table 11. Differences between mean peak-detected jammer emission spectra for 100 kHz and 1 MHz bandwidths.

| CMRS Band (MHz) | Location: Figure (100 kHz) | L, M, R Power Levels (dBm) | | | Location: Figure (1 MHz) | L, M, R Power Levels (dBm) | | | Deltas: 1 MHz minus 100 kHz (dB) | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 729–757 | I-1: 9 | -36 | -43 | -33 | I-1: A-1 | -22 | -22 | -20 | 14 | 21 | 13 |
| 869–894 | I-1: 11 | -35 | -42 | -35 | I-1: A-3 | -20 | -25 | -18 | 15 | 17 | 17 |
| 1930–1990 | I-1: 13 | -55 | -60 | -55 | I-1: A-5 | -40 | -41 | -42 | 15 | 19 | 13 |
| 2110–2155 | I-1: 15 | -50 | -60 | -52 | I-1: A-7 | -31 | -42 | -38 | 19 | 18 | 14 |
| 729–757 | I-2: 25 | -44 | -55 | -50 | I-2: A-9 | -30 | -35 | -35 | 14 | 20 | 15 |
| 869–894 | I-2: 27 | -57 | -60 | -53 | I-2: A-11 | -40 | -42 | -38 | 17 | 18 | 15 |
| 1930–1990 | I-2: 29 | -68 | -73 | -66 | I-2: A-13 | -48 | -50 | -50 | 20 | 23 | 16 |
| 2110–2155 | I-2: 31 | -59 | -68 | -60 | I-2: A-15 | -45 | -50 | -45 | 14 | 18 | 15 |

For each of the indoor locations, the power levels of the mean peak-detected curves were taken at the left horn, the middle frequency, and the right horn of the emission spectra in each of the two bandwidths. These levels (L, M, and R, respectively) are shown in the third and fifth columns of Table 11. The differences between the corresponding values in the two bandwidths are shown in the last column of the table.

The decibel average of the differences is[24] 16.7 dB. The decibel variance[25] is 7 dB. The decibel standard deviation[26] is 2.6 dB.

So the rate of change of the mean peak-detected jammer power is $16.7 \cdot \log(B_2/B_1)$ $\pm 2.6 \cdot \log(B_2/B_1)$, where $B_1$ and $B_2$ are any two bandwidths. According to [7], the peak-detected relationship would go as 10log for a continuous signal (and noise) and would go as 20log for a pulsed signal. The empirically determined coefficient of 16.7 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.

This intermediate value of the coefficient between 10 and 20 is, further, consistent with the time domain behavior of the bandwidth-limited jammer signal as described in Section 5.1 and shown in Figures 6–8. The relative closeness of 16.7 to 20 (pulse-like coefficient) relative to 10 (continuous signal coefficient) implies that the jammer signal is seen by the measurement system (or a CMRS receiver) as being more pulse-like than continuous when it is peak-detected.

[24] Sum of all decibel differences = 400, divided by 24 data point values.
[25] Sum of all of the squared decibel differences between each of the 24 deltas and the average of 16.7 dB, divided by 24.
[26] Square root of variance.

### 5.2.6 Jammer Peak to Average Power Ratio and Expected Average Power Variation with Bandwidth

Table 12 lists the differences between mean peak levels and RMS average power levels for the jammer as measured at indoor locations I-1 and I-2.

Table 12. Differences between mean peak and RMS average jammer levels in 100 kHz bandwidth.

| CMRS Band (MHz) | Location: Figure (100 kHz) | L, M, R Mean Peak Power Levels (dBm) | | | Location: Figure (100 kHz) | L, M, R RMS Average Power Levels (dBm) | | | Deltas: Peak minus Average (dB) | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 729–757 | I-1: 9 | -36 | -43 | -33 | I-1: 77 | -45 | -50 | -40 | 9 | 7 | 7 |
| 869–894 | I-1: 11 | -35 | -42 | -35 | I-1:figures t79 | -41 | -49 | -41 | 6 | 7 | 6 |
| 1930–1990 | I-1: 13 | -55 | -60 | -55 | I-1: 81 | -63 | -69 | -68 | 8 | 9 | 13 |
| 2110–2155 | I-1: 15 | -50 | -60 | -52 | I-1: 83 | -55 | -65 | -58 | 5 | 5 | 6 |
| 729–757 | I-2: 25 | -44 | -55 | -50 | I-2: 85 | -50 | -61 | -55 | 6 | 6 | 5 |
| 869–894 | I-2: 27 | -57 | -60 | -53 | I-2: 87 | -60 | -65 | -60 | 3 | 5 | 7 |
| 1930–1990 | I-2: 29 | -68 | -73 | -66 | I-2: 89 | -71 | -75 | -71 | 3 | 2 | 5 |
| 2110–2155 | I-2: 31 | -59 | -68 | -60 | I-2: 89 | -69 | -63 | -65 | 10 | -5 | 5 |

The mean decibel difference between the 24 mean peak and RMS average values in Table 12 is[27] 5.8 dB. The decibel variance[28] is 10.5 dB. The decibel standard deviation[29] is 3.2 dB. So the peak-to-average ratio for the jammer signal, in a 100 kHz bandwidth, is 6 dB ±3 dB. This peak to average relationship is explored further in Appendix B.

The RMS average-detected jammer signal power should vary directly with bandwidth, due to energy conservation considerations. This is discussed further in [7] and Appendix B. The rate of variation of the average-detected jammer signal will be at, or slightly less than, $10 \cdot \log(B_{rx}/B_c)$ where $B_{rx}$ is the receiver or measurement bandwidth and $B_c$ is the chirped bandwidth. This is discussed further in Appendix B.

### 5.2.7 Jammer Power in 180 kHz RB Bandwidth and Full Bandwidth

Using the information developed above, Table 13 shows the expected jammer power, peak and average, in an RB bandwidth of 180 kHz.

[27] Sum of differences equals 140 divided by 24.
[28] Sum of the squares of the differences between the deltas and the mean of 5.8 dB, which is (251.36/24).
[29] The square root of the variance.

Table 13. Jammer signal power in bandwidth of 180 kHz.

| CMRS Band (MHz) | Power in 100 kHz (RMS average = 0 dB in 100 kHz) | | Relative Power in 180 kHz (dB) | |
|---|---|---|---|---|
| | Average | Peak | Average | Peak |
| 729–757 | 0 | +6 | +2.6 | +10.3 |
| 869–894 | 0 | +6 | +2.6 | +10.3 |
| 1930–1990 | 0 | +6 | +2.6 | +10.3 |
| 2110–2155 | 0 | +6 | +2.6 | +10.3 |

### 5.3 Conversion of Circuit-Power Data to Incident Field Strength Units

The data in Figures 5 through 108 and A-1 through A-32 are graphed in units of dBm per unit measurement bandwidth with a given detection mode. These are units of power in the measurement system's 50 ohm circuitry at the antenna terminals. These data can be converted into incident field strength at the antenna. From (20) in [8], this conversion is:

$$FS = P_{load} + 77.2 - G_{meas\_ant} + 20 \cdot \log(f)$$

where:

$FS$ = incident field strength, decibels relative to a microvolt per meter (dBμV/m);

$P_{load}$ = power measured in a circuit, dBm;

$G_{meas\_ant}$ = gain of the measurement antenna relative to isotropic (dBi);

$f$ = frequency of the measurement (MHz).

For the Cumberland FCI measurement system (with its +2 dBi gain antenna), for example, a measured power of -80 dBm at 880 MHz would correspond to an incident field strength of:

$$FS = (-80 \text{ dBm} + 77.2 \text{ dB} - 2 \text{ dBi} + 20 \cdot \log(880)) = +54 \text{ dB}\mu\text{V/m}.$$

Field strength is a measure of incident power per unit area.[30] This conversion makes it possible to compare jammer levels to radhaz recommendations and limits. This topic is taken up at length in Section 4 of [8]. Table 14 charts conversions of circuit power to incident field strength for the Cumberland FCI data.

Note that only RMS average-detected power levels (not peak detected levels) should be compared to radhaz levels, per discussion in [8]. Note, too, that *total* RMS average power in the

[30] The stated units of microvolts per meter in field strength are actually squared; confusion is caused because the squaring is dropped for convenience in the shorthand notation for field strength. A voltage squared is a power unit. A length squared is an area. So microvolts squared per meter squared is power per unit area.

full bandwidths of the transmitter, as shown in the left-hand side of the last column of Table 13, should be used in radhaz integrations across all operational jammer frequencies.

Table 14. Power-Unit Conversions for Cumberland FCI data.

| **Measured Power (dBm)** | **dBμV/m 740 MHz** | **dBμV/m 880 MHz** | **dBμV/m 1960 MHz** | **dBμV/m 2130 MHz** |
|---|---|---|---|---|
| -10 | 122.6 | 124.0 | 131.0 | 131.8 |
| -20 | 112.6 | 114.0 | 121.0 | 121.8 |
| -30 | 102.6 | 104.0 | 111.0 | 111.8 |
| -40 | 92.6 | 94.0 | 101.0 | 101.8 |
| -50 | 82.6 | 84.0 | 91.0 | 91.8 |
| -60 | 72.6 | 74.0 | 81.0 | 81.8 |
| -70 | 62.6 | 64.0 | 71.0 | 71.8 |
| -80 | 52.6 | 54.0 | 61.0 | 61.8 |
| -90 | 42.6 | 44.0 | 51.0 | 51.8 |
| -100 | 32.6 | 34.0 | 41.0 | 41.8 |
| -110 | 22.6 | 24.0 | 31.0 | 31.8 |

## 6. SUMMARY

1) A contraband wireless device micro-jammer that was operated in four CMRS bands was temporarily installed and operated under an STA for a single day inside a Cumberland, Maryland FCI medium security housing unit. This micro-jammer, installed inside a utility closet, radiated its signal through a wall (concrete and steel, unspecified thickness) to a targeted prison cell on the other side. The cell was located on the ground floor. It had a single barred window to the outside. A commercially available light-reflective coating with unspecified electrical characteristics was temporarily installed on the outside of the window for the purpose of reducing the amount of jamming power that radiated outdoors.

2) The jammer consisted of a single unit containing four transmitters and associated antennas. The transmitters simultaneously produced sawtoothed FM (chirped) carrier waves that covered the CMRS bands 729–757 MHz, 869–894 MHz, 1930–1990 MHz, and 2110–2155 MHz. The jammer transmitters each produced 0.9 W per band, delivered into respective radiating antennas (combination of vertically and horizontally polarized) of +3 dBi gain. The unknown electrical characteristics of the wall through which the jammer radiated makes the unit's ERP unknown, other than that it was less than the sum of the transmitter power and the antenna gain, that is, it was less than +32.5 dBm.

3) The unit was operated in on *versus* off states while emission measurements proceeded at four locations: two places inside the targeted cell and two places outdoors, adjacent to the targeted cell. The outdoor locations were 6.1 m (20 ft) and 30.5 m (100 ft) outside the building, with clear LOS to the window of the targeted prison cell.

4) NTIA performed in-band (CMRS band) and adjacent-band, OoB, spurious, and harmonic band measurements of the jammer emissions relative to the ambient CMRS signal levels at the four specified measurement locations. The results of those measurements are provided in this report.

5) Our data show that inside the targeted jamming zone (the prison cell interior), the jammer signal power levels substantially exceeded those of the CMRS signals, as summarized in Table 8 and Table 9 of this report. At the outdoor measurement locations, the jammer signals were substantially lower than indoors and the ambient CMRS signals were substantially higher in power than indoors. The range of signal power levels observed for the jammer *versus* the ambient CMRS signals at these locations are summarized in Table 8 and Table 9.

6) Lack of accepted quantitative engineering criteria for jammer effectiveness within a targeted jamming zone and for harmful interference outside a targeted jamming zone make it impossible for us to state, based solely on the measured jamming signal power levels and ambient CMRS signal levels, the effectiveness of the micro-jammer or its potential for causing harmful interference. The data in this report could be used for such analysis if (or when) such criteria are ever developed.

7) 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 CMRS receivers (e.g., *S/I* thresholds) should be

developed if jamming technology is to be further developed for application in prison environments. Theoretical analytical and numerical models should be used in conjunction with selected laboratory measurements to determine these criteria.

8) Outside the targeted CMRS bands, the only spurious signals observed from the jammer were second harmonics of the 729–757 MHz band and the 2110–2155 MHz band. These harmonics, falling in aeronautical mobile telemetry and airborne radio altimeter bands, respectively, were about 24 dB lower than the intentional emission level for the associated 750 MHz band and 7 to 15 dB lower than the intentional emission for the 2.1 GHz band.

9) The results presented in this report are idiosyncratic to the technical particulars of this jammer transmitter and the housing unit building in which its signal was radiated. Different results would be expected for any given jammer installation at any given location.

10) Aggregate emissions from the numbers of micro-jammers that would be required to provide denial-of-service coverage to entire facilities such as Cumberland FCI will represent the sum total of emission power for those groups of jammers in such facilities. Seen at a distance from the facility, the total, aggregate power for such assemblages will tend to increase in direct proportion to the number of such transmitters deployed in each facility. It has been estimated that 50 to 100 jammer transmitters like the one observed in this report might be required to cover a single, large-size housing unit in a prison facility. There are eight such medium security housing units at Cumberland FCI, for example. Assessment of the aggregation effects of multiple jammer transmitters is beyond the scope of this report. Such assessment would require either a full micro-jammer deployment at a prison facility, or else a detailed theoretical-analytical study for a given facility, including detailed propagation modeling of all of the facilitiy's walls, ceilings, and floors.

11) Measured characteristics in the time domain are consistent with the chirped modulation of the micro-jammer transmitter.

12) Measured emission spectra have a lobed structure that is consistent with the chirped modulation of the micro-jammer transmitter.

13) Jammer transmitter detected peak power goes as 16.7·log(receiver IF bandwidth) for any given receiver. Detected average power will go as 10·log(receiver IF bandwidth) for any receiver. See Appendix B for experimental confirmation and further discussion of this topic.

14) The total-power emission bandwidth for the jammer transmitter goes, band-by-band, according to the values of Table 2. For peak detection the power-limiting bandwidths run between 1.4 and 2.5 MHz; for average detection the power limiting bandwidths are slightly wider than the chirp bandwidth, $B_c$. See Appendix B for further discussion.

15) The data in this report can be used with the unit conversion information provided in Section 5.3 and the supplemental material of [8] to compare with radhaz recommendations and limits.

## 7. REFERENCES


[1] 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://its.bldrdoc.gov/publications/2504.aspx.

[2] 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://its.bldrdoc.gov/publications/2503.aspx.

[3] Sanders, F. H, J. E. Carroll; G. A. Sanders and R. L. Sole, "Effects of Radar Interference on LTE Base Station Receiver Performcne," NTIA Technical Report 14-499, U.S. Dept. of Commerce, Dec. 2010. https://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://its.bldrdoc.gov/publications/2759.aspx.

[5] 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://its.bldrdoc.gov/publications/2481.aspx.

[6] 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://its.bldrdoc.gov/publications/2760.aspx.

[7] 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/download/12-488.pdf.

[8] Sanders F. H., "Derivations of Relationships Among Field Strength, Power in Transmitter-Receiver Circuits and Radiation Hazard Limits," NTIA Technical Memorandum TM-10-469, U.S. Dept. of Commerce, Jun. 2010. https://www.its.bldrdoc.gov/publications/2507.aspx.

## APPENDIX A: JAMMER EMISSIONS MEASURED IN 1 MHZ BANDWIDTH

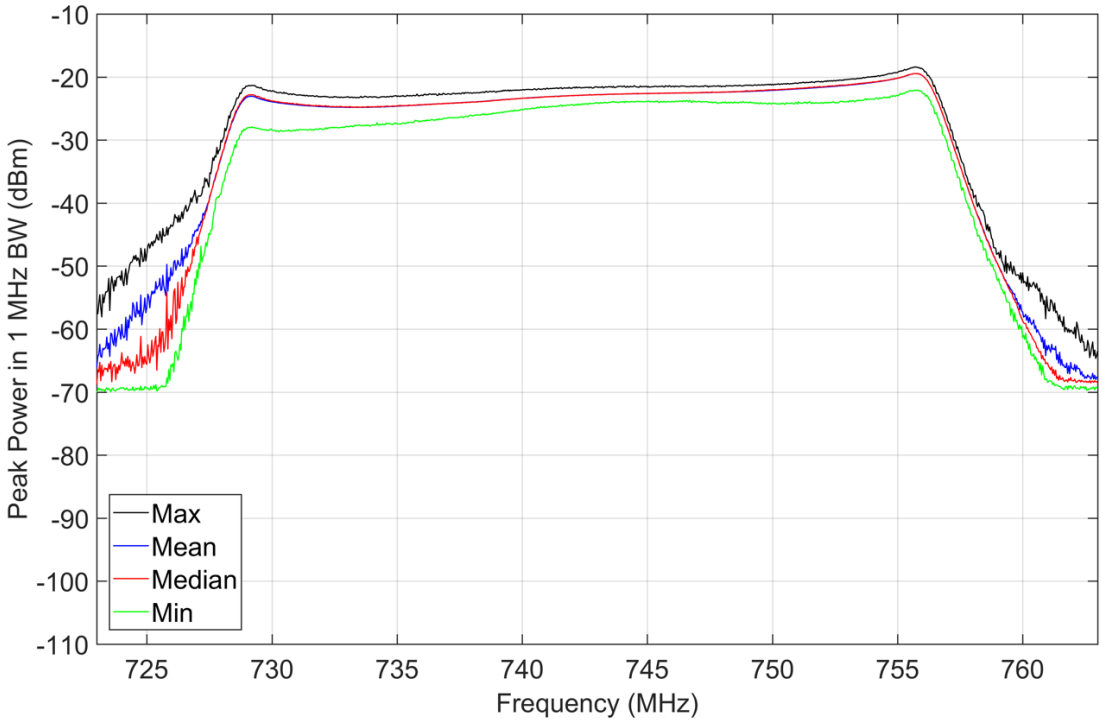


Figure A-1. M4 statistics, peak detection, jammer on, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

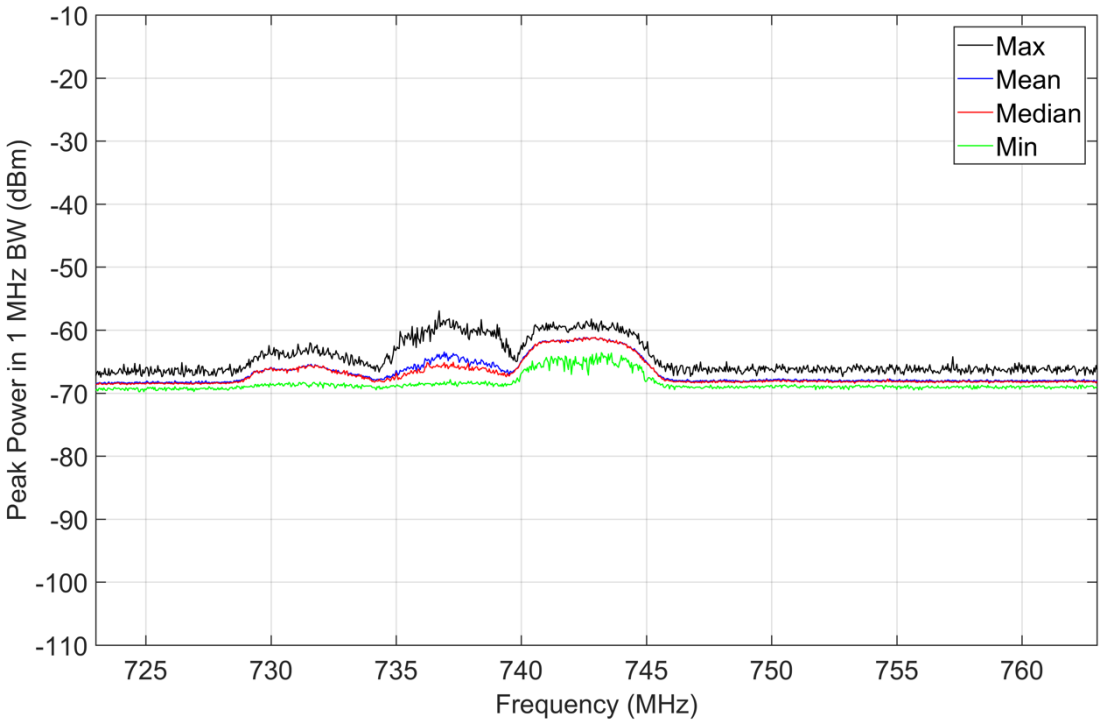


Figure A-2. M4 statistics, peak detection, jammer off, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

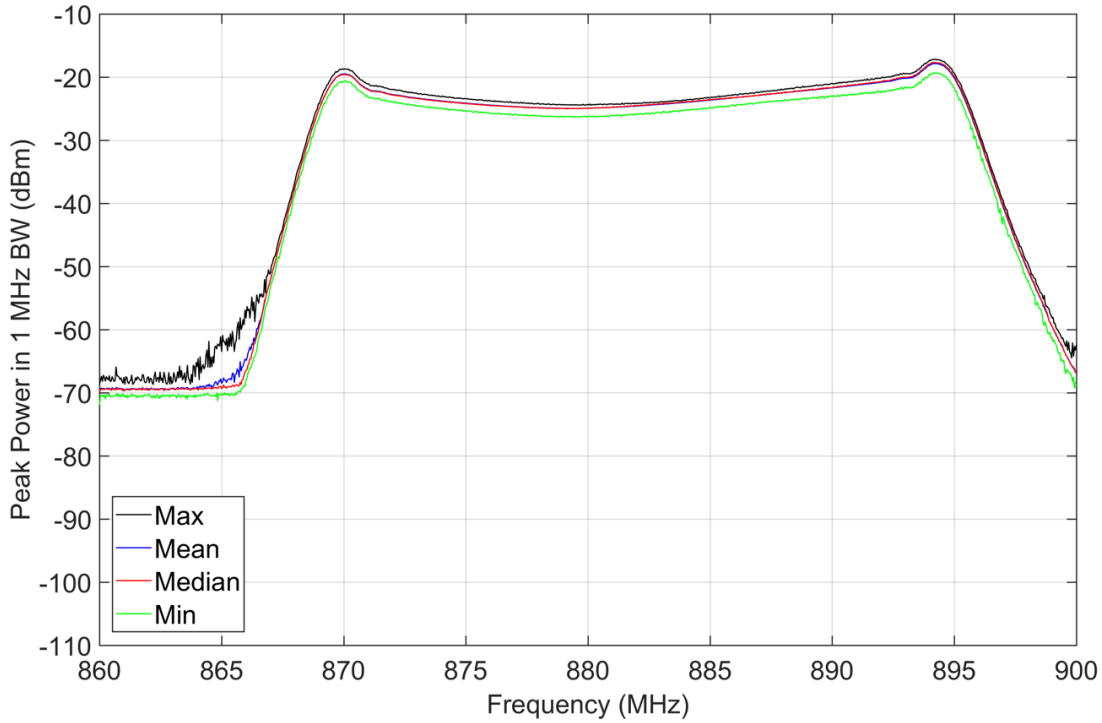


Figure A-3. M4 statistics, peak detection, jammer on, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

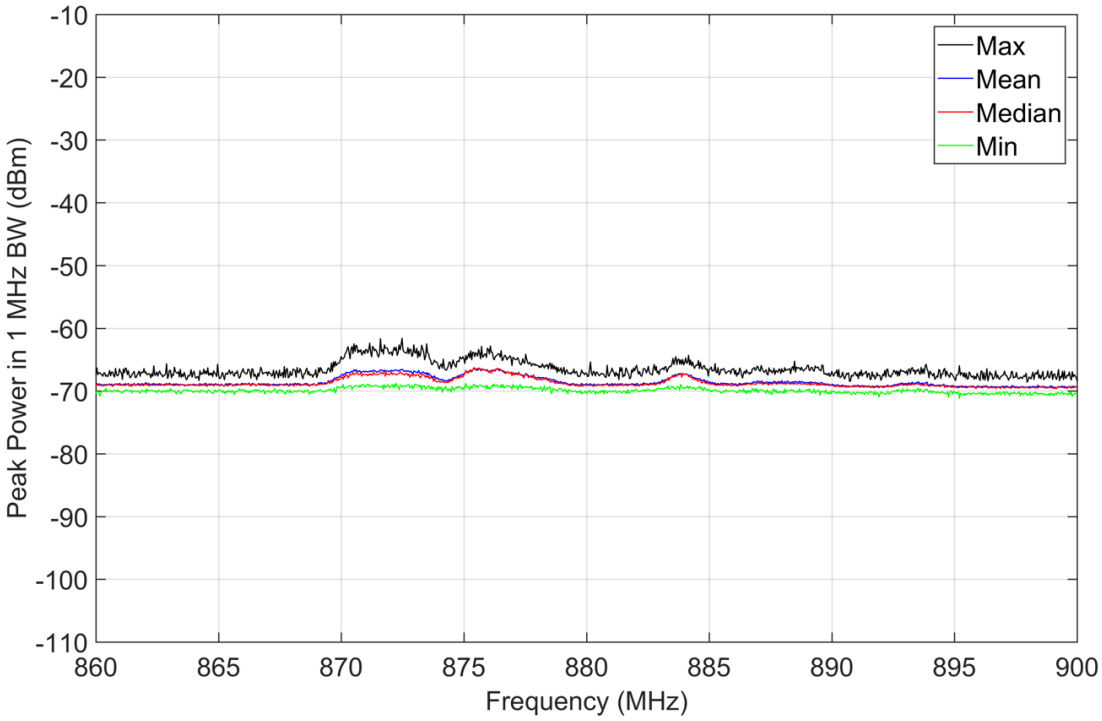


Figure A-4. M4 statistics, peak detection, jammer off, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

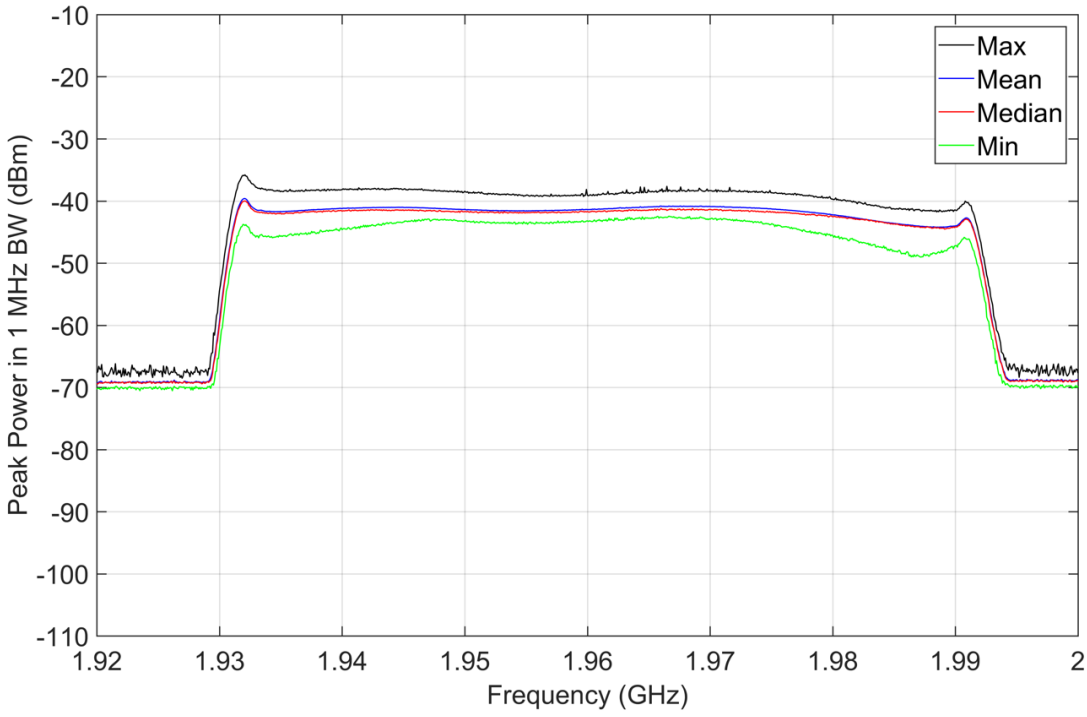


Figure A-5. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

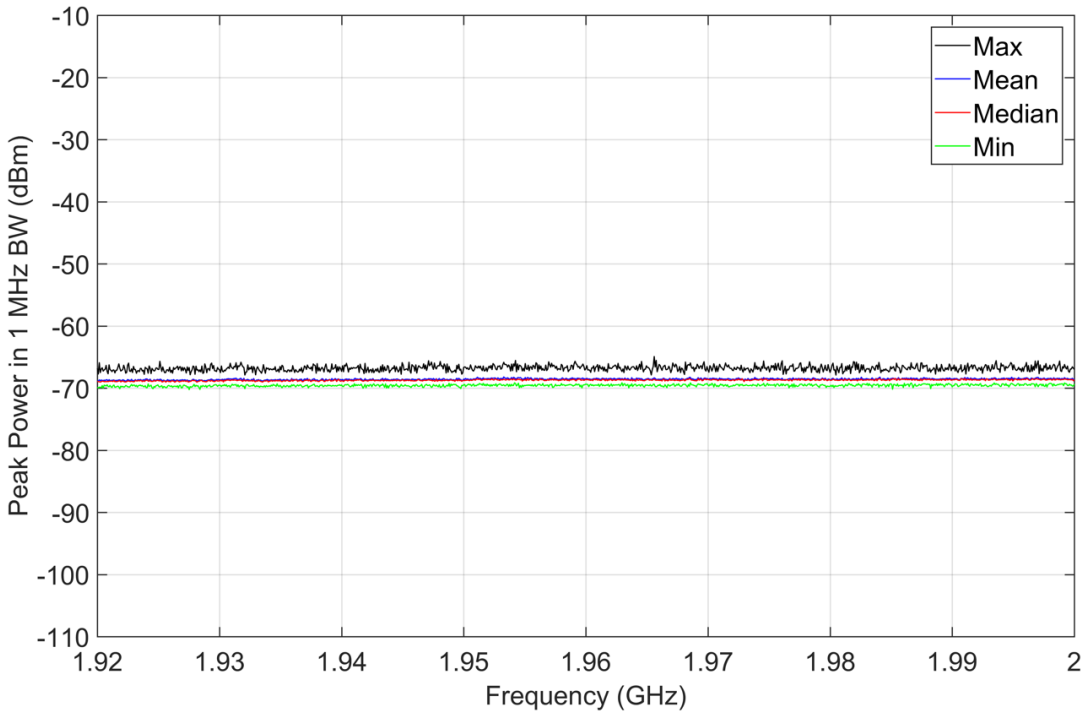


Figure A-6. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

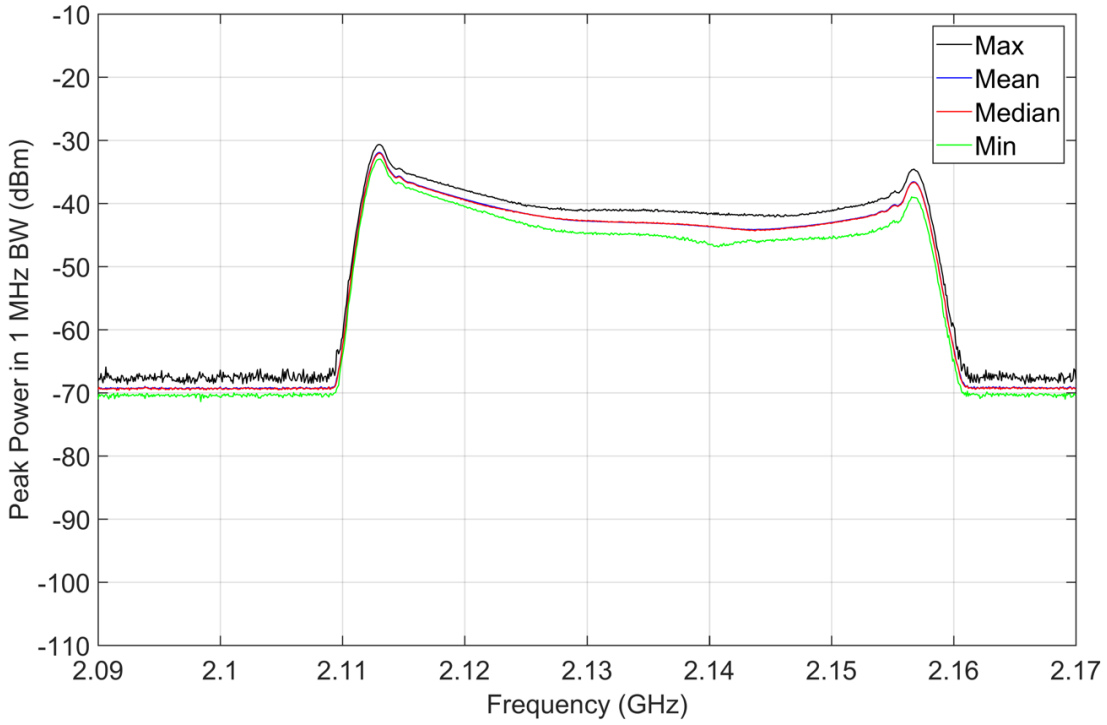


Figure A-7. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

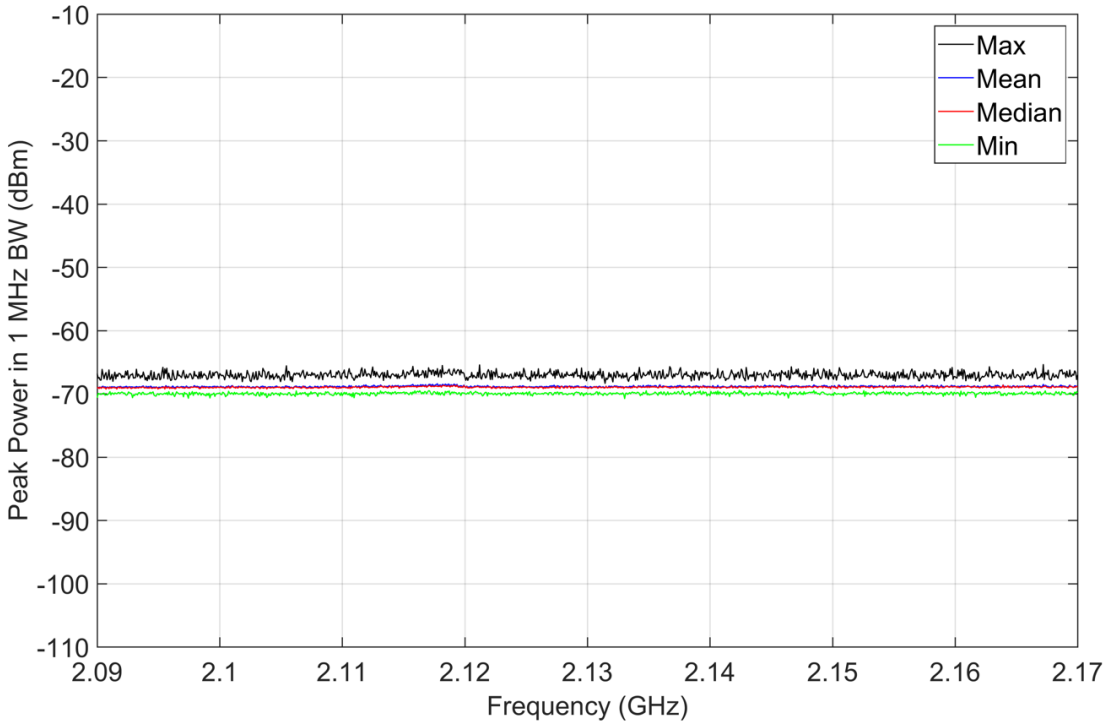


Figure A-8. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-1 inside targeted prison cell.

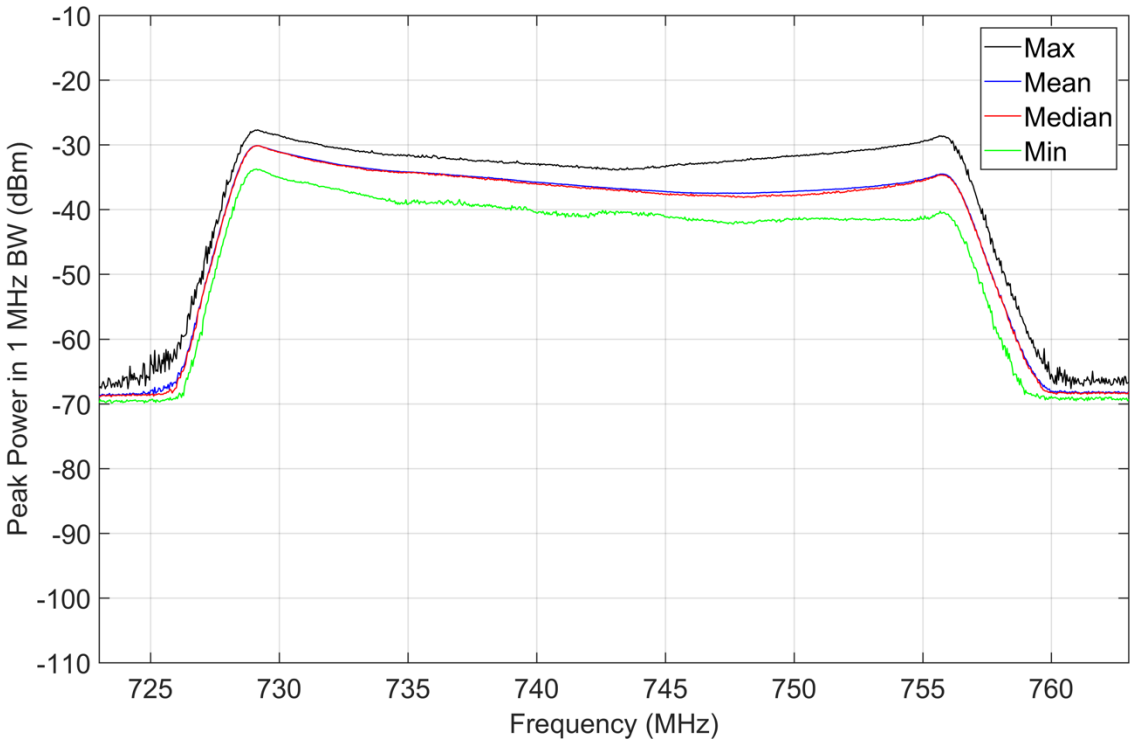


Figure A-9. M4 statistics, peak detection, jammer on, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

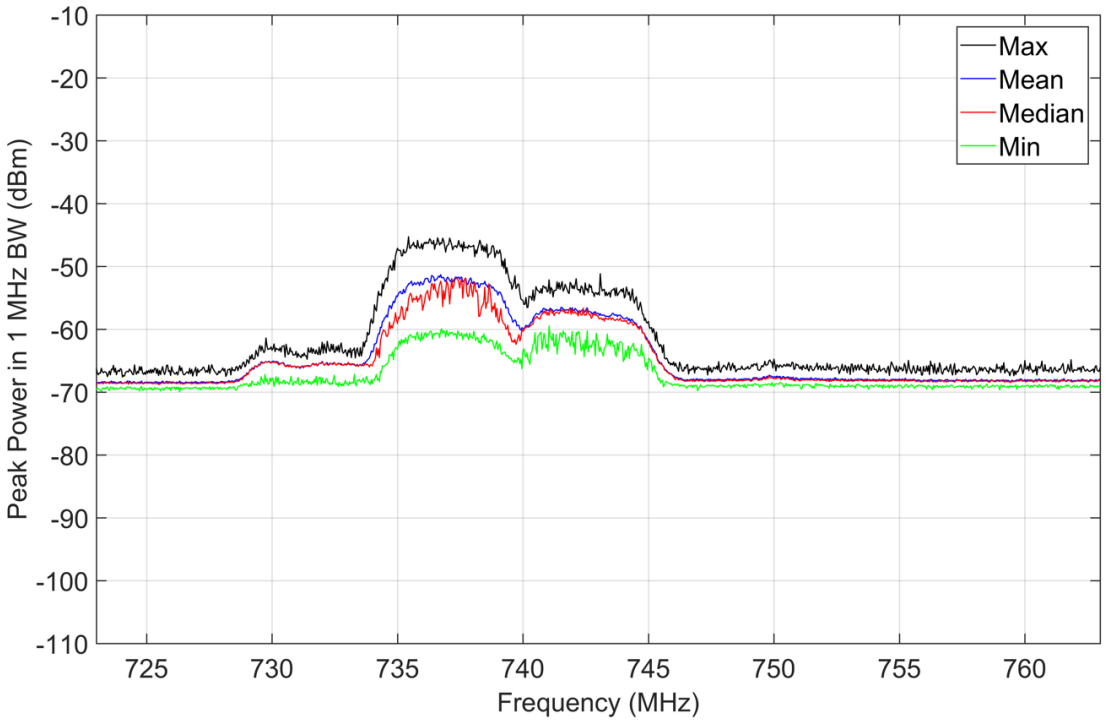


Figure A-10. M4 statistics, peak detection, jammer off, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

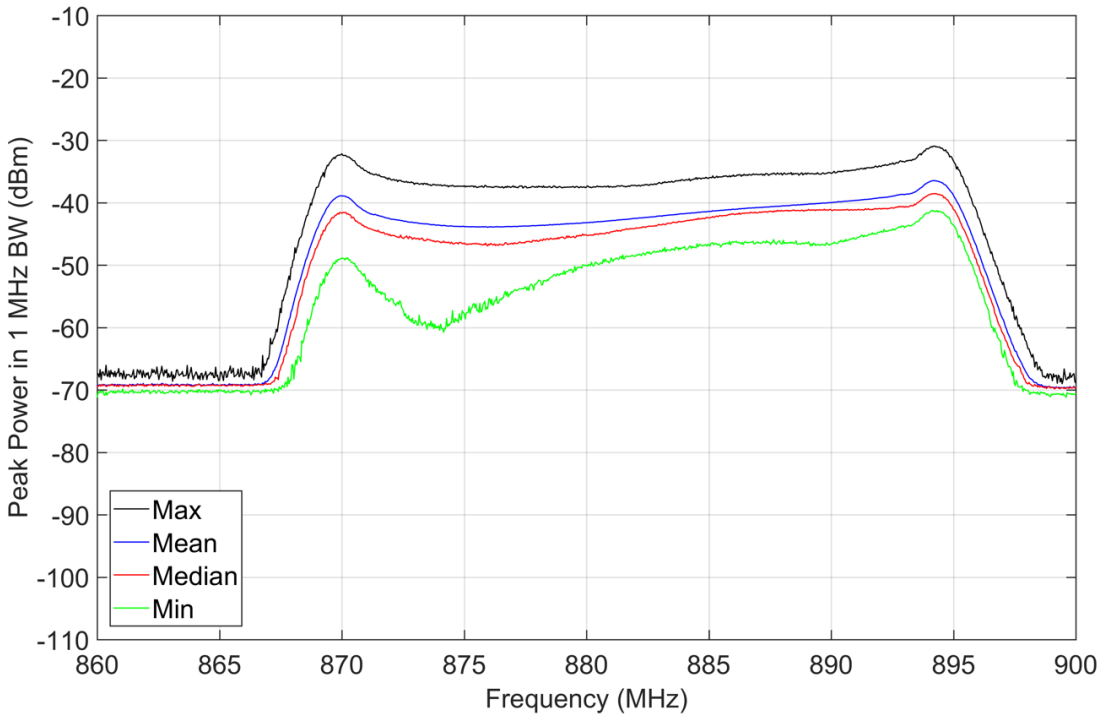


Figure A-11. M4 statistics, peak detection, jammer on, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

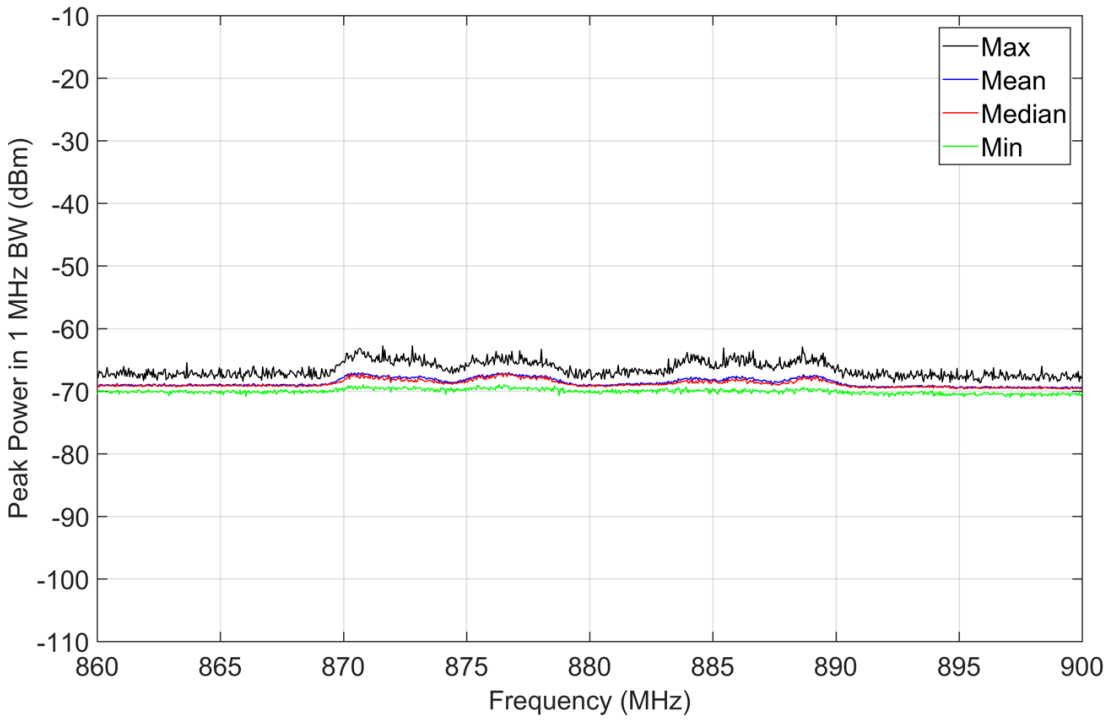


Figure A-12. M4 statistics, peak detection, jammer off, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

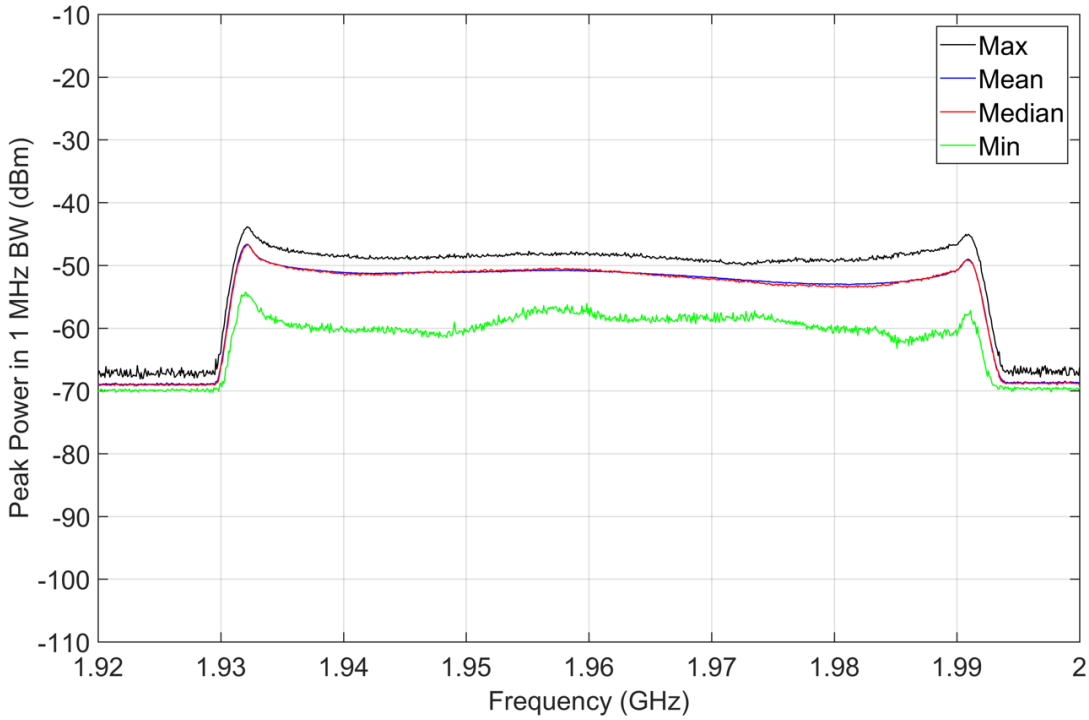


Figure A-13. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

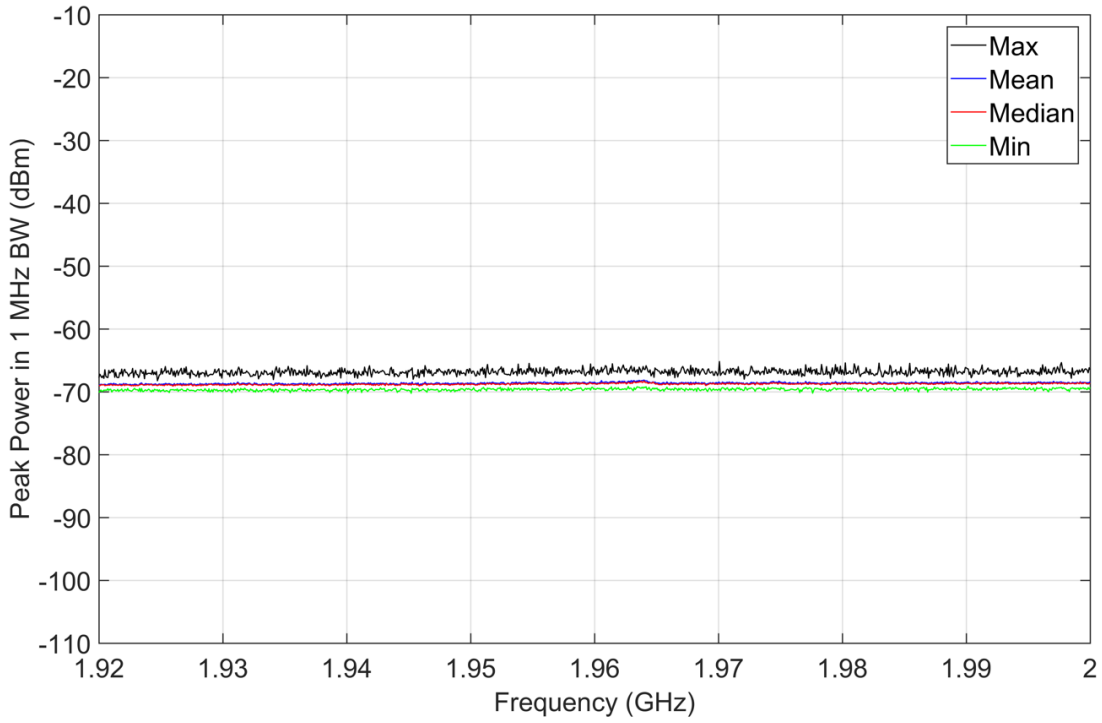


Figure A-14. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

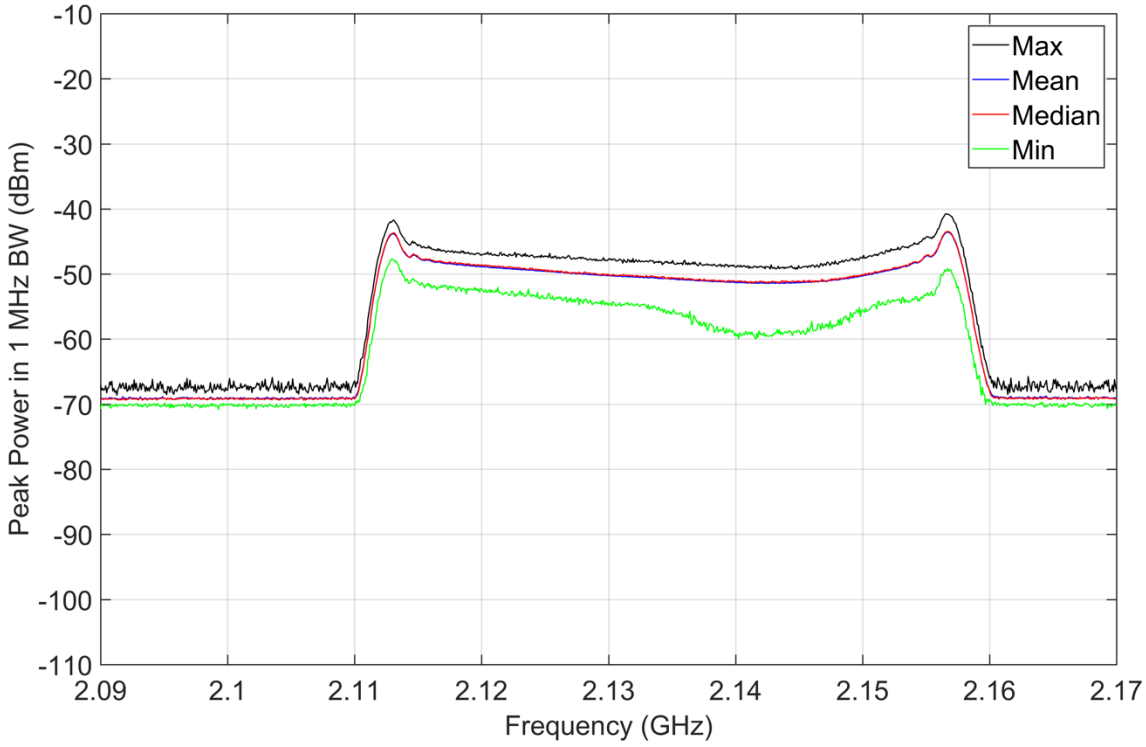


Figure A-15. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

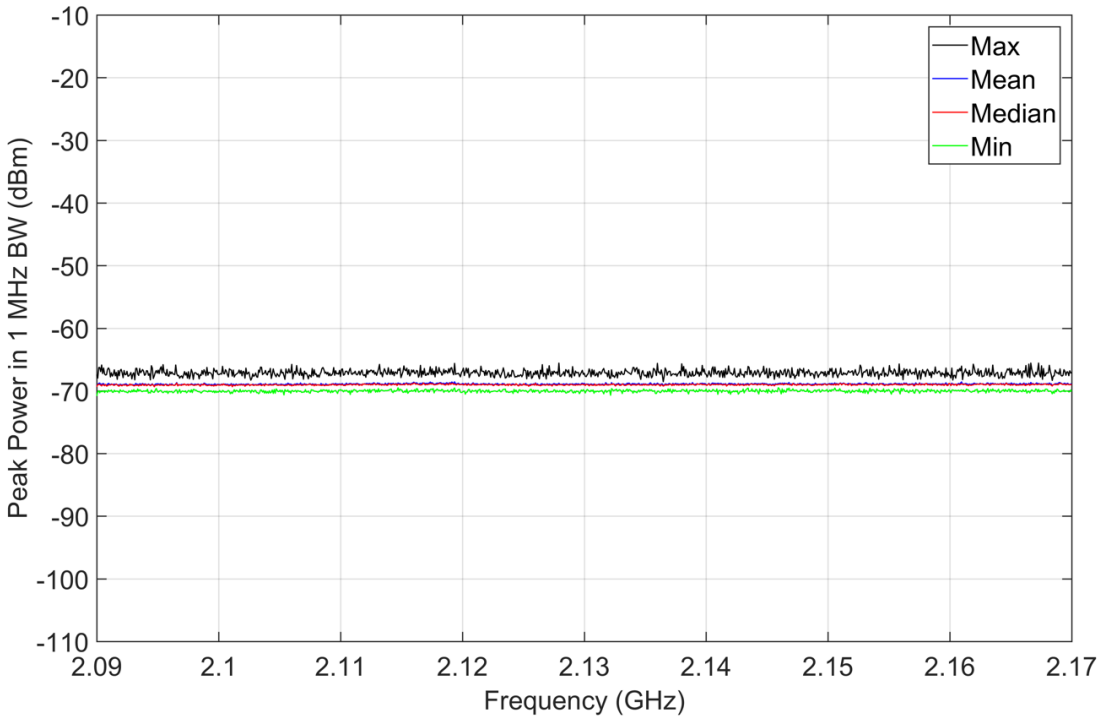


Figure A-16. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp off, location I-2 inside targeted prison cell.

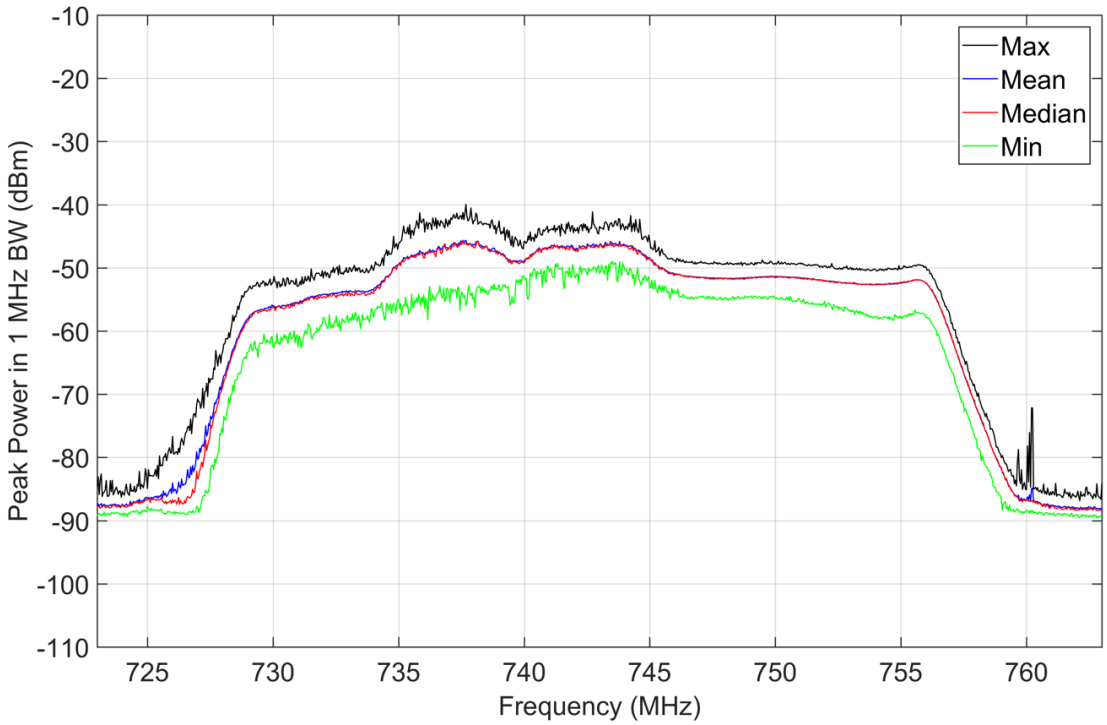


Figure A-17. M4 statistics, peak detection, jammer on, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

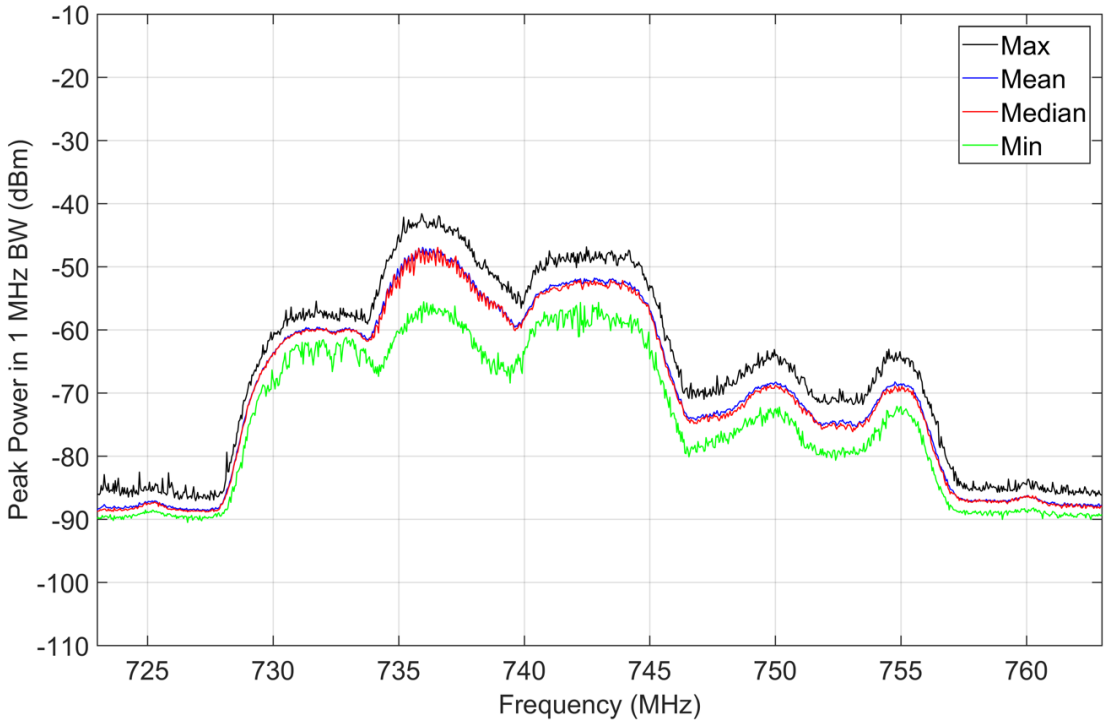


Figure A-18. M4 statistics, peak detection, jammer off, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

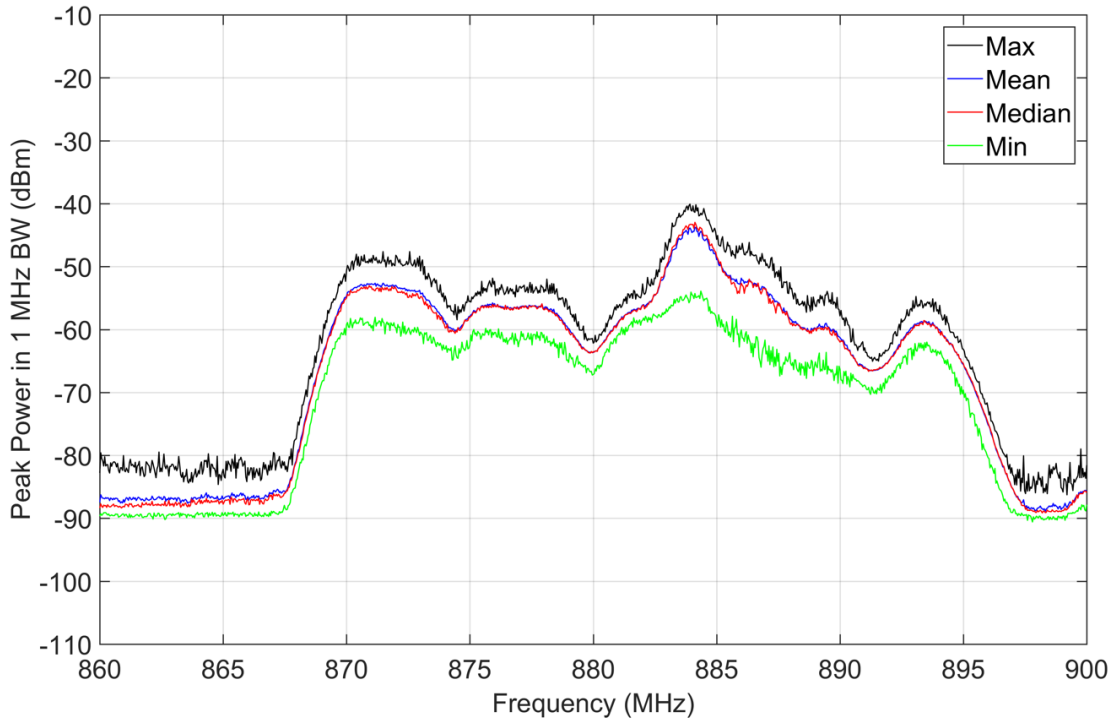


Figure A- 19. M4 statistics, peak detection, jammer on, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

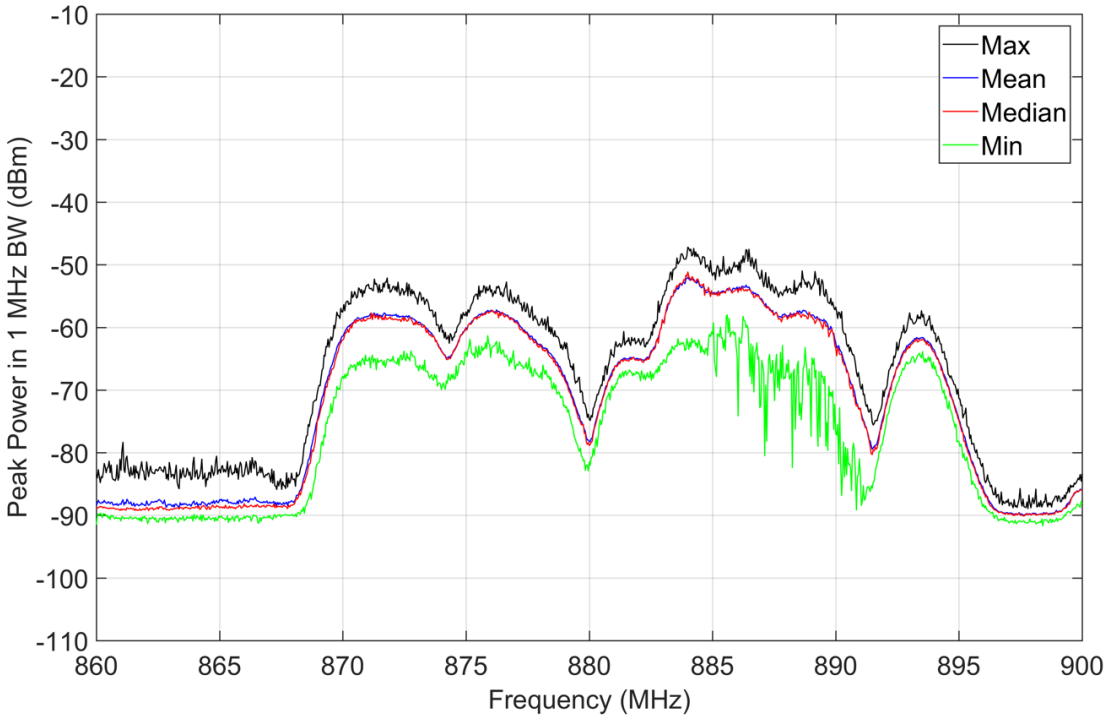


Figure A-20. M4 statistics, peak detection, jammer off, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

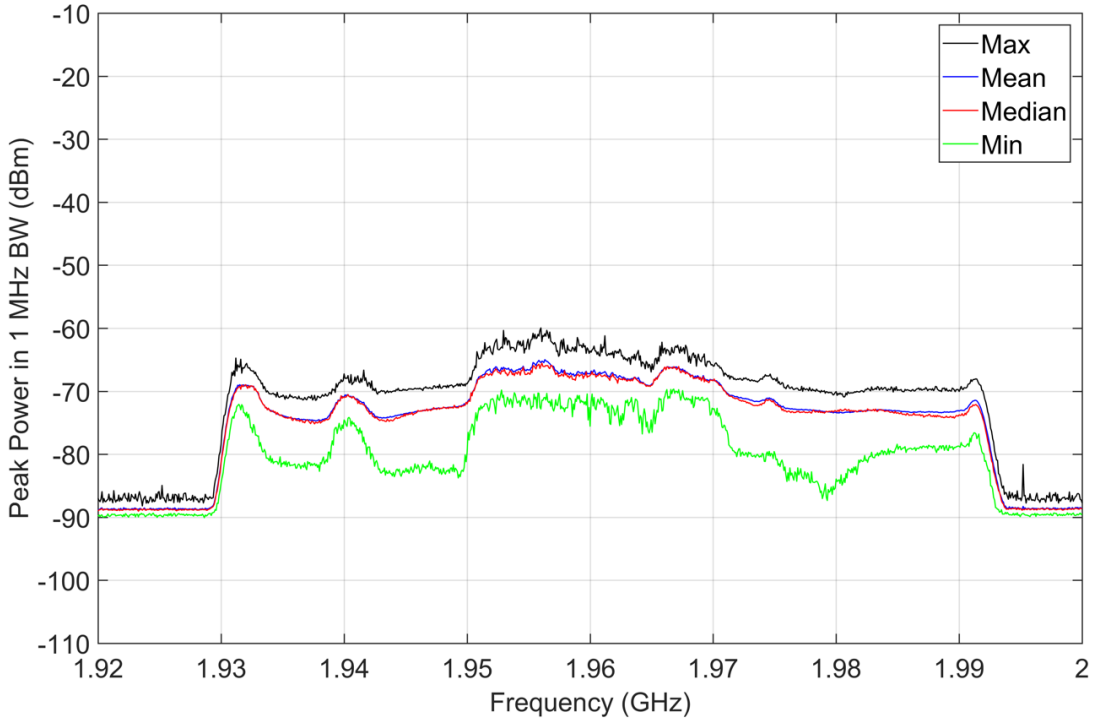


Figure A-21. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

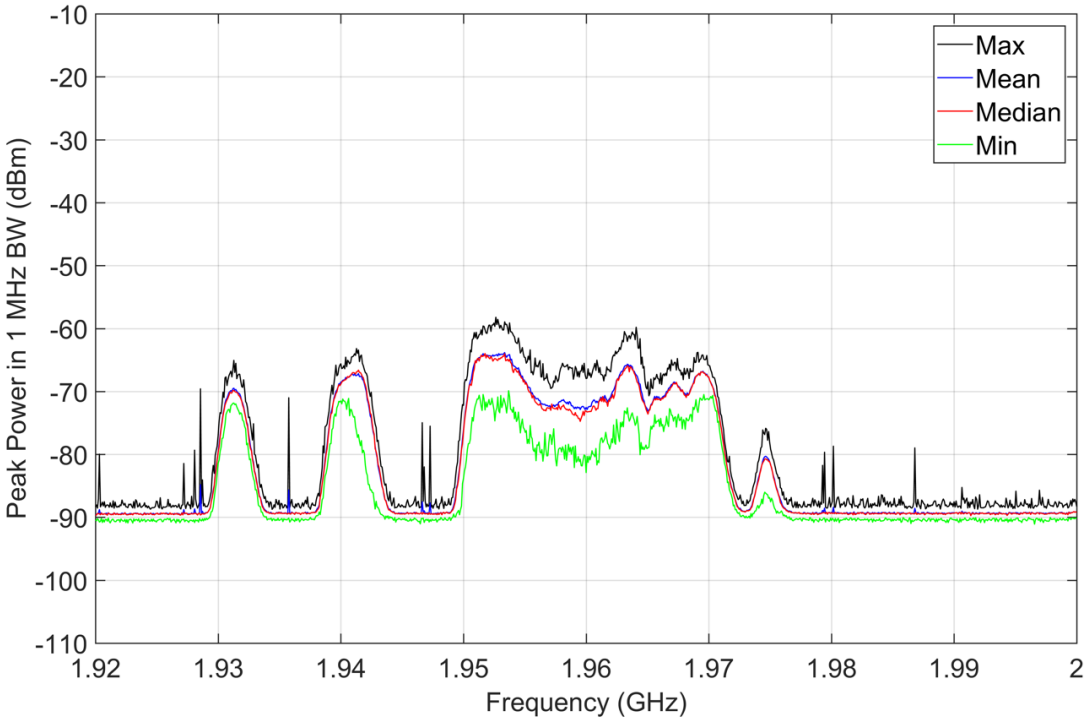


Figure A-22. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

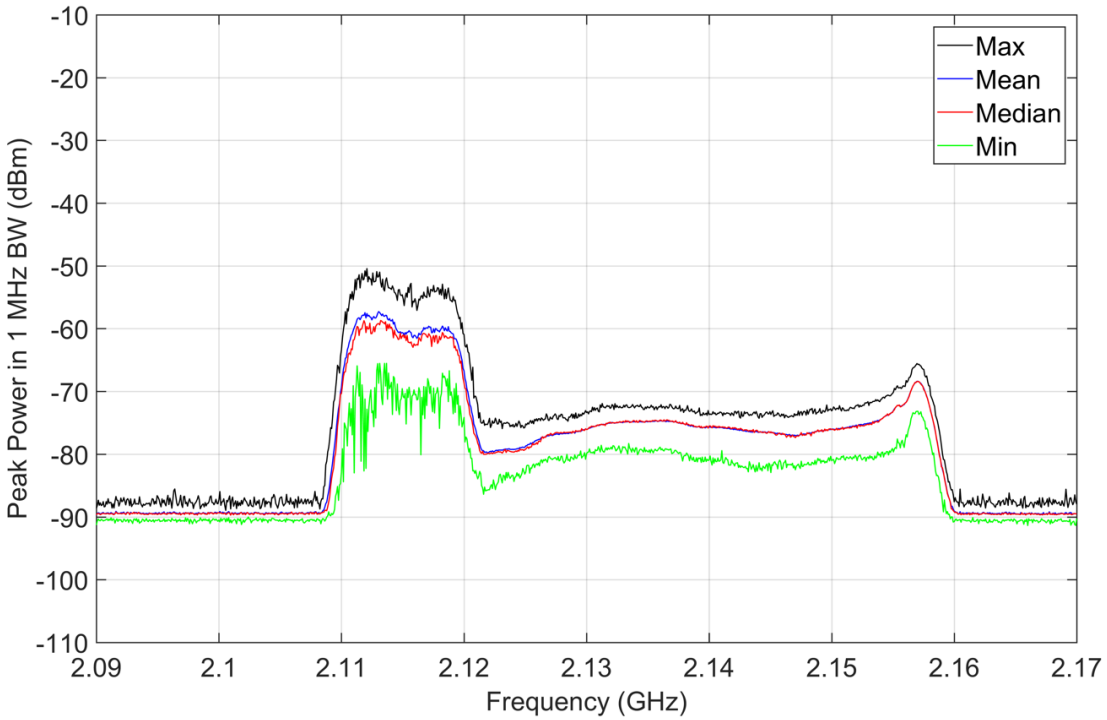


Figure A-23. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

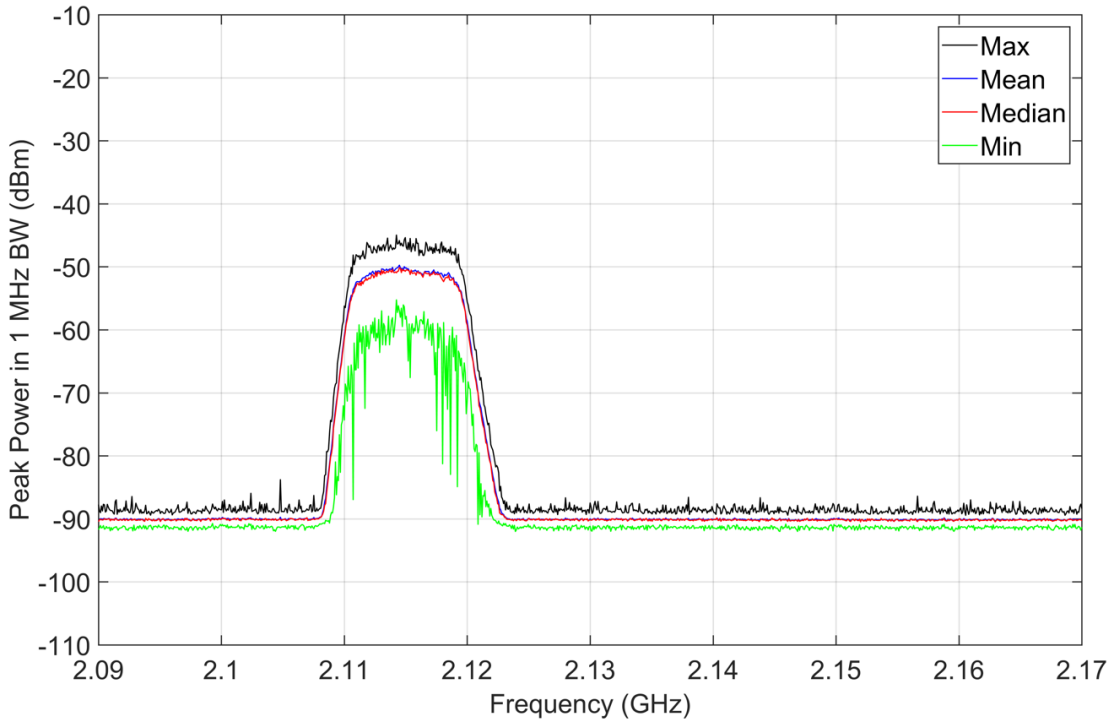


Figure A-24. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-1 outside targeted prison cell.

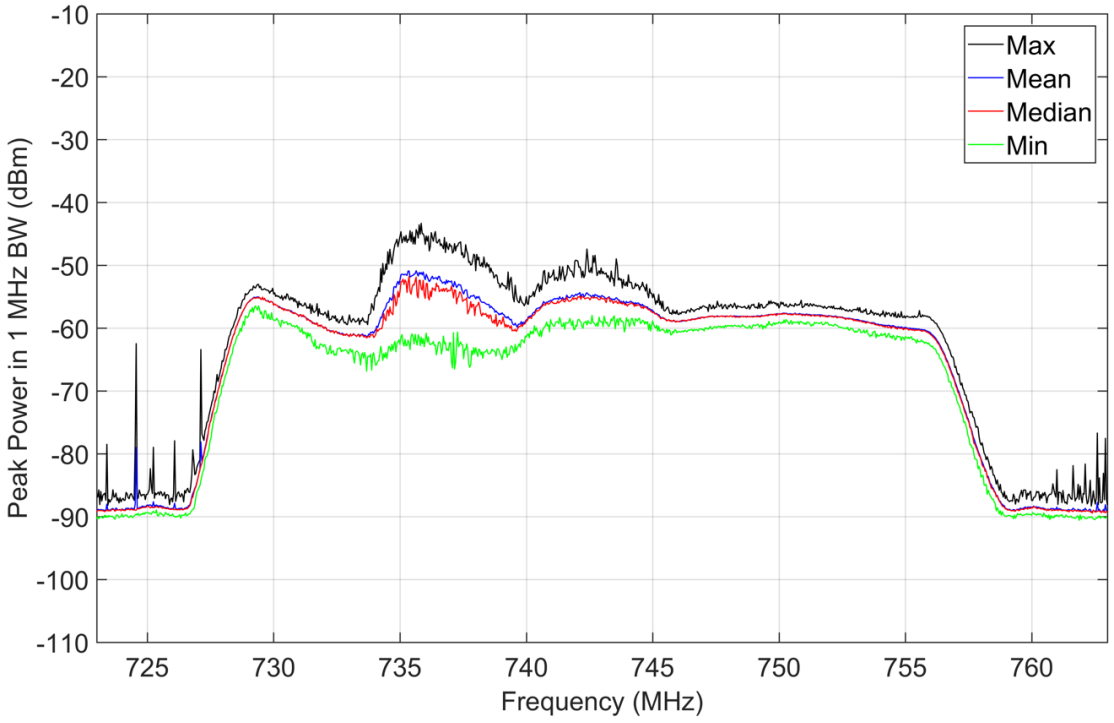


Figure A-25. M4 statistics, peak detection, jammer on, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

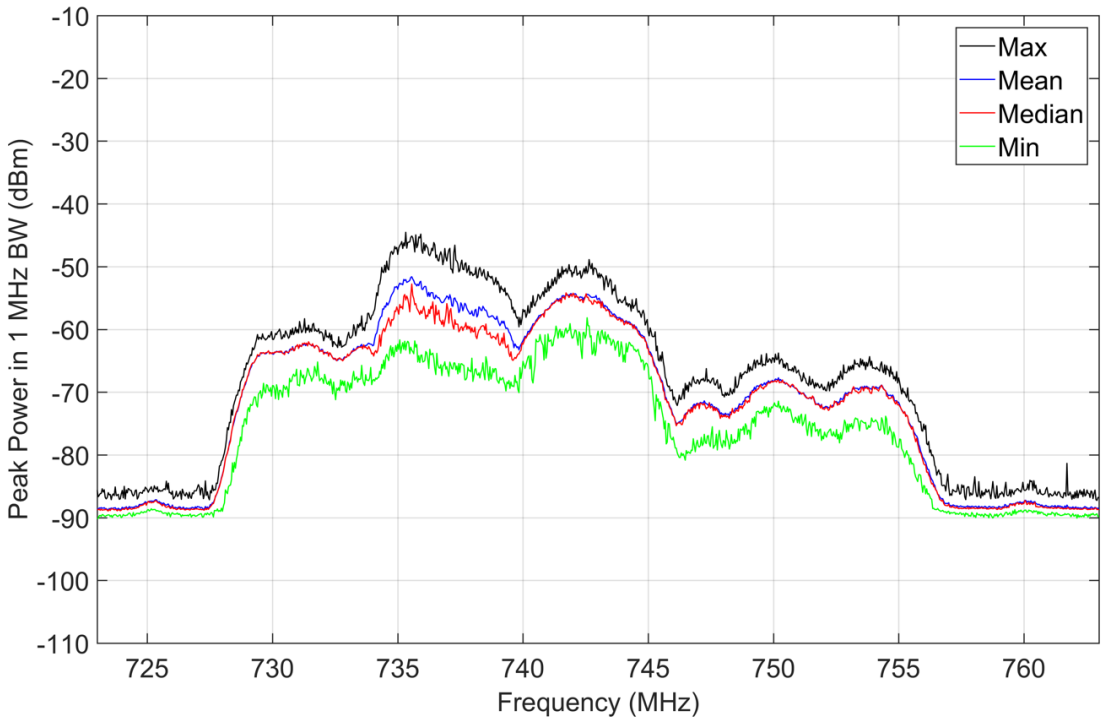


Figure A-26. M4 statistics, peak detection, jammer off, 723–763 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

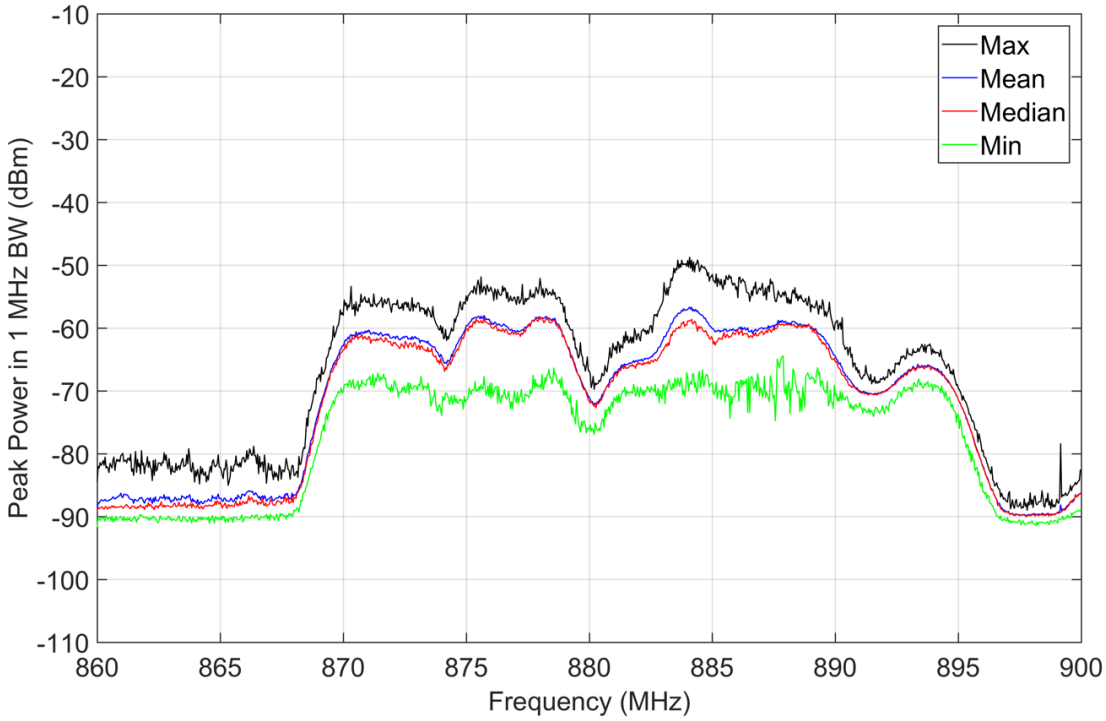


Figure A-27. M4 statistics, peak detection, jammer on, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

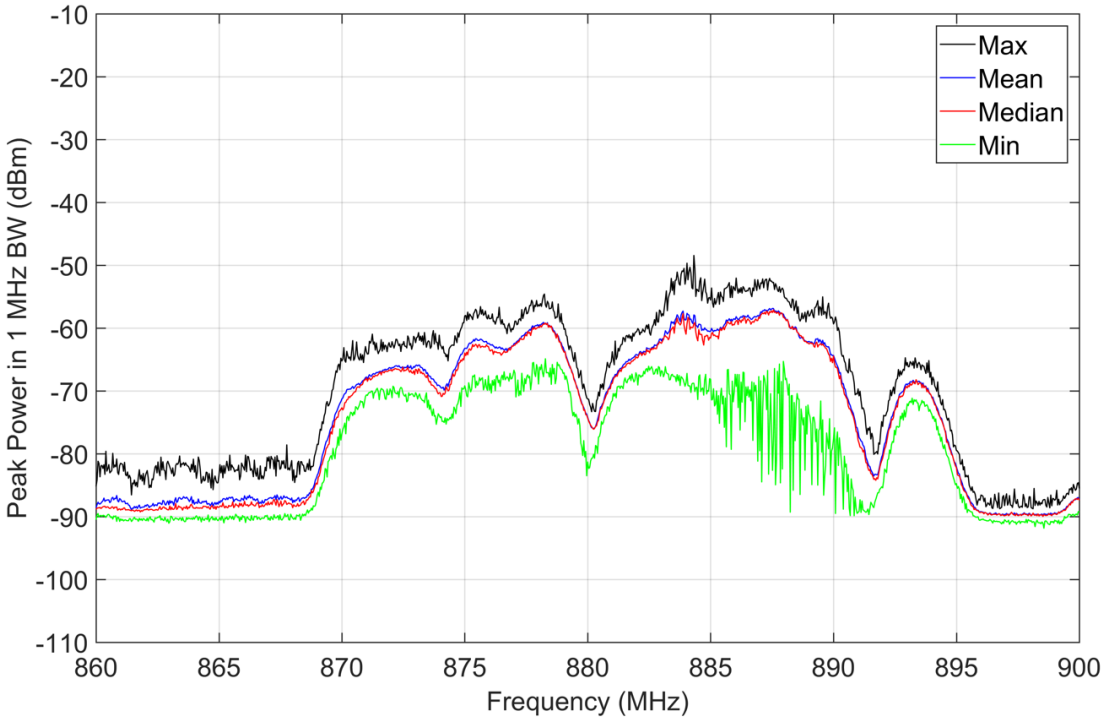


Figure A-28. M4 statistics, peak detection, jammer off, 860–900 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

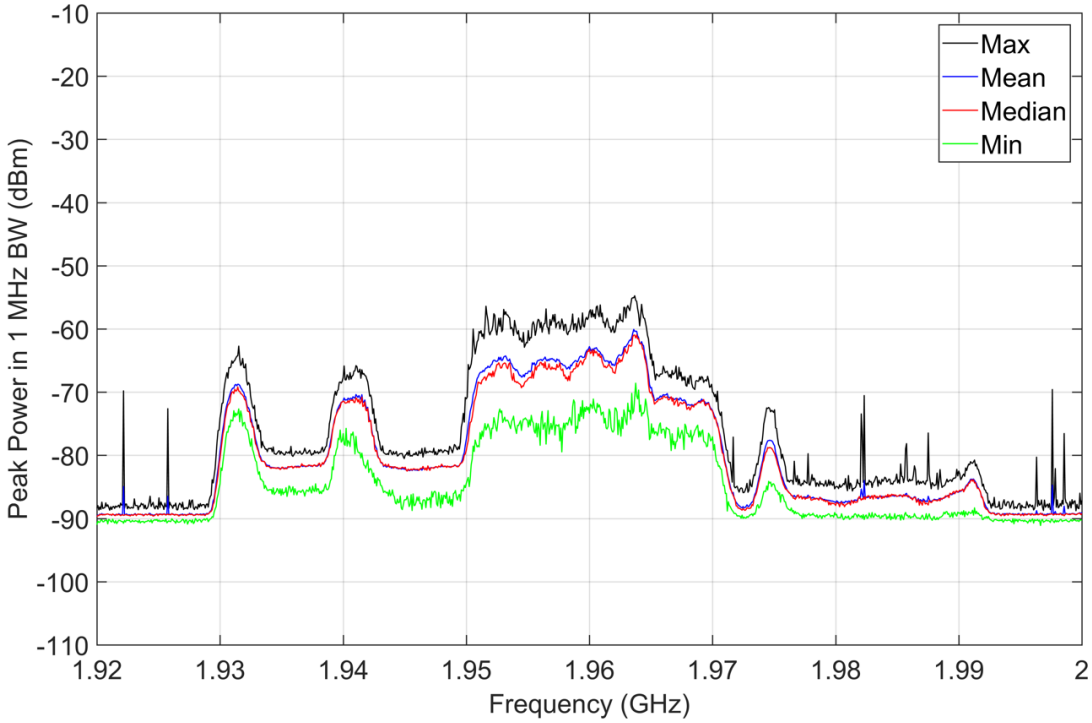


Figure A-29. M4 statistics, peak detection, jammer on, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

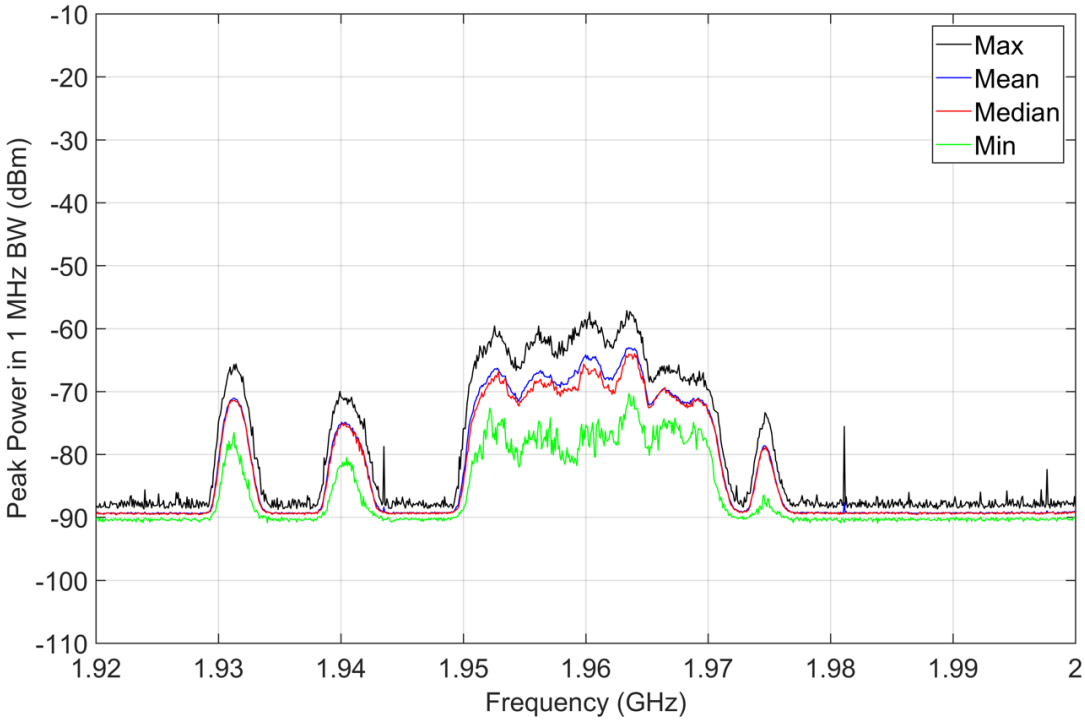


Figure A-30. M4 statistics, peak detection, jammer off, 1920–2000 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

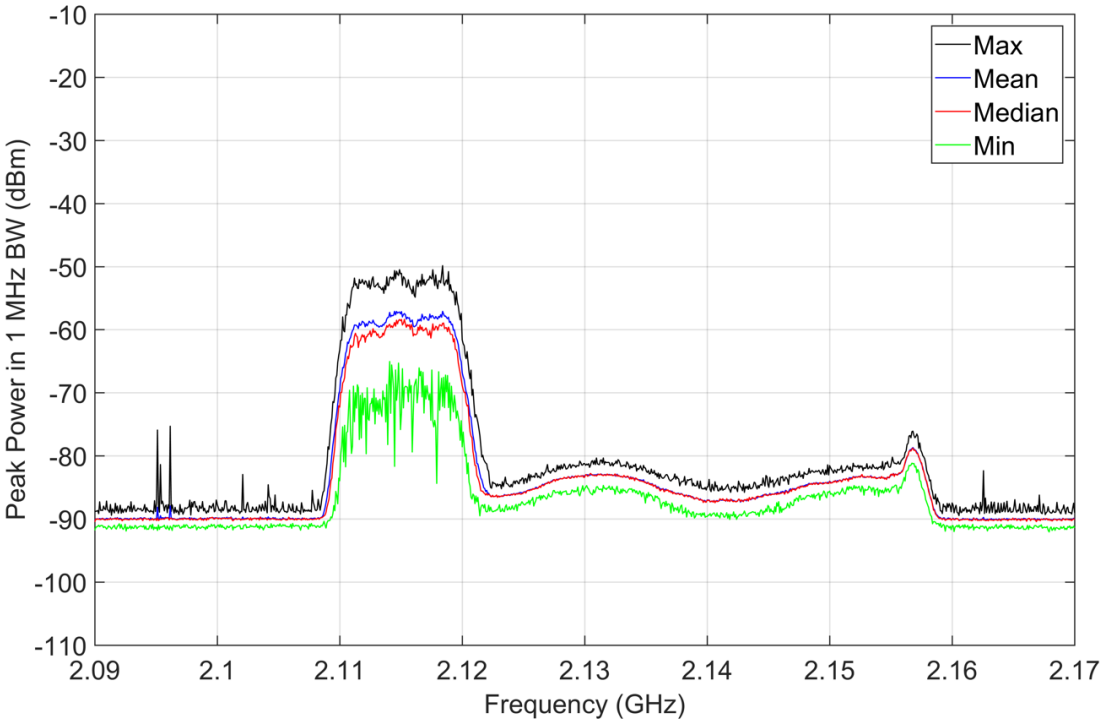


Figure A-31. M4 statistics, peak detection, jammer on, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

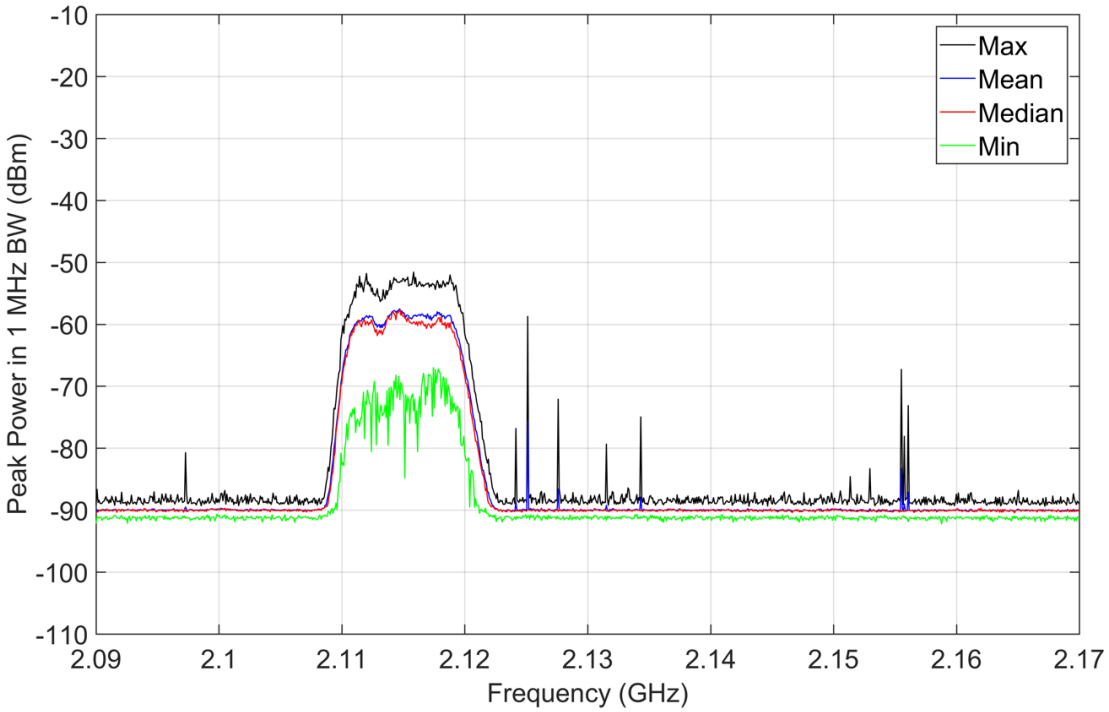


Figure A-32. M4 statistics, peak detection, jammer off, 2090–2170 MHz, 1 MHz bandwidth, 50 recorded sweeps, preamp on, location O-2 outside targeted prison cell.

## APPENDIX B: EXPERIMENTAL OBSERVATION OF POWER IN SAWTOOTH-CW (CHIRPED) SIGNALS AS A FUNCTION OF MEASUREMENT (RECEIVER) BANDWIDTH AND DETECTOR

### B.1 Introduction

To better illuminate the behavior of the chirped CMRS micro-jammer signal that is the subject of this report, the lead author and another ITS engineer[31] undertook an experiment at the ITS laboratory in Boulder, Colorado. They generated a set of four sawtooth-chirped waveforms (as in Figure 1) and measured the waveforms' power levels with a spectrum analyzer in five measurement bandwidths and two detection modes. That experiment, and its results, are described in this Appendix. The measured-power data demonstrate the dependence of power measurement results on the chirp range, $B_c$, of the waveform; the full period, $\tau$ (rather than the half period, or one-way, frequency ramp interval) of the sawtooth; the measurement (or receiver) bandwidth; and the detection mode.

### B.2 Experimental Setup

The experimental waveforms were generated using MATLAB® files with Keysight Signal Studio for Pulse Building® software. The waveform parameters are listed in Table B-1.

Table B-15. Characteristics of four experimental sawtooth-CW modulated waveforms.

| Waveform Number | Bc (= total Δf) (MHz) | Half Sawtooth Period (of Single, One-Way Frequency Ramp), τ/2 (μs) | Total Sawtooth Period, τ (μs) | RF center frequency (MHz) |
|---|---|---|---|---|
| 1 | 3 | 7.1 | 14.2 | 1960 |
| 2 | 10 | 7.1 | 14.2 | 1960 |
| 3 | 30 | 7.1 | 14.2 | 1960 |
| 4 | 60 | 7.1 | 14.2 | 1960 |

The waveforms, constructed at baseband, were generated at RF frequencies with a Keysight MXG series N5182B vector signal generator. The RF (arbitrarily centered at 1960 MHz) was fed into a Keysight MXG series N9030B spectrum analyzer. The total carrier wave power at the analyzer's input was -50.5 dBm. As shown in Table B-1, the chirp range was varied among the waveforms while the chirp interval was held constant.

Power measurements were performed in five bandwidths and two detector modes, for a total of ten combinations of bandwidth and detection. The measurement bandwidths were 100 kHz, 300 kHz, 1 MHz, 3 MHz, and 8 MHz.[32] The two detection modes were positive peak and RMS average. All power measurements were performed with a spectrum analyzer trace marker while

[31] Geoffrey Sanders, who generated the waveforms at baseband using Pulse Builder® and MATLAB® software and then generated them at RF using a Keysight N9030B vector signal generator.

[32] These are 3 dB bandwidths for Gaussian-shaped IF filters. The Gaussian shape factors were supposed to be identical from one filter to the next.

the analyzer was operated in a zero hertz span at the 1960 MHz center frequency of the RF signal. The spectrum analyzer was operated manually and power measurement data were transcribed manually into the lead author's laboratory notebook for later use in this Appendix.

## B.3 Experimental Results

Table B-2 shows the power measurement results for each combination of waveform, measurement bandwidth, and detection mode as copied from the lead author's laboratory notebook. Power measurement units are decibels relative to a milliwatt (dBm), with the full carrier wave power at the analyzer's input being -50.5 dBm, as noted above. In the table, $B_{meas}$ denotes the spectrum analyzer's resolution, or IF, bandwidth setting, which is taken to be the same as the measurement bandwidth. Positive peak and RMS average detection modes are denoted as "+pk" and "avg," respectively.

Table B-16. Power measurement results for the four sawtooth-chirped waveforms.

| **Waveform** | $B_{meas}$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 100 kHz | | 300 kHz | | 1 MHz | | 3 MHz | | 8 MHz | |
| | +pk | avg | +pk | avg | +pk | avg | +pk | avg | +pk | avg |
| 1 | -63.1 | -64.5 | -54.4 | -60.7 | -50.8 | -55.5 | -50.7 | -51.9 | -50.3 | -51.2 |
| 2 | -68.7 | -70.6 | -59.5 | -66.1 | -51.6 | -60.8 | -50.9 | -56.0 | -50.8 | -52.2 |
| 3 | -73.3 | -75.1 | -64.1 | -70.8 | -54.2 | -65.6 | -50.9 | -60.7 | -50.7 | -56.6 |
| 4 | -76.5 | -78.1 | -67.1 | -74.0 | -56.9 | -68.7 | -51.2 | -63.9 | -50.7 | -59.8 |

The data of Table B-2 are graphed in Figure B-1. In this figure are four color-coded sets of measured data points and eight corresponding best-fit lines. Waveform 1 (3 MHz chirp) points and lines are blue; Waveform 2 (10 MHz chirp) points and lines are green; Waveform 3 (30 MHz chirp) points and lines are red; and Waveform 4 (60 MHz chirp) points and lines are black. Two sets of points and lines are plotted for each waveform: peak detected and average detected.

The data points are plotted discretely (dots and crossed circles for Waveform 1 peak and average; inverted triangles and crosses for Waveform 2; open squares and triangles for Waveform 3; and open circles and filled squares for Waveform 4). The lines drawn through them are best-fit based on elementary linear regression.

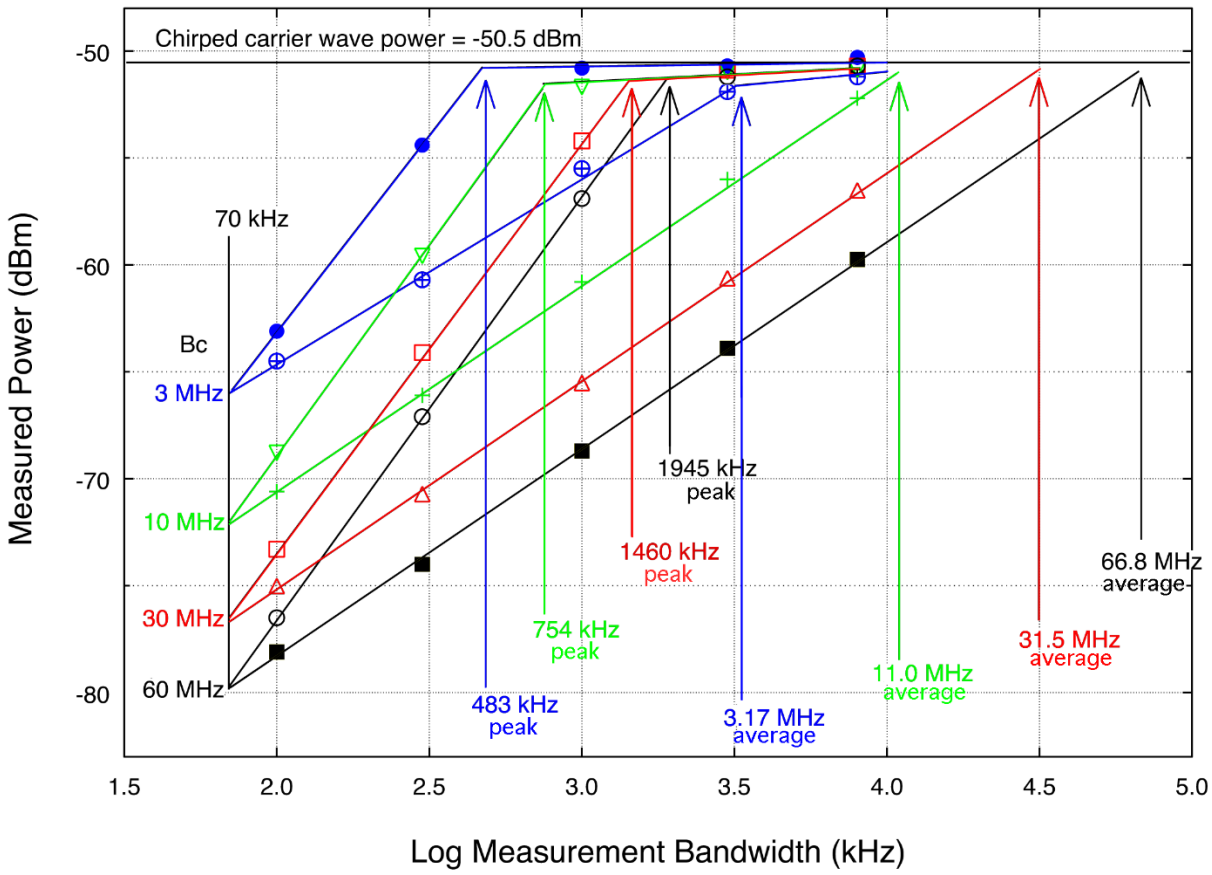


Figure B-1. Graphed data of Table B-2 for four sawtooth-chirped waveforms as a function of measurement bandwidth and detection mode.

## B.4 Analysis.

### B.4.1 Minimum Power that Can be Measured in a Sawtooth Chirped Waveform

The graphed data of Figure B-1 contain much information about the behavior of sawtooth-chirped waveforms. First, the graph shows a lower limit for the power measurement. All peak and average measurements converge at a bandwidth that is equal to the inverse of the *full-cycle* period (not the one-way frequency ramp interval) of the sawtooth. In this case, this bandwidth is (1/14.2 μs) = 70.4 kHz. (In Figure B-1, the nearest resolution that could be read off the graph for this limiting bandwidth was 70 kHz.)

This limiting bandwidth is graphed as a vertical line near the left side of the plot. At this limiting bandwidth, the peak and average-detected power levels collapse to an identical value; they will continue to be identical for any narrower measurement bandwidths. Seen in the time domain in such narrow bandwidths (less than 1/(full period of the sawtooth)), the sawtooth waveforms will appear to be constant-power carrier waves.

This lower limit on the measured power (relative to the full power of the waveform's carrier wave) is determined by the ratio of the measurement (or receiver) bandwidth to the chirped bandwidth of the waveform:

$$P_{meas\_min} = 10 \cdot \log(B_{meas\_min}/B_c),$$

where

$P_{meas\_min}$ = minimum power that can be measured;

$B_{meas\_min}$ = minimum measurement or receiver bandwidth of (1/sawtooth period) or less;

$B_c$ = chirped bandwidth.

For the data of Table B-2 and Figure B-1, this is borne out by the analysis shown in Table B-3:

Table B-3. Comparison of measured and calculated minimum power levels for sawtooth chirped waveforms.

| Waveform | Minimum Measured Power (dBm) | Minimum Measured Power Relative to Full (-50.5 dBm) Input (dB) | Calculated 10·log(Bmeas_min/Bc) (dB) |
|---|---|---|---|
| 1 | -66.0 | -15.5 | -16.3 |
| 2 | -72.0 | -21.5 | -21.5 |
| 3 | -76.6 | -26.1 | -26.3 |
| 4 | -79.8 | -29.3 | -29.3 |

The near-identical values in the last two columns of Table B-3 show excellent agreement between predicted and measured minimum power for each of the waveforms. The equation given above for $P_{meas\_min}$ does indeed give the minimum power value that can be measured for such waveforms.

### B.4.2 Slopes of Peak-Detected and Average-Detected Power Values with Increasing Bandwidths

Figure B-1 shows clearly that, starting at $B_{meas\_min}$, the peak-detected and average-detected power values increase with bandwidth. With power in decibels and bandwidth plotted logarithmically (that is, on a log-log plot) as in Figure B-1, these values increase linearly. The peak-detected line slopes are roughly twice as steep as the average-detected line slopes. Table B-4 shows analysis of these line slopes from the data of Figure B-1.

Per the analysis shown in Table B-4, the average of the peak-detected line slopes was 18.7·log(bandwidth) ± 0.95. The average coefficient for the average-detected line slopes was 9.4 ± 0.58. These coefficient values are both slightly less than the theoretically predicted slopes of 20 and 10, respectively. The peak-detected average line-slope of 18.7 ± 0.95 is within the bounds of the slope of 16.7 ± 2.6 that was measured for the jammer at Cumberland FCI.

Table B-4. Measured peak and average power variation (line slopes) with bandwidth for sawtooth-chirped waveforms.

| Waveform | Peak Rise/Run | Peak Slope | Average Rise/Run | Average Slope |
|---|---|---|---|---|
| 1 | 15.32/0.8224 | 18.6 | 14.2/1.68 | 8.45 |
| 2 | 20.49/1.035 | 19.8 | 21.99/2.199 | 10.0 |
| 3 | 25.26/1.322 | 19.1 | 25.56/2.656 | 9.62 |
| 4 | 28.61/1.659 | 17.2 | 28.7/2.983 | 9.62 |

### B.4.3 Peak and Average Detected Intercepts with Maximum Measurable Power Levels

Because they have different slopes as a function of measurement (receiver) bandwidths, peak and average detected power lines intercept the maximum measurable power for sawtooth chirped waveforms at different limiting bandwidths. These intercept points are shown for peak and average detected power in Figure B-1, labelled with arrowed lines as nearly as could be read from the graph. These intercept points are further analyzed in Tables B-5 and B-6 for peak and average, respectively.

Table B-5. Peak-Detected maximum-power intercept points for sawtooth-chirped waveforms.

| Waveform | Maximum-Power Intercept (kHz) | (Bc/Full Period)1/2 (kHz) | Percentage Difference |
|---|---|---|---|
| 1 | 483 | 650 | -4.8 |
| 2 | 754 | 1187 | +11.4 |
| 3 | 1460 | 2056 | -0.48 |
| 4 | 1945 | 2907 | +5.7 |

Table B-6. Average-detected maximum-power intercept points for sawtooth-chirped waveforms.

| Waveform | Maximum-Power Intercept (kHz) | Bc | Percentage Difference |
|---|---|---|---|
| **1** | 3.17 | 3 | +5.7 |
| **2** | 11.0 | 10 | +10 |
| **3** | 31.5 | 30 | +5 |
| **4** | 66.8 | 60 | +11 |

The peak-detected maximum-power intercept points differ from $(B_c/\textit{full sawtooth period})^{1/2}$ by an average percentage of $3.0 \pm 6.1$. The average-detected maximum-power intercept points differ from $B_c$ (actually, always exceed $B_c$) by an average percentage of $7.9 \pm 2.6$.

### B.5 Summary of Experimental Sawtooth-Chirped Waveform Measurements

The experimental results for these sawtooth-chirped wavforms of chirped bandwidth $B_c$ are summarized as:

1) Peak and average power levels are equal in a bandwidth, $B_{meas\_min}$, of

$$B_{meas\_min} = (1/\text{full sawtooth period}).$$

2) This minimum measurable power is

$$P_{meas\_min} = P_{total} \cdot 10 \cdot \log(B_{meas\_min}/B_c)$$

where $P_{total}$ is the full power in the waveform's carrier wave.

3) Starting at this minimum-power point at $B_{meas\_min}$, the peak and average detected power levels diverge with increasing bandwidth. The peak-detected log-log line slope is $18.7 \pm 0.58$; the average-detected log-log line slope is $9.4 \pm 0.95$.

4) The measured log-log line slopes are slightly less than the theoretically expected slopes of 20 and 10, respectively, although the uncertainty in the measured RMS average line slope puts it within range (one standard deviation) of the theoretical result.

5) The peak-detected and average-detected lines continue until they intercept the full power level of the sawtooth-chirped waveform's carrier wave. The bandwidths of these intercept points are:

$$\text{Peak detected power maximum at } B_{meas} \geq (B_c/\textit{full sawtooth period})^{1/2}$$

$$\text{Average detected power maximum at } B_{meas} \geq \text{about } 1.11 \cdot B_c$$

NTIA FORM 29
(4-80)

U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

# BIBLIOGRAPHIC DATA SHEET

| 1. PUBLICATION NO. | 2. Government Accession No. | 3. Recipient's Accession No. |
|---|---|---|
| TR-18-533 | | |

| 4. TITLE AND SUBTITLE | 5. Publication Date |
|---|---|
| Emission Measurements of a Contraband Wireless Device Jammer at a Federal Prison | June 2018 |
| | 6. Performing Organization Code<br>NTIA/ITS.D |

| 7. AUTHOR(S) | 9. Project/Task/Work Unit No. |
|---|---|
| Frank H. Sanders, Robert T. Johnk and Edward F. Drocella | 3152012-300 |

| 8. PERFORMING ORGANIZATION NAME AND ADDRESS | 10. Contract/Grant Number. |
|---|---|
| Institute for Telecommunication Sciences<br>National Telecommunications & Information Administration<br>U.S. Department of Commerce<br>325 Broadway<br>Boulder, CO 80305 | |

| 11. Sponsoring Organization Name and Address | 12. Type of Report and Period Covered |
|---|---|
| National Telecommunications & Information Administration<br>Herbert C. Hoover Building<br>14th & Constitution Ave., NW<br>Washington, DC 20230 | |

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 and time domain measurements of a contraband wireless device micro-jammer that was operated temporarily in four Commercial Mobile Radio Service (CMRS) bands at a Federal Correctional Institution (FCI) at Cumberland, Maryland. The four jammed CMRS bands were between 730 MHz and 2.155 GHz. The micro-jammer targeted CMRS service indoors, in a single medium-security prison cell. Spectrum measurements of the jammer emissions were performed at two places inside the targeted prison cell and at two non-targeted nearby locations outdoors. Jammer emission measurements were performed at each location with multiple measurement bandwidths and detectors across a frequency range of 300 MHz to 4.34 GHz. Measurements at each location were performed twice, with the jammer device on versus off, so as to show the relative power levels of the jamming signal versus the ambient CMRS signals at each location. Aggregate emissions from multiple micro-jammer devices such as would be required to cover an entire prison facility were not measured. Jammer emissions are presented in units of power per unit bandwidth in measurement system circuitry; a table for conversion of those data to units of incident field strength in space is provided.

16. Key Words (Alphabetical order, separated by semicolons)
aggregate emissions; cellular communications jamming; commercial mobile radio service (CMRS) jamming; denial-of-service jamming; electromagnetic compatibility (EMC); emission bandwidth; harmful interference; in-band emissions; communications jamming; micro-jammer; radiation hazard (radhaz); radio jamming; wireless device jamming

| 17. AVAILABILITY STATEMENT | 18. Security Class. (This report) | 20. Number of pages |
|---|---|---|
| ☒ UNLIMITED. | Unclassified | 141 |
| ☐ FOR OFFICIAL DISTRIBUTION. | 19. Security Class. (This page)<br>Unclassified | 21. Price:<br>n/a |

# 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.doc.gov.