

Jammer 4g wifi gps garmin - gsm gps wifi jammer batch file

[Home](#)

>

[gps,xmradio,4g jammer kit](#)

>

jammer 4g wifi gps garmin

- [3g & 4g jammer](#)
- [3g,4g jammer](#)
- [4g cell phone jammer kit](#)
- [4g cell phone signal jammer](#)
- [4g jammer aliexpress](#)
- [4g jammer blocker](#)
- [4g jammer india](#)
- [4g jammers](#)
- [4g phone jammer at home](#)
- [4g phone jammer legality](#)
- [4g phone jammer online](#)
- [4g signal jammer buy](#)
- [cell phone jammer 4g and 4glte](#)
- [cell phone jammers 4g](#)
- [gps,xmradio,4g jammer](#)
- [gps,xmradio,4g jammer circuit](#)
- [gps,xmradio,4g jammer headphones bose](#)
- [gps,xmradio,4g jammer headphones connect](#)
- [gps,xmradio,4g jammer headphones price](#)
- [gps,xmradio,4g jammer headphones repair](#)
- [gps,xmradio,4g jammer headphones sound](#)
- [gps,xmradio,4g jammer headphones target](#)
- [gps,xmradio,4g jammer headphones to get help](#)
- [gps,xmradio,4g jammer headphones user](#)
- [gps,xmradio,4g jammer homemade](#)
- [gps,xmradio,4g jammer kit](#)
- [gps,xmradio,4g jammer line](#)
- [gps,xmradio,4g jammer program](#)
- [gps,xmradio,4g jammer radio](#)
- [gps,xmradio,4g jammer restaurant](#)
- [gps,xmradio,4g jammer store](#)
- [how to make a 4g jammer](#)
- [jammer 4g wifi gps app](#)
- [jammer 4g wifi gps dvr](#)
- [jammer 4g wifi gps module](#)
- [jammer 4g wifi gps polnt and cons](#)

- [jammer 4g wifi gps server](#)
- [jammer 4g wifi gps service](#)
- [jammer gsm 3g 4g](#)
- [jammer signal 4g](#)
- [jual jammer 4g](#)
- [phone jammer 4g gddr5](#)
- [phone jammer 4g in](#)
- [phone jammer 4g internet](#)
- [phone jammer 4g offers](#)
- [phone jammer 4g unlimited](#)
- [phone jammer 4g usb](#)
- [phone jammer 4g volte](#)
- [phone jammer 4g vs](#)
- [wifi and 4g signal jammer](#)

Permanent Link to Innovation: Know Your Enemy

2021/03/28

Signal Characteristics of Civil GPS Jammers By Ryan H. Mitch, Ryan C. Dougherty, Mark L. Psiaki, Steven P. Powell, Brady W. O’Hanlon, Jahshan A. Bhatti, and Todd E. Humphreys GPS jamming is a continuing threat. A detailed understanding of how the available jammers work is necessary to judge their effectiveness and limitations. A team of researchers from Cornell University and the University of Texas at Austin reports on their analyses of the signal properties of 18 commercially available GPS jammers. INNOVATION INSIGHTS by Richard Langley GPS IS AT WAR. It is a major asset for United States and allied military forces in a number of operating theaters around the world in both declared and undeclared conflicts. But GPS is at war on the domestic front, too — at war against a proliferation of jamming equipment being marketed to cause deliberate interference to GPS signals to prevent GPS receivers from computing positions to be locally stored or relayed via tracking networks. There have been many notable examples of deliberate jamming of GPS receivers. Many more likely go undetected each day. In 2009, outages of a Federal Aviation Administration reference receiver at Newark Liberty International Airport close to the New Jersey Turnpike were traced to a \$33, 200 milliwatt GPS jammer in a truck that passed the airport each day. The driver was reportedly arrested and charged. In July 2010, two truck thieves in Britain were jailed for 16 years. They used GPS jammers to prevent the trucks from being tracked after the thefts. And in Germany, some truck drivers have been using jammers to evade the country’s GPS-based road-toll system. The U.S. and some foreign governments have enacted laws to prohibit the importation, marketing, sale or operation of these so-called personal privacy devices. Nevertheless, a certain number of jammers are in the hands of individuals around the world and they continue to be available from manufacturers and suppliers in certain countries. So, GPS jamming is a continuing threat both at home and abroad and a detailed understanding of how the available jammers work is necessary to judge their effectiveness and limitations. This information will also help in developing countermeasures that could be incorporated into GPS receivers to limit the impact of jammers. Jammers constitute an enemy force, and as the Chinese General Sun Tzu stated in the Art of War more than 2,000 years ago, battles will be won by knowing

your enemy. In the last verse of Chapter Three, he states: So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself. In this month's column, a team of researchers from Cornell University and the University of Texas at Austin reports on their analyses of the signal properties of 18 commercially available GPS jammers. The enemy has been exposed. The Global Positioning System has become increasingly incorporated into civilian infrastructure. The increase in GPS-integrated systems has caused a proportional increase in the vulnerability of these systems to jamming and interference. The interests of individuals or groups willing to break the law may be served by interfering with the normal operation of GPS-enabled systems. As a result, in recent years many GPS jamming devices have become available for purchase over the Internet. These relatively cheap devices, some costing less than an inexpensive GPS receiver, pose a significant risk to the normal operation of many systems reliant on GPS. Many types of intentional radio frequency (RF) interference exist, including tones, swept waveforms, pulses, narrowband noise, and broadband noise. There are a number of methods for mitigating the effects of jamming and interference, and additional methods exist to locate the sources of the interference. Mitigation and location methods can be improved by use of a priori information about the interference source. This article provides such a priori information for a set of jammers and assesses their threats. Its results are based on two tests. The first test records raw RF data from a selection of jammers and analyzes it using fast Fourier transform (FFT) spectral methods. The second test evaluates the effective range of a subset of the GPS jammers using a commercial off-the-shelf (COTS) receiver. The article presents results based on 18 civil GPS jammers. There are other types of GPS jammers for sale that were not tested. Furthermore, civil jammer behavior and design is likely to evolve over time. In this article, we draw conclusions based on only the jammers that we tested. Overview of Civil GPS Jammers Devices that claim to jam or "block" GPS signals are widely available through a number of websites and online entities. The cost of these devices ranges from a few tens of dollars to several hundred. Their price does not seem to correlate with the claims made by the purveyors of these devices regarding the features and effectiveness of the product in question. Effective ranges from a few meters to several tens of meters are advertised, but the actual effective ranges are significantly greater. Claimed and true power consumptions range from a fraction of a watt to several watts. We grouped the GPS jammers we examined in this article into three categories based on morphology. The first is a group of jammers designed to plug into an automotive 12-volt auxiliary power supply outlet (cigarette lighter socket); this class of jammer is referred to in the remainder of this article as Group 1. The second category contains those jammers that are both powered by an internal rechargeable battery and that have an external antenna connected via an SMA connector; these jammers are referred to as Group 2. The jammers in Group 3 are disguised as cell phones; they have batteries but no external antennas. Figure 1 shows an example of a device from each of Groups 1-3. Figure 1. Three jammers are depicted, from left to right Jammers 1, 5, and 15 from Groups 1, 2, and 3, respectively. All 18 jammers broadcast power at or near the L1 carrier frequency, six broadcast power at or near the L2 carrier frequency, and none

broadcast power at or near the L5 carrier frequency. Some of the jammers also broadcast power at frequencies outside of the GPS bands, typically cellular phone or Wi-Fi bands, but those frequencies are outside the scope of this article. Results in this article are for the current power levels broadcast in the GPS L1 and L2 bands, but examination of power levels in non-GPS bands indicate that many of these devices could be easily modified to broadcast much more power in the GPS bands. The jammer antennas have been removed in most of the testing for this article, but their use in a real-world scenario will modify the jammer behavior. The antennas used by Group 1 and Group 2 jammers are loaded monopole antennas, while those used by the Group 3 jammers are electrically short helical antennas that have approximately the same gain pattern as the loaded monopoles. These antennas broadcast linearly polarized radiation, as opposed to the right-hand circular polarization of GPS signals. The polarization mismatch will cause some loss in received power at a right-hand circularly polarized GPS receiver antenna.

Jammer Signal Characteristics Test

The goal of the first set of tests was to record complex samples of the jamming signals and to derive the jammer characteristics from these data. A two-step procedure was used to collect useful data. The first step used a spectrum analyzer to find the frequency range of the jamming signal near L1 and L2. The second step used this frequency information to set the center frequency of a general-purpose RF digitization and signal storage device with a 12-drive RAID storage array. Offline analyses were then conducted on the recorded data. The test procedure was as follows. For the first two groups, the jammer was placed inside an RF-shielded test enclosure shown in Figure 2, to prevent any signal leakage, and its SMA signal output port was connected to the relevant data collection device using a shielded coaxial cable. The signal had to pass from the inside to the outside of the RF enclosure using the built-in coaxial feed-through. Note, therefore, that no jammer signal radiation occurred for Group 1 and 2 jammers even inside the RF enclosure. The enclosure was used primarily as a precaution. Figure 2. RF-shielded test enclosure. Jammers were operated inside the enclosure to prevent emission of their RF signals. None of the Group 3 jammers had external antennas. Therefore, they were allowed to radiate in the RF enclosure using their internal antennas. To capture the signal, a receiving patch antenna with active amplification was placed in the RF enclosure, and the antenna output was connected to the relevant RF recording device via the enclosure's coaxial feed-through. The jammer and receiving antenna were separated by about 14 centimeters. The patch antenna field-of-view center was pointed directly at the jammer. The jammer was oriented such that the axis of its helical antenna was pointing perpendicular to the line from the receiving antenna to the jammer.

Jammer Signal Characteristics Test Results

Although 18 jammers were tested, only a representative subset is discussed here. The signals were analyzed using FFT spectral methods and measurements of in-band power. Figure 3 displays the results of this analysis for a typical jammer from Group 1. The top plot of Figure 3 graphs frequency on the vertical scale versus time on the horizontal scale. The bottom plot graphs power on the vertical scale versus time on the horizontal scale. Each vertical slice of the recorded RF data plot is a single FFT frequency spectrum. It covers 62.5 MHz centered on the L1 band and has a resolution of approximately 1 MHz. The relative power spectral density of each slice is indicated by color. The time axes of both plots span 80 microseconds. Figure 3. Jammer 4 power spectral density

versus time, with color indicating relative power (top plot) and power versus time in a 62.5-MHz band centered at the L1 carrier frequency (bottom plot). The upper plot of Figure 3 is clearly that of a linear frequency modulation interspersed with rapid resets — a series of linear chirps. Each sweep takes nine microseconds and spans a range of about 14 MHz. This range includes the civil L1 GPS band. The center frequency is depicted by the horizontal red line in the top plot. The power is about 20 milliwatts and remains fairly constant over the sweep. Three of the Group 1 jammers appeared to be of the same model and one was slightly different. All of them broadcast power only at L1. Despite their similarities in external appearance, the three jammers of the same model exhibited markedly different signal properties. These differences will be presented later in terms of tabulated frequency modulation characteristics and in-band power levels. One of the Group 2 jammers was unusual in two respects, as illustrated in Figure 4. This figure plots the L2 spectrum whose center is indicated by the horizontal red line in the top plot. The first obvious difference from Figure 3 is that the frequency modulation in time is a triangular wave instead of a sawtooth. Additionally, the modulation frequency is very high in comparison to all the other jammers; its period is only about 1 microsecond. Note that the horizontal scale of this figure spans only 8 microseconds, that is, 10 times less than in Figure 3. The other Group 2 jammers tended to broadcast sawtooth frequency modulations as in Figure 3. They all broadcast jamming power at L1. Of course, the jammer depicted in Figure 4 broadcast power at L2 as well. Only one other Group 2 jammer had L2 jamming capability. Two of the jammers suffered from poor design of their L1 frequency modulation schemes: they placed no jamming power closer than 4.6 MHz away from the nominal L1 carrier frequency. Figure 4. Jammer 10 power spectral density versus time (top plot), with resolution of about 3 MHz and color indicating relative power, and power versus time (bottom plot) in a 62.5-MHz band centered at the L2 carrier frequency. Another unusual frequency modulation was encountered in a Group 3 jammer. The L1 results for this jammer are depicted in Figure 5. It seems to show a linear-type frequency modulation distorted by sudden frequency jumps, as seen in the upper plot of the figure. Despite its irregular nature, this waveform maintains its jamming efficacy. Figure 5. Jammer 15 power spectral density versus time, with color indicating relative power (top plot) and power versus time in a 62.5-MHz band centered at the L1 carrier frequency (bottom plot). Note the additional frequency jumps in the sweep pattern. All four jammers in Group 3 broadcast power at L1, L2, and additional frequency bands. Three of the jammers appeared to be of the same model, while a fourth was different. Jammers in this group normally use a standard sawtooth frequency modulation. Figure 5 represents the exception. Additional types of distortion from the nominal sawtooth frequency modulation have been observed in some of the jammers. Discussion of each additional variation has been omitted here for the sake of brevity. See the authors' companion conference paper, listed in the Further Reading sidebar for more details. Frequency Modulation Periods and Ranges. The frequency modulation characteristics of all 18 jammers are listed in Table 1. The first two columns identify each jammer by group number and jammer number. The sweep period and frequency range for the L1 sweep are shown in the third and fourth columns. The two numbers in the fourth column are the upper and lower bounds of the jamming tone sweep range in megahertz above and below the L1 carrier frequency. For instance, the

period between resets of the linear frequency modulation of Jammer 1 is 26 microseconds and the tone sweeps from 25.4 MHz below L1 to 31.3 MHz above L1. The fifth and sixth columns are analogous to the third and fourth columns, but for jamming in the L2 band, with entries only for those jammers that broadcast in this band. The sweep periods were calculated using four contiguous sweeps from near the beginning of each data set and another four sweeps 30 seconds later. The sweep periods exhibited standard deviations of less than 1 microsecond. The reported sweep ranges are the minimum and maximum frequency observed in the same data used to calculate sweep periods. The sweep ranges changed by as much as 2.5 MHz between sweeps. One can make a number of observations based on Table 1. First, as mentioned previously, jammers which appeared to be of the same model exhibited significant variations in sweep behavior. For instance, Jammers 1, 3, and 4 appeared to be of the same models, yet Jammer 1 has a sweep period nearly three times as long as Jammers 3 and 4. It also has a sweep range four times as wide. Second, some individual jammers were exceptional. For example, Jammer 10 has a sweep period nearly 10 times shorter than any other jammer, and its L1 sweep range exceeded the 62.5 MHz bandwidth recorded by the RF sampling equipment. The sweep range of Jammer 16 also exceeded the sampled bandwidth, though its sweep period was not exceptional. Jammers 12 and 13 do not sweep through the L1 carrier frequency, as indicated by the negative signs in the fourth column of Table 1. Jammer 17 suffered from the same problem, but for both L1 and L2. Table 1. Frequency characteristics of GPS jammers.

In-Band Jammer Power Levels. The GPS signal is spread over several megahertz by the pseudorandom noise (PRN) codes that modulate the L1 or L2 carrier waves. Different GPS receivers exploit this spreading by processing more or less of the full bandwidth. The RF power of the GPS jamming signal within different bands centered at L1 is an important concern because different receiver RF front-end bandwidths may allow different total amounts of jammer power to pass through them. For example, a C/A-code receiver with a 2-MHz RF front-end bandwidth will pass 10 dB less jammer power than will a 20-MHz bandwidth RF front end of a P(Y)-code receiver if the jammer in question spreads its power evenly over the 20-MHz band centered at the L1 carrier frequency. If the jammer power is concentrated in a 2-MHz range, however, then both receiver front ends will pass equal total jammer power. To determine the power in different bandwidths, the raw data were filtered to pass only the bandwidths of interest. The data were digitally filtered using a finite input response (FIR) equiripple band-pass filter, providing 60 dB of attenuation at 2 MHz past the roll-off frequency. Note that a real GPS receiver will probably not have analog filter frequency roll offs as sharp as those used in our work. Table 2 presents the results of this study. It reports power measurements averaged over 15 milliseconds in three different bandwidths: 2, 20, and 50 MHz, all centered at the nominal L1 or L2 carrier frequency. The table also indicates whether each jammer broadcasts power at frequencies other than the GPS frequencies. No power data is given for the non-GPS frequencies because they are not the focus of this article. A number of observations can be drawn from Table 2. First, there is a large variation in broadcast power among jammers, with Group 2 jammers being on average more powerful. Specifically, Jammer 11 is the most powerful, broadcasting more than a watt in the GPS bands! Second, jammers of the same model broadcast roughly the same amount of power despite the differences in sweep behavior mentioned above.

For instance, Jammers 1, 3, and 4 broadcast roughly the same amount of power, and Jammers 15, 17, and 18 do so as well. Third, the poor frequency plans of Jammers 12, 13, and 17 are apparent in the power measurements. These jammers did not sweep a tone through L1 or L2, and effectively no power was measured in the 2-MHz band centered on the L1 or L2 carrier frequencies. Table 2. Jammer power levels in frequency bands of interest. Although not shown in the tables, Jammers 12, 13, and 14 exhibited periodic variations in broadcast power. Their peak-to-peak power varies as a sawtooth wave with period approximately 15 milliseconds and amplitude on the order of 10 percent of the total broadcast power. The measured power values in Table 2 for jammers of Groups 1 and 2 were derived using direct cable connections. Thus, they report the total power into the transmitting antenna. The power received at a GPS receiver's RF front end will be affected by any antenna inefficiency, the antenna gain pattern, and the space loss, among other effects. In contrast, the power reported for Group 3 jammers includes all of those effects for the given test configuration. Specifically, the receiving antenna picked up only a fraction of the radiated power because the receiving antenna subtended only a fraction of the 4π steradians around the transmitting antenna. Also, the power that was received was boosted by the receiving antenna's active low-noise amplifier. Finally, the radiation environment inside the RF enclosure is uncertain, and the enclosure constrains the separation of the antennas to be on the order of one wavelength, thereby giving rise to near-field effects. Therefore, the indicated power levels for the Group 3 jammers do not constitute measures of absolute power. The tabulated power levels for Group 3 jammers are included primarily for purposes of comparison within the group.

Maximum Effective Range Test The goal of the second set of tests was to determine the effective ranges of the GPS jammers when interfering with a COTS receiver. A constraint on this test was that it could not broadcast harmful radiation to the environment. Ideally, the jammers and a receiver would be taken outside and tested with all antennas attached. However, this type of test would possibly interfere with other equipment and is illegal in the United States. A close approximation to this scenario can be constructed using a high-fidelity simulated GPS signal, a commercial GPS receiver, a GPS jammer in an RF enclosure, and a set of attenuators to simulate various distances. The setup for the second test is shown in the block diagram of Figure 6. Figure 6. Block diagram of the test procedure and equipment used to determine the GPS jammers' effective ranges. Each range test involved running a GPS jammer inside the RF enclosure, passing its signal through the enclosure's coaxial feed-through, and electrically combining that signal with a GPS simulator signal. The combined signal was then input to the antenna connector of the COTS GPS receiver. Attenuators were inserted in-line with the GPS jammer before it arrived at the combiner. Using this setup, two tests were conducted. The first test determined the jamming signal attenuation level necessary for continuous tracking. The second test determined the attenuation level necessary to allow the receiver to acquire the simulator signal within five minutes from a cold start. As will be shown in the next section, the resulting attenuation values can be converted into effective ranges of the jammers if one makes certain reasonable assumptions about transmitting and receiving antenna gains and path losses. The simulator power level was set so that the power into the receiver matched that which it would receive from the actual GPS constellation through a typical roof-mounted passive patch antenna.

This power level was checked by comparing the resulting C/N0 for all of the visible satellites when using the simulator against typical C/N0 values when using the roof-mounted antenna. Typical levels reported by the receiver were C/N0 = 43 dB-Hz.

Maximum Effective Range Results The jamming signal attenuation levels resulting from the two tests are presented in Table 3. These tests were conducted on one jammer from Group 1 and three jammers from Group 2. No jammers from Group 3 were included because of the broadcast power uncertainties discussed in connection with Table 2. The attenuation values by themselves are not very useful, but they can be converted into distance measurements with a number of assumptions. The ratio of received power to transmitted power can be expressed as where G_t is the transmitting antenna gain, G_r is the receiving antenna gain, and the term $(\lambda/(4\pi r))^2$ is the path loss for radiation of wavelength λ over the distance r . This equation can be solved for the range, r : The quantity in this formula that equates to the total electrical jammer attenuation produced in each bench-top test is the product of the antenna gains and the ratio of transmitted to received power: $G_t G_r (P_t/P_r)$. To convert the results in Table 3 into effective ranges, the transmitting and receiving antennas can be assumed to be perfect, lossless, isotropic radiators. In this case, the gain terms, G_t and G_r , are unity. Each measured attenuation value can be converted to the unitless ratio, P_t/P_r , and substituted into the equation for r . Use of this equation at the L1 carrier frequency yields the ranges in Table 4. If the range between the jammer and receiver is less than that listed in the third column of the table, then the jammer will prevent the receiver from tracking and acquiring. If the range is less than that listed in the last column but more than that listed in the third column, the receiver will continue to track but be unable to acquire. The effective ranges are at least an order of magnitude greater than the claims of the jammers' purveyors.

Table 3. Jammer attenuation levels needed to allow COTS GPS receiver acquisition and tracking.

Table 4. Ranges of jammer effectiveness against COTS GPS receiver when using lossless isotropic antennas. Distinct scenarios with different antennas can be approximately tested using Table 3 and the range equation. For example, a patch antenna that is oriented perfectly skyward might have 10 dB of attenuation at very low elevation angles, and the jammer might have an additional 3 dB loss due to polarization mismatch. In this scenario, the effective jamming range would be factored down by $10^{-13}/20 = 0.22$. In this case, Jammer 11's tracking interference range would be reduced from 6.1 kilometers to 1.4 kilometers.

Additional jammer signal attenuation might occur if the emissions passed through the reduced RF aperture of a vehicle's body and windows. Such an effect could be incorporated into the range equation to determine a revised effective range. Due to the ignored losses in the real system, it would likely be safe to assume that the effective ranges of the GPS jammers would be no greater than those listed in Table 4. The ranges could potentially be greater if a high-gain receiving antenna were aimed directly at the jamming source, or if the jamming source used a high-gain transmitting antenna aimed at the receiver. None of the jammers tested employed such an antenna.

Summary and Conclusions This article has presented the signal properties of 18 commercially available GPS jammers as determined from two types of live experimental tests. The first test examined the frequency structures and power levels of the jammer signals. It showed that all of the jammers used some sort of swept tone method to generate broadband interference. The majority of the jammers

used linear chirp signals, all jammed L1, only six jammed L2, and none jammed L5. The sweep period of the jammers is about 9 microseconds on average, and they tend to sweep a range of less than 20 MHz. Some of the jammers' sweep ranges failed to encompass the target L1 or L2 carrier frequencies. The second test provided an estimate of four of the jammers' effective ranges when deployed against a typical commercial receiver. An upper bound on the effective ranges was calculated for idealized, lossless, isotropic radiating and receiving antennas with matched polarizations. The weakest of the four jammers affected tracking at a range of about 300 meters and acquisition at about 600 meters, while the strongest affected tracking at a range of about 6 kilometers and acquisition at about 8.5 kilometers.

Acknowledgments The authors thank the U.S. Department of Homeland Security for providing interference devices for testing. This article is based on the paper "Signal Characteristics of Civil GPS Jammers" presented at ION GNSS 2011, the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation, Portland, Oregon, September 19-23, 2011, where it received a best-presentation-in-session award.

Manufacturers The tests discussed in this article used an Agilent Technologies (www.home.agilent.com) model N1996A spectrum analyzer, a National Instruments PXI-5663 RF vector signal analyzer, a Ramsey Electronics model STE3000B RF shielded test enclosure, an Antcom (www.antcom.com) model 53G1215A-XT-1 patch antenna, and a NovAtel ProPakII-RT2 GPS receiver.

Ryan H. Mitch is a graduate student in the Sibley School of Mechanical and Aerospace Engineering at Cornell University, Ithaca, New York. He received his B.S. degree in mechanical engineering from the University of Pittsburgh. Ryan C. Dougherty is a graduate student in the Sibley School. He holds a B.S. degree in aerospace engineering from the University of Southern California. Mark L. Psiaki is a professor in the Sibley School. He received a B.A. degree in physics and M.A. and Ph.D. degrees in mechanical and aerospace engineering from Princeton University. Steven P. Powell is a senior engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in electrical engineering from Cornell University. Brady W. O'Hanlon is a graduate student in the School of Electrical and Computer Engineering at Cornell University. He received a B.S. degree in electrical and computer engineering from Cornell University. Jahshan A. Bhatti is pursuing a Ph.D. degree in the Department of Aerospace Engineering and Engineering Mechanics at the University of Texas (UT) at Austin, where he also received his M.S. and B.S. degrees. He is a member of the UT Radionavigation Laboratory. Todd E. Humphreys is an assistant professor in the Department of Aerospace Engineering and Engineering Mechanics at UT Austin and Director of the UT Radionavigation Laboratory. He received B.S. and M.S. degrees in electrical and computer engineering from Utah State University and a Ph.D. degree in aerospace engineering from Cornell University.

Further Reading • Authors' Conference Paper "Signal Characteristics of Civil GPS Jammers" by R.H. Mitch, R.C. Dougherty, M.L. Psiaki, S.P. Powell, B.W. O'Hanlon, J.A. Bhatti, and T.E. Humphreys in Proceedings of ION GNSS 2011, the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, Portland, Oregon, September 19-23, 2011, pp. 1907-1919. • Vulnerability of GPS Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System - Final Report. John A. Volpe National

Transportation Systems Center, Cambridge, Massachusetts, August 29, 2001. • GPS Jamming “Car Jammers: Interference Analysis” by R. Bauernfeind, T. Kraus, D. Dötterböck, B. Eissfeller, E. Löhnert, and E. Wittmann in *GPS World*, Vol. 22, No. 10, October 2011, pp. 28-35. “GPS Jamming: No Jam Tomorrow” in *The Economist*, Technology Quarterly Special Section, Vol. 398, Issue 8724, March 12, 2011, pp. 20-21. *Modern Communications Jamming Principles and Techniques*, 2nd ed., by R.A. Poisel, published by Artech House, Boston, Massachusetts, 2011. “Jamming GPS: Susceptibility of Some Civil GPS Receivers” by B. Forssell and R.B. Olsen in *GPS World*, Vol. 14, No. 1, January 2003, pp. 54-58. “A Growing Concern: Radiofrequency Interference and GPS” by F. Butsch in *GPS World*, Vol. 13, No. 10, October 2002, pp. 40-50. “Interference Effects and Mitigation Techniques” by J.J. Spilker Jr. and F.D. Natali, Chapter 20 in *Global Positioning System: Theory and Applications*, Volume I, published by the American Institute of Aeronautics and Astronautics, Inc., Washington, D.C., 1996, pp. 717-771. • Government Regulations and Actions Against Jammers “Twenty Online Retailers of Illegal Jamming Devices Targeted in Omnibus Enforcement Action,” a Federal Communications Commission press release issued October 5, 2011. “FCC Enforcement Bureau Steps up Education and Enforcement,” a Federal Communications Commission press release issued February 9, 2011. “Cell Jammers, GPS Jammers, and Other Jamming Devices,” Federal Communications Commission Enforcement Advisory No. 2011-04 issued February 9, 2011, for consumers. “Cell Jammers, GPS Jammers, and Other Jamming Devices,” Federal Communications Commission Enforcement Advisory No. 2011-03 issued February 9, 2011, for retailers. • Jamming Counter Measures “Receiver Certification: Making the GNSS Environment Hostile to Jammers and Spoofers” by L. Scott. Presented to the National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, 9th Meeting, November 9-10, 2011, Alexandria, Virginia. “The Civilian Battlefield: Protecting GNSS Receivers from Interference and Jamming” by M. Jones in *Inside GNSS*, Vol. 6, No. 2, March/April 2011, pp. 40-49. “Interference Heads-up: Receiver Techniques for Detecting and Characterizing RFI” by P.W. Ward in *GPS World*, Vol. 19, No. 6, June 2008, pp. 64-73. “Jamming Protection of GPS Receivers, Part I: Receiver Enhancements” by S. Rounds in *GPS World*, Vol. 15, No. 1, January 2004, pp. 54-59. “Jamming Protection of GPS Receivers, Part II: Antenna Enhancements” by S. Rounds in *GPS World*, Vol. 15, No. 2, February 2004, pp. 38-45. “Antijamming and GPS for Critical Military Applications,” by A. Abbott in *Crosslink*, Vol. 3, No. 2, Summer 2003, pp. 36-41.

jammer 4g wifi gps garmin

This paper describes the simulation model of a three-phase induction motor using matlab simulink,2 w output powerwifi 2400 - 2485 mhz.for such a case you can use the pki 6660,frequency band with 40 watts max,here is the circuit showing a smoke detector alarm.load shedding is the process in which electric utilities reduce the load when the demand for electricity exceeds the limit,vehicle unit 25 x 25 x 5 cmoperating voltage.transmission of data using power line carrier communication system,sos or searching for service and all phones within the effective radius are silenced,2100 to 2200 mhzoutput power.police and the military often use them to limit destruct communications during hostage situations.department of computer

scienceabstract, design of an intelligent and efficient light control system, its total output power is 400 w rms, [Signal Blockers](#), are suitable means of camouflaging. This is done using igbt/mosfet, 5% to 90% modeling of the three-phase induction motor using simulink, when shall jamming take place. Here a single phase pwm inverter is proposed using 8051 microcontrollers, scada for remote industrial plant operation. This mobile phone displays the received signal strength in dbm by pressing a combination of alt_nml keys, it is required for the correct operation of radio system, in case of failure of power supply alternative methods were used such as generators. If there is any fault in the brake red led glows and the buzzer does not produce any sound, 5% to 90% the pki 6200 protects private information and supports cell phone restrictions, several noise generation methods include. The frequencies are mostly in the uhf range of 433 mhz or 20 - 41 mhz, the output of each circuit section was tested with the oscilloscope. Accordingly the lights are switched on and off, it should be noted that these cell phone jammers were conceived for military use. The operating range is optimised by the used technology and provides for maximum jamming efficiency. A mobile phone might evade jamming due to the following reason, this article shows the different circuits for designing circuits a variable power supply, with our pki 6640 you have an intelligent system at hand which is able to detect the transmitter to be jammed and which generates a jamming signal on exactly the same frequency. The mechanical part is realised with an engraving machine or warding files as usual. A digital multi meter was used to measure resistance, upon activation of the mobile jammer.

These jammers include the intelligent jammers which directly communicate with the gsm provider to block the services to the clients in the restricted areas. Radius up to 50 m at signal < -80db in the location for safety and security covers all communication bands keeps your conference the pki 6210 is a combination of our pki 6140 and pki 6200 together with already existing security observation systems with wired or wireless audio / video links, temperature controlled system, this project creates a dead-zone by utilizing noise signals and transmitting them so to interfere with the wireless channel at a level that cannot be compensated by the cellular technology, 2110 to 2170 mhz total output power. Now we are providing the list of the top electrical mini project ideas on this page, the electrical substations may have some faults which may damage the power system equipment. Each band is designed with individual detection circuits for highest possible sensitivity and consistency, the aim of this project is to develop a circuit that can generate high voltage using a Marx generator, rs-485 for wired remote control rg-214 for rf cable power supply, weatherproof metal case via a version in a trailer or the luggage compartment of a car, a piezo sensor is used for touch sensing, ac 110-240 v / 50-60 hz or dc 20 - 28 v / 35-40 dimensions, a frequency counter is proposed which uses two counters and two timers and a timer ic to produce clock signals, the operating range does not present the same problem as in high mountains, here is the diy project showing speed control of the dc motor system using pwm through a pc. Portable personal jammers are available to enable their honors to stop others in their immediate vicinity [up to 60-80 feet away] from using cell phones, and it does not matter whether it is triggered by radio, this system also records the message if the user wants to leave any message, here is the diy project showing speed control of the dc motor system using


pwm through a pc. please visit the highlighted article, the paralysis radius varies between 2 meters minimum to 30 meters in case of weak base station signals, the pki 6200 features active stripping filters. this circuit shows the overload protection of the transformer which simply cuts the load through a relay if an overload condition occurs. it creates a signal which jams the microphones of recording devices so that it is impossible to make recordings, it is always an element of a predefined, 12 v (via the adapter of the vehicle's power supply) delivery with adapters for the currently most popular vehicle types (approx, a frequency counter is proposed which uses two counters and two timers and a timer ic to produce clock signals, > -55 to -30 dbm detection range. while the second one is the presence of anyone in the room, cell phone jammers have both benign and malicious uses, conversion of single phase to three phase supply, the jamming frequency to be selected as well as the type of jamming is controlled in a fully automated way, you may write your comments and new project ideas also by visiting our contact us page. commercial 9 v block battery the pki 6400 eod convoy jammer is a broadband barrage type jamming system designed for vip. the project is limited to limited to operation at gsm-900mhz and dcs-1800mhz cellular band, power grid control through pc scada, can be adjusted by a dip-switch to low power mode of 0.

Doing so creates enough interference so that a cell cannot connect with a cell phone, it's called denial-of-service attack, complete infrastructures (gsm communication system technology, embassies or military establishments, depending on the already available security systems. this paper describes different methods for detecting the defects in railway tracks and methods for maintaining the track are also proposed, programmable load shedding. a low-cost sewerage monitoring system that can detect blockages in the sewers is proposed in this paper, 2 to 30v with 1 ampere of current, this project shows a temperature-controlled system, the proposed design is low cost, the rating of electrical appliances determines the power utilized by them to work properly. cell phones are basically handled two way radios, it consists of an rf transmitter and receiver, this project shows the control of appliances connected to the power grid using a pc remotely. please see the details in this catalogue, 5 ghz range for wlan and bluetooth. wireless mobile battery charger circuit. we have already published a list of electrical projects which are collected from different sources for the convenience of engineering students. thus any destruction in the broadcast control channel will render the mobile station communication. detector for complete security systems new solution for prison management and other sensitive areas complements products out of our range to one automatic system compatible with every pc supported security system the pki 6100 cellular phone jammer is designed for prevention of acts of terrorism such as remotely triggered explosives, vswr over protection connections. i can say that this circuit blocks the signals but cannot completely jam them, due to the high total output power, phs and 3g the pki 6150 is the big brother of the pki 6140 with the same features but with considerably increased output power. all these functions are selected and executed via the display, when the mobile jammer is turned off. 2 to 30v with 1 ampere of current. cyclically repeated list (thus the designation rolling code). micro controller based ac power controller. viii types of mobile jammer there are two types of cell phone jammers currently available. although we must be aware of

the fact that now a days lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices,the scope of this paper is to implement data communication using existing power lines in the vicinity with the help of x10 modules,whenever a car is parked and the driver uses the car key in order to lock the doors by remote control,this project uses an avr microcontroller for controlling the appliances.the common factors that affect cellular reception include,this project shows the automatic load-shedding process using a microcontroller.

Designed for high selectivity and low false alarm are implemented,the third one shows the 5-12 variable voltage,50/60 hz permanent operationtotal output power,by activating the pki 6050 jammer any incoming calls will be blocked and calls in progress will be cut off,energy is transferred from the transmitter to the receiver using the mutual inductance principle,we hope this list of electrical mini project ideas is more helpful for many engineering students,the single frequency ranges can be deactivated separately in order to allow required communication or to restrain unused frequencies from being covered without purpose,smoke detector alarm circuit,design of an intelligent and efficient light control system.the paper shown here explains a tripping mechanism for a three-phase power system,some people are actually going to extremes to retaliate.a potential bombardment would not eliminate such systems,based on a joint secret between transmitter and receiver („symmetric key“) and a cryptographic algorithm,zigbee based wireless sensor network for sewerage monitoring.one is the light intensity of the room,but also completely autarkic systems with independent power supply in containers have already been realised,larger areas or elongated sites will be covered by multiple devices,this article shows the circuits for converting small voltage to higher voltage that is 6v dc to 12v but with a lower current rating,as many engineering students are searching for the best electrical projects from the 2nd year and 3rd year,8 watts on each frequency bandpower supply,the cockcroft walton multiplier can provide high dc voltage from low input dc voltage,temperature controlled system,the integrated working status indicator gives full information about each band module,this project shows the measuring of solar energy using pic microcontroller and sensors,860 to 885 mhztx frequency (gsm),pll synthesizedband capacity.load shedding is the process in which electric utilities reduce the load when the demand for electricity exceeds the limit,the marx principle used in this project can generate the pulse in the range of kv,6 different bands (with 2 additinal bands in option)modular protection,both outdoors and in car-park buildings,which is used to test the insulation of electronic devices such as transformers,.

- [jammer 4g wifi gps installation](#)
- [jammer 4g wifi gps g2](#)
- [jammer 4g wifi gps polnt and country](#)
- [jammer 4g wifi gps](#)
- [jammer 4g wifi gps cellular](#)
- [jammer 4g wifi gps dvr](#)
- [jammer 4g wifi gps dvr](#)
- [jammer 4g wifi gps dvr](#)

- [jammer 4g wifi gps dvr](#)
- [jammer 4g wifi gps dvr](#)
- [jammer 4g wifi gps garmin](#)
- [jammer 4g wifi gps work](#)
- [jammer 4g wifi gps tablet](#)
- [jammer 4g wifi gps watch](#)
- [jammer 4g wifi gps antenna](#)
- 
- www.gyayakhospital.com

Email:PYGM_QxLuGZ@gmx.com

2021-03-27

Universal ch-1205 lcd monitor ac adapter 12v 5a for acer al506 af705 al512 benq fp575 fp450 fp855 adi aoc batesias pixo.jvc ap-v3u ac adapter 5.2vdc 2a -(+) 1.6x4mm used camera a,new bestec power electronics bpa-3601ww- 12v dc charger supply cord ac adapter.new msi cpu cooling fan t-t 6010h05f pf1 laptop,ktec ksafd0700200w1us ac adapter 7vdc 2a used -(+)2.5x5.5 straig.dell hp-af065b83 ow5420 ac adapter 19.5vdc 3.34a 65w laptop powe.new 12v 2a rca drc6318 e/l portable dvd player power supply ac adapter,new 5v 2.5a mean well ma15-050 ac adapter..

Email:PwF8_8oI3tQ@aol.com

2021-03-24

Oem netgear ad 051a ac adapter 5vdc 1a -(+)- 2.5x5.5mm plug-in c,new original 18.5v 2.7a sunydeal st-c-075-18500380ct ac adapter..

Email:Abn_0l7bhOO@yahoo.com

2021-03-22

12v ac / dcpower adapter for neclcd1711m 17in lcd monitor,set01b-60w electronic transformer 12vac 110vac crystal halogen l,genuine fsp group ac/dc adapter fsp150-aban1 19v 7.89a 4 pin din 9na1501611 we are powersellers so be assured you wil,bi bi07-050100-adu ac adapter 5vdc 1a used usb connector class 2,dpd-120500b ac adapter 12vdc 500ma power supply,24v ac adapter for minolta dimage scan elite ii af-2920.ac / dc power adapter for hp photosmart d7355 printer,.

Email:KKP_wQ2M4Qus@aol.com

2021-03-22

5v ac adapter for dlink dp-311p wireless print server.linearity 1 lad1512dc1 ac adapter 15vdc 1a -()- 2.5x5.5mm new p.new ibm lenovo b570 g570 v570 keyboard us black frame 25-011847.genuine danelo for asus a55vm a85vm k46ca laptop charger adapter g62,globtek sys1089-1005-t3 ac dc adapter 5v 2a power supply,wrg10f-055a ac adapter +5.5vdc 1.5a used -(+) 0.5x2.3mm 90° degr.atlinks usa 5-2575 ac adapter 15vdc 500ma -(+) 2x5.5mm 120vac cl,.

Email:Jd5re_UUcQft6U@mail.com

2021-03-19

Finecom js-12060-3k ac adapter 12vdc 6a 4pin replacement power,hp dv6 15.6" led hinges fbut3052010, fbut3053010 new!!,3y3 gpu481201830wa00 ac adapter 12vac

1830ma.4.5v-9.5vdc 100ma ac adapter used cell phone connector power sup.medela
9207010 u090100d31 ac adapter power 9v part for breast pumps medela 9207010
u090100d31 ac adapter power 9v part.hp adp-12hb ac adapter 12vdc 1a used -(+)
3.4x5.5mm 90° connecto,.