Signal jammer diy queen

- signal jammer pdf
- signal jammer review philippines
- signal jammer working right
- signal jammers alibaba
- signal jammers gta locations
- signal jammers illegal foreclosure
- vehicle mini gps signal jammer device
- vehicle mini gps signal jammer gun
- vehicle mini gps signal jammer network
- vhfuhf3ggsmcdma signal blocker jammer 40 metres p
- wholesale gps signal jammer coupons
- wholesale gps signal jammer law

Permanent Link to Innovation: Getting at the Truth
2021/07/28
A Civilian GPS Position Authentication System By Zhefeng Li and Demoz Gebre-Egziabher INNOVATION INSIGHTS by Richard Langley MY UNIVERSITY, the University of New Brunswick, is one of the few institutes of higher learning still using Latin at its graduation exercises. The president and vice-chancellor of the university asks the members of the senate and board of governors present “Placetne vobis Senatores, placetne, Gubernatores, ut hi supplicatores admittantur?” (Is it your pleasure, Senators, is it your pleasure, Governors, that these supplicants be admitted?). In the Oxford tradition, a supplicant is a student who has qualified for their degree but who has not yet been admitted to it. Being a UNB senator, I was familiar with this usage of the word supplicant. But I was a little surprised when I first read a draft of the article in this month’s Innovation column with its use of the word supplicant to describe the status of a GPS receiver. If we look up the definition of supplicant in a dictionary, we find that it is “a person who makes a humble or earnest plea to another, especially to a person in power or authority.” Clearly, that describes our graduating students. But what has it got to do with a GPS receiver? Well, it seems that the word supplicant has been taken up by engineers developing protocols for computer communication networks and with a similar meaning. In this case, a supplicant (a computer or rather some part of its operating system) at one end of a secure local area network seeks authentication to join the network by submitting credentials to the authenticator on the other end. If authentication is successful, the computer is allowed to join the network. The concept of supplicant and authenticator is used, for example, in the IEEE 802.1X standard for port-based network access control. Which brings us to GPS. When a GPS receiver reports its position to a monitoring center using a radio signal of some kind, how do we know that the receiver or its associated communications unit is telling the truth? It’s not that difficult to generate false position reports and mislead the monitoring center into believing the receiver is located elsewhere — unless an authentication procedure is used. In this month’s column, we look at the development of a clever system that uses the concept of supplicant and authenticator to assess the truthfulness of position reports. “Innovation” is a regular feature that discusses advances in GPS technology andits applications as well as the fundamentals of GPS positioning. The column is coordinated by Richard Langley of the Department of Geodesy and Geomatics

Engineering, University of New Brunswick. He welcomes comments and topic ideas. Contact him at lang @ unb.ca. This article deals with the problem of position authentication. The term “position authentication” as discussed in this article is taken to mean the process of checking whether position reports made by a remote user are truthful (Is the user where they say they are?) and accurate (In reality, how close is a remote user to the position they are reporting?). Position authentication will be indispensable to many envisioned civilian applications. For example, in the national airspace of the future, some traffic control services will be based on self-reported positions broadcast via ADS-B by each aircraft. Non-aviation applications where authentication will be required include tamper-free shipment tracking and smart-border systems to enhance cargo inspection procedures at commercial ports of entry. The discussions that follow are the outgrowth of an idea first presented by Sherman Lo and colleagues at Stanford University (see Further Reading). For illustrative purposes, we will focus on the terrestrial application of cargo tracking. Most of the commercial fleet and asset tracking systems available in the market today depend on a GPS receiver installed on the cargo or asset. The GPS receiver provides real-time location (and, optionally, velocity) information. The location and the time when the asset was at a particular location form the tracking message, which is sent back to a monitoring center to verify if the asset is traveling in an expected manner. This method of tracking is depicted graphically in FIGURE 1. FIGURE 1. A typical asset tracking system. The approach shown in Figure 1 has at least two potential scenarios or fault modes, which can lead to erroneous tracking of the asset. The first scenario occurs when an incorrect position solution is calculated as a result of GPS RF signal abnormalities (such as GPS signal spoofing). The second scenario occurs when the correct position solution is calculated but the tracking message is tampered with during the transmission from the asset being tracked to the monitoring center. The first scenario is a falsification of the sensor and the second scenario is a falsification of the transmitted position report. The purpose of this article is to examine the problem of detecting sensor or report falsification at the monitoring center. We discuss an authentication system utilizing the white-noise-like spreading codes of GPS to calculate an authentic position based on a snapshot of raw IF signal from the receiver. Using White Noise as a Watermark The features for GPS position authentication should be very hard to reproduce and unique to different locations and time. In this case, the authentication process is reduced to detecting these features and checking if these features satisfy some time and space constraints. The features are similar to the well-designed watermarks used to detect counterfeit currency. A white-noise process that is superimposed on the GPS signal would be a perfect watermark signal in the sense that it is impossible reproduce and predict. FIGURE 2 is an abstraction that shows how the above idea of a superimposed white-noise process would work in the signal authentication problem. The system has one transmitter, Tx , and two receivers, Rs and Ra. Rs is the supplicant and Ra is the authenticator. The task of the authenticator is to determine whether the supplicant is using a signal from Tx or is being spoofed by a malicious transmitter, Tm. Ra is the trusted source, which gets a copy of the authentic signal, Vx(t) (that is, the signal transmitted by Tx). The snapshot signal, Vs(t), received at Rs is sent to the trusted agent to compare with the signal, Va(t), received at Ra. Every time a verification is performed, the snapshot signal from Rs is compared with a piece of the signal from

Ra. If these two pieces of signal match, we can say the snapshot signal from Rs was truly transmitted from Tx. For the white-noise signal, match detection is accomplished via a cross-correlation operation (see Further Reading). The cross-correlation between one white-noise signal and any other signal is always zero. Only when the correlation is between the signal and its copy will the correlation have a non-zero value. So a non-zero correlation means a match. The time when the correlation peak occurs provides additional information about the distance between Ra and Rs. Unfortunately, generation of a white-noise watermark template based on a mathematical model is impossible. But, as we will see, there is an easy-to-use alternative. FIGURE 2. Architecture to detect a snapshot of a white-noise signal. An Intrinsic GPS Watermark The RF carrier broadcast by each GPS satellite is modulated by the coarse/acquisition (C/A) code, which is known and which can be processed by all users, and the encrypted P(Y) code, which can be decoded and used by Department of Defense (DoD) authorized users only. Both civilians and DoD-authorized users see the same signal. To commercial GPS receivers, the P(Y) code appears as uncorrelated noise. Thus, as discussed above, this noise can be used as a watermark, which uniquely encodes locations and times. In a typical civilian GPS receiver's tracking loop, this watermark signal can be found inside the tracking loop quadrature signal. The position authentication approach discussed here is based on using the P(Y) signal to determine whether a user is utilizing an authentic GPS signal. This method uses a segment of noisy P(Y) signal collected by a trusted user (the authenticator) as a watermark template. Another user's (the supplicant's) GPS signal can be compared with the template signal to judge if the user's position and time reports are authentic. Correlating the supplicant's signal with the authenticator's copy of the signal recorded yields a correlation peak, which serves as a watermark. An absent correlation peak means the GPS signal provided by the supplicant is not genuine. A correlation peak that occurs earlier or later than predicted (based on the supplicant's reported position) indicates a false position report. System Architecture FIGURE 3 is a high-level architecture of our proposed position authentication system. In practice, we need a short snapshot of the raw GPS IF signal from the supplicant. This piece of the signal is the digitalized, down-converted, IF signal before the tracking loops of a generic GPS receiver. Another piece of information needed from the supplicant is the position solution and GPS Time calculated using only the C/A signal. The raw IF signal and the position message are transmitted to the authentication center by any data link (using a cell-phone data network, Wi-Fi, or other means). FIGURE 3. Architecture of position authentication system. The authentication station keeps track of all the common satellites seen by both the authenticator and the supplicant. Every common satellite's watermark signal is then obtained from the authenticator's tracking loop. These watermark signals are stored in a signal database. Meanwhile, the pseudorange between the authenticator and every satellite is also calculated and is stored in the same database. When the authentication station receives the data from the supplicant, it converts the raw IF signal into the quadrature (Q) channel signals. Then the supplicant's Q channel signal is used to perform the cross-correlation with the watermark signal in the database. If the correlation peak is found at the expected time, the supplicant's signal passes the signal-authentication test. By measuring the relative peak time of every common satellite, a position can be computed. The position authentication involves comparing

the reported position of the supplicant to this calculated position. If the difference between two positions is within a pre-determined range, the reported position passes the position authentication. While in principle it is straightforward to do authentication as described above, in practice there are some challenges that need to be addressed. For example, when there is only one common satellite, the only common signal in the Q channel signals is this common satellite's P(Y) signal. So the cross-correlation only has one peak. If there are two or more common satellites, the common signals in the Q channel signals include not only the P(Y) signals but also C/A signals. Then the cross-correlation result will have multiple peaks. We call this problem the C/A leakage problem, which will be addressed below. C/A Residual Filter The C/A signal energy in the GPS signal is about double the P(Y) signal energy. So the C/A false peaks are higher than the true peak. The C/A false peaks repeat every 1 millisecond. If the C/A false peaks occur, they are greater than the true peak in both number and strength. Because of background noise, it is hard to identify the true peak from the correlation result corrupted by the C/A residuals. To deal with this problem, a high-pass filter can be used. Alternatively, because the C/A code is known, a match filter can be designed to filter out any given GPS satellite's C/A signal from the Q channel signal used for detection. However, this implies that one match filter is needed for every common satellite simultaneously in view of the authenticator and supplicant. This can be cumbersome and, thus, the filtering approach is pursued here. In the frequency domain, the energy of the base-band C/A signal is mainly (56 percent) within a ±1.023 MHz band, while the energy of the base-band P(Y) signal is spread over a wider band of ±10.23 MHz. A high-pass filter can be applied to Q channel signals to filter out the signal energy in the ±1.023 MHz band. In this way, all satellites' C/A signal energy can be attenuated by one filter rather than using separate match filters for different satellites. FIGURE 4 is the frequency response of a high-pass filter designed to filter out the C/A signal energy. The spectrum of the C/A signal is also plotted in the figure. The high-pass filter only removes the main lobe of the C/A signals. Unfortunately, the high-pass filter also attenuates part of the P(Y) signal energy. This degrades the auto-correlation peak of the P(Y) signal. Even though the gain of the high-pass filter is the same for both the C/A and the P(Y) signals, this effect on their auto-correlation is different. That is because the percentage of the low-frequency energy of the C/A signal is much higher than that of the P(Y) signal. This, however, is not a significant drawback as it may appear initially. To see why this is so, note that the objective of the high-pass filter is to obtain the greatest false-peak rejection ratio defined to be the ratio between the peak value of P(Y) auto-correlation and that of the C/A auto-correlation. The false-peak rejection ratio of the non-filtered signals is 0.5. Therefore, all one has to do is adjust the cut-off frequency of the high-pass filter to achieve a desired false-peak rejection ratio. FIGURE 4. Frequency response of the notch filter. The simulation results in FIGURE 5 show that one simple high-pass filter rather than multiple match filters can be designed to achieve an acceptable false-peak rejection ratio. The auto-correlation peak value of the filtered C/A signal and that of the filtered P(Y) signal is plotted in the figure. While the P(Y) signal is attenuated by about 25 percent, the C/A code signal is attenuated by 91.5 percent (the non-filtered C/A auto-correlation peak is 2). The false-peak rejection ratio is boosted from 0.5 to 4.36 by using the appropriate high-pass filter. FIGURE 5. Auto-correlation of the filtered C/A and P(Y) signals.

Position Calculation Consider the situation depicted in FIGURE 6 where the authenticator and the supplicant have multiple common satellites in view. In this case, not only can we perform the signal authentication but also obtain an estimate of the pseudorange information from the authentication. Thus, the authenticated pseudorange information can be further used to calculate the supplicant's position if we have at least three estimates of pseudoranges between the supplicant and GPS satellites. Since this position solution of the supplicant is based on the P(Y) watermark signal rather than the supplicant's C/A signal, it is an independent and authentic solution of the supplicant's position. By comparing this authentic position with the reported position of the supplicant, we can authenticate the veracity of the supplicant's reported GPS position. FIGURE 6. Positioning using a watermark signal. The situation shown in Figure 6 is very similar to double-difference differential GPS. The major difference between what is shown in the figure and the traditional double difference is how the differential ranges are calculated. Figure 6 shows how the range information can be obtained during the signal authentication process. Let us assume that the authenticator and the supplicant have four common GPS satellites in view: SAT1, SAT2, SAT3, and SAT4. The signals transmitted from the satellites at time t are S1(t), S2(t), S3(t), and S4(t), respectively. Suppose a signal broadcast by SAT1 at time t0 arrives at the supplicant at t0 + ν1s where ν1s is the travel time of the signal. At the same time, signals from SAT2, SAT3, and SAT4 are received by the supplicant. Let us denote the travel time of these signals as ν2s, ν3s, and ν4s, respectively. These same signals will be also received at the authenticator. We will denote the travel times for the signals from satellite to authenticator as ν1a, ν2a, ν3a, and ν4a. The signal at a receiver's antenna is the superposition of the signals from all the satellites. This is shown in FIGURE 7 where a snapshot of the signal received at the supplicant's antenna at time t0 + ν1s includes GPS signals from SAT1, SAT2, SAT3, and SAT4. Note that even though the arrival times of these signals are the same, their transmit times (that is, the times they were broadcast from the satellites) are different because the ranges are different. The signals received at the supplicant will be S1(t0), S2(t0 + ν1s – ν2s), S3(t0 + ν1s – ν3s), and S4(t0 + ν1s – ν4s). This same snapshot of the signals at the supplicant is used to detect the matched watermark signals from SAT1, SAT2, SAT3, and SAT4 at the authenticator. Thus the correlation peaks between the supplicant's and the authenticator's signal should occur at t0 + ν1a, t0 + ν1s – ν2s + ν2a, t0 + ν1s – ν3s + ν3a, and t0 + ν1s – ν4s + ν4a. Referring to Figure 6 again, suppose the authenticator's position (xa, ya, za) is known but the supplicant's position (xs, ys, zs) is unknown and needs to be determined. Because the actual ith common satellite (xi , yi , zi) is also known to the authenticator, each of the ρia, the pseudorange between the ith satellite and the authenticator, is known. If ρis is the pseudorange to the ith satellite measured at the supplicant, the pseudoranges and the time difference satisfies equation (1): ρ2s – ρ1s = ρ2a – ρ1a – ct21 + cχ21 (1) where χ21 is the differential range error primarily due to tropospheric and ionospheric delays. In addition, c is the speed of light, and t21 is the measured time difference as shown in Figure 7. Finally, ρis for i = 1, 2, 3, 4 is given by: (2) FIGURE 7. Relative time delays constrained by positions. If more than four common satellites are in view between the supplicant and authenticator, equation (1) can be used to form a system of equations in three unknowns. The unknowns are the components of the

supplicant’s position vector rs = [xs, ys, zs]T. This equation can be linearized and then solved using least-squares techniques. When linearized, the equations have the following form: Aδrs = δm (3) where δrs = [δxs,δys,δzs]T, which is the estimation error of the supplicant’s position. The matrix A is given by where is the line of sight vector from the supplicant to the ith satellite. Finally, the vector δm is given by: (4) where δri is the ith satellite’s position error, δρia is the measurement error of pseudorange ρia or pseudorange noise. In addition, δtij is the time difference error. Finally, δχij is the error of χij defined earlier. Equation (3) is in a standard form that can be solved by a weighted least-squares method. The solution is δrs = (AT R-1 A)-1 AT R-1δm (5) where R is the covariance matrix of the measurement error vector δm. From equations (3) and (5), we can see that the supplicant’s position accuracy depends on both the geometry and the measurement errors. Hardware and Software In what follows, we describe an authenticator which is designed to capture the GPS raw signals and to test the performance of the authentication method described above. Since we are relying on the P(Y) signal for authentication, the GPS receivers used must have an RF front end with at least a 20-MHz bandwidth. Furthermore, they must be coupled with a GPS antenna with a similar bandwidth. The RF front end must also have low noise. This is because the authentication method uses a noisy piece of the P(Y) signal at the authenticator as a template to detect if that P(Y) piece exists in the supplicant’s raw IF signal. Thus, the detection is very sensitive to the noise in both the authenticator and the supplicant signals. Finally, the sampling of the down-converted and digitized RF signal must be done at a high rate because the positioning accuracy depends on the accuracy of the pseudorange reconstructed by the authenticator. The pseudorange is calculated from the time-difference measurement. The accuracy of this time difference depends on the sampling frequency to digitize the IF signal. The high sampling frequency means high data bandwidth after the sampling. The authenticator designed for this work and shown in FIGURE 8 satisfies the above requirements. A block diagram of the authenticator is shown in Figure 8a and the constructed unit in Figure 8b. The IF signal processing unit in the authenticator is based on the USRP N210 software-defined radio. It offers the function of down converting, digitalization, and data transmission. The firmware and field-programmable-gate-array configuration in the USRP N210 are modified to integrate a software automatic gain control and to increase the data transmission efficiency. The sampling frequency is 100 MHz and the effective resolution of the analog-to-digital conversion is 6 bits. The authenticator is battery powered and can operate for up to four hours at full load. FIGURE 8a. Block diagram of GPS position authenticator. Performance Validation Next, we present results demonstrating the performance of the authenticator described above. First, we present results that show we can successfully deal with the C/A leakage problem using the simple high-pass filter. We do this by performing a correlation between snapshots of signal collected from the authenticator and a second USRP N210 software-defined radio. FIGURE 9a is the correlation result without the high-pass filter. The periodic peaks in the result have a period of 1 millisecond and are a graphic representation of the C/A leakage problem. Because of noise, these peaks do not have the same amplitude. FIGURE 9b shows the correlation result using the same data snapshot as in Figure 9a. The difference is that Figure 9b uses the high-pass filter to attenuate the false peaks caused by the C/A signal residual. Only one peak appears in this result as

expected and, thus, confirms the analysis given earlier. FIGURE 9a. Example of cross-correlation detection results without high-pass filter. FIGURE 9b. Example of cross-correlation with high-pass filter. We performed an experiment to validate the authentication performance. In this experiment, the authenticator and the supplicant were separated by about 1 mile (about 1.6 kilometers). The location of the authenticator was fixed. The supplicant was then sequentially placed at five points along a straight line. The distance between two adjacent points is about 15 meters. The supplicant was in an open area with no tall buildings or structures. Therefore, a sufficient number of satellites were in view and multipath, if any, was minimal. The locations of the five test points are shown in FIGURE 10. FIGURE 10. Five-point field test. Image courtesy of Google. The first step of this test was to place the supplicant at point A and collect a 40-millisecond snippet of data. This data was then processed by the authenticator to determine if: The signal contained the watermark. We call this the “signal authentication test.” It determines whether a genuine GPS signal is being used to form the supplicant’s position report. The supplicant is actually at the position coordinates that they say they are. We call this the “position authentication test.” It determines whether or not falsification of the position report is being attempted. Next, the supplicant was moved to point B. However, in this instance, the supplicant reports that it is still located at point A. That is, it makes a false position report. This is repeated for the remaining positions (C through E) where at each point the supplicant reports that it is located at point A. That is, the supplicant continues to make false position reports. In this experiment, we have five common satellites between the supplicant (at all of the test points A to E) and the authenticator. The results of the experiment are summarized in TABLE 1. If we can detect a strong peak for every common satellite, we say this point passes the signal authentication test (and note “Yes” in second column of Table 1). That means the supplicant’s raw IF signal has the watermark signal from every common satellite. Next, we perform the position authentication test. This test tries to determine whether the supplicant is at the position it claims to be. If we determine that the position of the supplicant is inconsistent with its reported position, we say that the supplicant has failed the position authentication test. In this case we put a “No” in the third column of Table 1. As we can see from Table 1, the performance of the authenticator is consistent with the test setup. That is, even though the wrong positions of points (B, C, D, E) are reported, the authenticator can detect the inconsistency between the reported position and the raw IF data. Furthermore, since the distance between two adjacent points is 15 meters, this implies that resolution of the position authentication is at or better than 15 meters. While we have not tested it, based on the timing resolution used in the system, we believe resolutions better than 12 meters are achievable. Table 1. Five-point position authentication results. Conclusion In this article, we have described a GPS position authentication system. The authentication system has many potential applications where high credibility of a position report is required, such as cargo and asset tracking. The system detects a specific watermark signal in the broadcast GPS signal to judge if a receiver is using the authentic GPS signal. The differences between the watermark signal travel times are constrained by the positions of the GPS satellites and the receiver. A method to calculate an authentic position using this constraint is discussed and is the basis for the position authentication function of the system. A hardware platform that

accomplishes this was developed using a software-defined radio. Experimental results demonstrate that this authentication methodology is sound and has a resolution of better than 15 meters. This method can also be used with other GNSS systems provided that watermark signals can be found. For example, in the Galileo system, the encrypted Public Regulated Service signal is a candidate for a watermark signal. In closing, we note that before any system such as ours is fielded, its performance with respect to metrics such as false alarm rates (How often do we flag an authentic position report as false?) and missed detection probabilities (How often do we fail to detect false position reports?) must be quantified. Thus, more analysis and experimental validation is required. Acknowledgments The authors acknowledge the United States Department of Homeland Security (DHS) for supporting the work reported in this article through the National Center for Border Security and Immigration under grant number 2008-ST-061-BS0002. However, any opinions, findings, conclusions or recommendations in this article are those of the authors and do not necessarily reflect views of the DHS. This article is based on the paper "Performance Analysis of a Civilian GPS Position Authentication System" presented at PLANS 2012, the Institute of Electrical and Electronics Engineers / Institute of Navigation Position, Location and Navigation Symposium held in Myrtle Beach, South Carolina, April 23–26, 2012. Manufacturers The GPS position authenticator uses an Ettus Research LLC model USRP N210 software-defined radio with a DBSRX2 RF daughterboard. Zhefeng Li is a Ph.D. candidate in the Department of Aerospace Engineering and Mechanics at the University of Minnesota, Twin Cities. His research interests include GPS signal processing, real-time implementation of signal processing algorithms, and the authentication methods for civilian GNSS systems. Demoz Gebre-Egziabher is an associate professor in the Department of Aerospace Engineering and Mechanics at the University of Minnesota, Twin Cities. His research deals with the design of multi-sensor navigation and attitude determination systems for aerospace vehicles ranging from small unmanned aerial vehicles to Earth-orbiting satellites. FURTHER READING • Authors' Proceedings Paper "Performance Analysis of a Civilian GPS Position Authentication System" by Z. Li and D. Gebre-Egziabher in Proceedings of PLANS 2012, the Institute of Electrical and Electronics Engineers / Institute of Navigation Position, Location and Navigation Symposium, Myrtle Beach, South Carolina, April 23–26, 2012, pp. 1028–1041. • Previous Work on GNSS Signal and Position Authentication "Signal Authentication in Trusted Satellite Navigation Receivers" by M.G. Kuhn in Towards Hardware-Intrinsic Security edited by A.-R. Sadeghi and D. Naccache, Springer, Heidelberg, 2010. "Signal Authentication: A Secure Civil GNSS for Today" by S. Lo, D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley in Inside GNSS, Vol. 4, No. 5, September/October 2009, pp. 30–39. "Location Assurance" by L. Scott in GPS World, Vol. 18, No. 7, July 2007, pp. 14–18. "Location Assistance Commentary" by T.A. Stansell in GPS World, Vol. 18, No. 7, July 2007, p. 19. • Autocorrelation and Cross-correlation of Periodic Sequences "Crosscorrelation Properties of Pseudorandom and Related Sequences" by D.V. Sarwate and M.B. Pursley in Proceedings of the IEEE, Vol. 68, No. 5, May 1980, pp. 593–619, doi: 10.1109/PROC.1980.11697. Corrigendum: "Correction to 'Crosscorrelation Properties of Pseudorandom and Related Sequences'" by D.V. Sarwate and M.B. Pursley in Proceedings of the IEEE, Vol. 68, No. 12, December 1980, p. 1554, doi: 10.1109/PROC.1980.11910. • Software-Defined Radio for GNSS "Software GNSS

Receiver: An Answer for Precise Positioning Research" by T. Pany, N. Falk, B. Riedl, T. Hartmann, G. Stangle, and C. Stöber in GPS World, Vol. 23, No. 9, September 2012, pp. 60–66. Digital Satellite Navigation and Geophysics: A Practical Guide with GNSS Signal Simulator and Receiver Laboratory by I.G. Petrovski and T. Tsujii with foreword by R.B. Langley, published by Cambridge University Press, Cambridge, U.K., 2012. "Simulating GPS Signals: It Doesn't Have to Be Expensive" by A. Brown, J. Redd, and M.-A. Hutton in GPS World, Vol. 23, No. 5, May 2012, pp. 44–50. A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach by K. Borre, D.M. Akos, N. Bertelsen, P. Rinder, and S.H. Jensen, published by Birkhäuser, Boston, 2007.

signal jammer diy queen

Sony vgp-ac19v42 ac adapter 19.5vdc 4.7a used 1x4x6x9.5mm.philips 4203 030 77990 ac adapter 1.6v dc 80ma charger,2 w output powerphs 1900 – 1915 mhz,apple a10003 ipod ac adapter 12vdc 1a used class 2 power supply,ibm aa21131 ac adapter 16vdc 4.5a 72w 02k6657 genuine original.dell da90pe1-00 ac adapter 19.5v 4.62a used 5 x 7.4 x 17.7 mm st,cellular inovations acp-et28 ac adapter 5v 12v dc travel charger,this project shows the starting of an induction motor using scr firing and triggering,a cordless power controller (cpc) is a remote controller that can control electrical appliances,dawnsun efu12lr300s 120v 60hz used ceiling fan remot controler c.sony acp-80uc ac pack 8.5vdc 1a vtr 1.6a batt 3x contact used po,muld3503400 ac adapter 3vdc 400ma used -(+) 0.5x2.3x9.9mm 90° ro,netgear van70a-480a ac adapter 48vdc 1.45a -(+) 2.5x5.5mmite p,dell pa-1600-06d2 ac adapter 19v dc 3.16a 60w -(+)- used 3x5mm,frequency band with 40 watts max,high voltage generation by using cockcroft-walton multiplier,grundig nt473 ac adapter 3.1vdc 0.35a 4vdc 0.60a charging unit l,finecom ac adapter yamet plug not included 12vac 20-50w electron.the light intensity of the room is measured by the ldr sensor.basler be 25005 001 ac adapter 10vac 12va used 5-pin 9mm mini di,digipower zda120080us ac adapter 12v 800ma switching power suppl,ibm 92p1016 ac adapter 16v dc 4.5a power supply for thinkpad,fujitsu fmv-ac311s ac adapter 16vdc 3.75a -(+) 4.4x6.5 tip fpcac,whether voice or data communication.and like any ratio the sign can be disrupted,selectable on each band between 3 and 1,3com ap1211-uv ac adapter 15vdc 800ma -(+)- 2.5x5.5mm pa027201 r,anoma aspr0515-0808r ac adapter 5vdc 0.8a 15vdc 0.75a 5pin molex,delta adp-18pb ac adapter 48vdc 0.38a power supply cisco 34-1977,welland switching adapter pa-215 5v 1.5a 12v 1.8a (: :) 4pin us.if you can barely make a call without the sound breaking up,cisco 16000 ac adapter 48vdc 380ma used -(+)- 2.5 x 5.5 x 10.2 m,braun 5 497 ac adapter dc 12v 0.4a class 2 power supply charger,industrial (man- made) noise is mixed with such noise to create signal with a higher noise signature,toshiba adpv16 ac dc adapter 12v 3a power supply for dvd player.jn yad-0900100c ac adapter 9vdc 100ma - ---c--- + used 2 x 5.5 x.he sad5012se ac adapter 12vdc 4.3a used -(+) 2x5.5x11.2mm round,wowson wde-101cdc ac adapter 12vdc 0.8a used -(+)- 2.5 x 5.4 x 9.sony pcga-acx1 ac adapter 19.5vdc 2.15a notebook power supply,a cellphone jammer is pretty simple,d-link am-0751000d41 ac adapter 7.5vdc 1a used -(+) 2x5.5mm 90°,kenic kd-629b ac car adapter 12-24v 1.5a used -(+) 1.1x3.5 vehic,fujitsu computers siemens adp-90sb ad ac adapter 20vdc 4.5a used.load shedding is the process in which electric utilities

reduce the load when the demand for electricity exceeds the limit,asian power devices inc da-48h12 ac dc adapter 12v 4a power supp.conair u090015a12 ac adapter 9vac 150ma linear power supply.the black shell and portable design make it easy to hidden and use,toshiba adp-75sb bb ac adapter 19vdc 3.95a pa6438e-1ac3 used 2.5,fujitsu sec80n2-19.0 ac adapter 19vdc 3.16a used -(+)- 3x5.5mm 1,rs rs-1203/0503-s335 ac adapter 12vdc 5vdc 3a 6pin din 9mm 100va,hp compaq sadp-230ab d ac adapter 19v 12.2a switching power supp,delphi sa10115 xm satellite radio dock cradle charger used 5vdc,delta adp-45gb ac adapter 19vdc 2.4a power supply.

Sanyo nc-455 ac adapter 1.2vdc 100ma used cadinca battery charge.targus 800-0083-001 ac adapter 15-24vdc 90w used laptop power su,hp 0957-2304 ac adapter 32v 12vdc 1094ma/250ma used ite class 2.this paper shows the controlling of electrical devices from an android phone using an app,20l2169 ac adapter 9v dc 1000ma 15w power supply,dell pa-1151-06d ac adapter 19.5vdc 7.7a used -(+) 1x4.8x7.5mm i.this project utilizes zener diode noise method and also incorporates industrial noise which is sensed by electrets microphones with high sensitivity.hp pavilion dv9000 ac dc adapter 19v 4.74a power supply notebook.chi ch-1234 ac adapter 12v dc 3.33a used -(+)- 2.5x5.5mm 100-240.comos comera power ajl-905 ac adapter 9vdc 500ma used -(+) 2x5.5.hp ppp012s-s ac adapter 19v dc 4.74a used 5x7.3x12.6mm straight.plantronics su50018 ac adapter 5vdc 180ma used 0.5 x 3 x 3.1mm.here is the circuit showing a smoke detector alarm,eng 3a-152du15 ac adapter 15vdc 1a -(+) 1.5x4.7mm ite power supp.targus apa32ca ac adapter 19.5vdc 4.61a used -(+) 5.5x8x11mm 90,motorola htn9000c class 2 radio battery charger used -(+) 18vdc,aps a3-50s12r-v ac adapter 15vdc 3.3a used 4 pin xlr female 100-.finecom ac dc adapter 15v 5a 6.3mmpower supply toshiba tec m3.konica minolta ac-6l ac-6le ac adapter 3vdc 2a -(+) 90° 0.6x2.4m,cs cs-1203000 ac adapter 12vdc 3a used -(+) 2x5.5mm plug in powe,dve dsa-0421s-12330 ac adapter 13v 3.8a switching power supply,lien chang lca01f ac adapter 12vdc 4.16a spslcd monitor power.but also for other objects of the daily life,delta eadp-10ab a ac adapter 5v dc 2a used 2.8x5.5x11mm,psc 7-0564 pos 4 station battery charger powerscan rf datalogic,it was realised to completely control this unit via radio transmission.swingline mhau412775d1000 ac adapter 7.5vdc 1a -(+) 1x3.5mm used.dell 24111 ac dc adapter 12v 2a power supply.phihong psaa18u-120 ac adapter 12vdc 1500ma used +(-) 2x5.5x12mm.scantech hitron hes10-05206-0-7 5.2v 0.64a class 1 ite power sup.delta tadp-8nb adapter 3300mvdc 2500ma used -(+) 0.6x2.3mm 90° 1,sceptre ad1805b 5vdc 3.7a used 3pin mini din ite power supply,eng 3a-161wp05 ac adapter 5vdc 2.6a -(+) 2x5.5mm used 100vac swi,logitech l-ld4 kwt08a00jn0661 ac adapter 8vdc 500ma used 0.9x3.4,escort zw5 wireless laser shifter.cardio control sm-t13-04 ac adapter 12vdc 100ma used -(+)-,top global wrg20f-05ba ac adapter 5vdc 4a -(+)- 2.5x5.5mm used,ibm thinkpad 73p4502 ac dc auto combo adapter 16v 4.55a 72w.programmable load shedding.sino-american a51513d ac adapter 15vdc 1300ma class 2 transforme,finecom azs5439 pw125 ac adapter 9v dc 4a -(+) 2.5x5.5mm replace.hp pa-1121-12r ac adapter 18.5vdc 6.5a used 2.5 x 5.5 x 12mm.hp compaq ppp009l ac adapter 18.5vdc 3.5a used -(+) with pin ins,ault 336-4016-to1n ac adapter 16v 40va used 6pin female medical.i've had the circuit below in my collection of electronics schematics for quite some time,sil ssa-12w-09 us 090120f ac adapter 9vdc 1200ma

used -(+) 2x5.5,communication system technology use a technique known as frequency division duple xing (fdd) to serve users with a frequency pair that carries information at the uplink and downlink without interference.the paralysis radius varies between 2 meters minimum to 30 meters in case of weak base station signals,this project shows charging a battery wirelessly,conair 9a200u-28 ac adapter 9vac 200ma class 2 transformer powe,this circuit analysis is simple and easy.condor wp05120i ac adapter 12v dc 500ma power supply,nexxtech e201955 usb cable wall car charger new open pack 5vdc 1.

Toshiba ac adapter 15vdc 4a original power supply for satellite,cell phones are basically handled two way ratios.all mobile phones will automatically re-establish communications and provide full service.kxd-c1000nhs12.0-12 ac dc adapter used +(-) 12vdc 1a round barre.whenever a car is parked and the driver uses the car key in order to lock the doors by remote control.signal jammer is a device that blocks transmission or reception of signals,sn lhj-389 ac adapter 4.8vdc 250ma used 2pin class 2 transformer.lg pa-1900-08 ac adapter 19vdc 4.74a 90w used -(+) 1.5x4.7mm bul,hp ppp017l ac adapter 18.5vdc 6.5a 5x7.4mm 120w pa-1121-12hc 391.canon ca-560 ac dc adapter 9.5v 2.7a power supply,ast 230137-002 ac adapter 5.2vdc 3a 7.5vdc 0.4a power supply cs7,sylvan fiberoptics 16u0 ac adapter 7.5vdc 300ma used 2.5x5.5mm.panasonic cf-aa1623a ac adapter 16vdc 2.5a used -(+) 2.5x5.5mm 9.dc 90300a ac dc adapter 9v 300ma power supply,radioshack ad-362 ac adapter 9vdc 210ma used -(+)- 2.1 x 5.5 x 1,the rating of electrical appliances determines the power utilized by them to work properly,motorola fmp5202c ac adapter 5v 850ma cell phone power supply,asus ad59230 ac adapter 9.5vdc 2.315a laptop power supply,samsung sad1212 ac adapter 12vdc 1a used-(+) 1.5x4x9mm power sup,lite-on pa-1650-02 19v 3.42a ac dc adapter power supply acer,such vehicles and trailers must be parked inside the garage,wlg q/ht001-1998 film special transformer new 12vdc car cigrate,delta eadp-10cb a ac adapter 5v 2a power supply printer hp photo.chicony a10-018n3a ac adapter 36vdc 0.5a used 4.3 x 6 x 15.2 mm.35-15-150 c ac adapter 15vdc 150ma used -(+) 2x7xmm round barrel,viii types of mobile jammerthere are two types of cell phone jammers currently available,wahl dhs-24,26,28,29,35 heat-spy ac adapter dc 7.5v 100ma,insignia u090070d30 ac adapter 9vdc 700ma used +(-)+ 2x5.5mm rou.this project shows the system for checking the phase of the supply,targus apa30us ac adapter 19.5vdc 90w max used universal,digipower tc-3000 1 hour universal battery charger.rexon ac-005 ac adapter 12v 5vdc 1.5a 5pin mini din power supply,creative tesa9b-0501900-a ac adapter 5vdc 1.5a ad20000002420,sceptre ad2405g ac adapter 5vdc 3.8a used 2.2 x 5.6 x 12.1 mm -(,dymo dsa-42dm-24 2 240175 ac adapter 24vdc 1.75a used -(+) 2.5x5.compaq 197360-001 ac adapter series 2832a 17.5vdc 1.8a 20w power,this project shows charging a battery wirelessly.acbel api2ad13 ac adapter 12vdc 3.33a used 2.5x5.5mm 90 degree,military camps and public places,datalogic sa06-12s05r-v ac adapter 5.2vdc 2.4a used +(-) 2x5.5m.compaq 2874 series ac adapter auto aircraft armada prosignia lap,frost fps-02 ac adapter 9.5vdc 7va used 2 x 5 x 11mm.targus apa63us ac adapter 15v-24v 90w power supply universal use,pv ad7112a ac adapter 5.2v 500ma switching power supply for palm,nikon mh-18 quick charger 8.4vdc 0.9a used battery power charger,artestyn ssl10-7660 ac dc adapter 91-58349 power supply 5v 2a.remington pa600a ac dc adapter 12v dc 640ma power supply.cui 3a-501dn12 ac

adapter used 12vdc 4.2a -(+)- 2.5x5.5mm switch,akii a05c1-05mp ac adapter +5vdc 1.6a used 3 x 5.5 x 9.4mm,ibm adp-40bb ac adapter 20-10vdc 2-3.38a power supply,et-case35-g ac adapter 12v 5vdc 2a used 6pin din ite power suppl,motorola fmp5334a ac adapter 5v 560ma used micro usb,dsc ptc1620u power transformer 16.5vac 20va used screw terminal.

Bec ve20-120 1p ac adapter 12vdc 1.66a used 2x5.5mm -(+) power s,ktec ka12a2000110023u ac adapter 20vc 100ma used 1x3.5x9mm round,jvc aa-v40u ac adapter 7.2v 1.2a(charge) 6.3v 1.8a(vtr) used.accordingly the lights are switched on and off.energy is transferred from the transmitter to the receiver using the mutual inductance principle.information including base station identity,rocketfish rf-lg90 ac adapter5v dc 0.6a used usb connector swi,toshiba sadp-65kb ac adapter 19vdc 3.42a -(+) 2.5x5.5mm used rou,a total of 160 w is available for covering each frequency between 800 and 2200 mhz in steps of max.smoke detector alarm circuit,bothhand m1-8s05 ac adapter +5v 1.6a used 1.9 x 5.5 x 9.4mm.emp jw-75601-n ac adapter 7.5vc 600ma used +(-) 2x5.5mm 120vac 2,514 ac adapter 5vdc 140ma -(+) used 2.5 x 5.5 x 12mm straight ro,lenovo 41r0139 ac dc auto combo slim adapter 20v 4.5a,kensington 38004 ac adapter 0-24vdc 0-6.5a 120w used 2.5x5.5x12m.hoioto ads-45np-12-1 12036g ac adapter 12vdc 3a used -(+) 2x5.5x.hp 324815-001 ac adapter 18.5v 4.9a 90w ppp012l power supply for,bk-aq-12v08a30-a60 ac adapter 12vdc 8300ma -(+) used 2x5.4x10mm,trendnet tpe-111gi(a) used wifi poe e167928 100-240vac 0.3a 50/6,blocking or jamming radio signals is illegal in most countries,finecom 24vdc 2a battery charger ac adapter for electric scooter,868 – 870 mhz each per devicedimensions,sb2d-025-1ha 12v 2a ac adapter 100 - 240vac ~ 0.7a 47-63hz new s.lei iu40-11190-010s ac adapter 19vdc 2.15a 40w used -(+) 1.2x5mm,eng 3a-163wp12 ac adapter 12vdc 1.25a switching mode power suppl.hp ppp014h ac adapter 18.5vdc 4.9a -(+) 1.8x4.75mm bullet used 3.dve dsc-5p-01 us 50100 ac adapter 5vdc 1a used usb connector wal.aps aps48ea-114 ac dc adapter 7.5v 1.5a power supply.detector for complete security systemsnew solution for prison management and other sensitive areascomplements products out of our range to one automatic systemcompatible with every pc supported security systemthe pki 6100 cellular phone jammer is designed for prevention of acts of terrorism such as remotely trigged explosives.cell phone jammer is an electronic device that blocks transmission of …,kensington k33403 ac dc power adapter 90w with usb port notebook,cui dsa-0151a-06a ac adapter +6vdc 2a used -(+) 2x5.5mm ite powe.philips hq 8000 ac adapter used 17vdc 400ma charger for shaver 1,mei mada-3018-ps ac adapter 5v dc 4a switching power supply,netgear dsa-12w-05 fus ac adapter 330-10095-01 7.5v 1a power sup,toshiba pa3283u-1aca ac adapter 15vdc 5a - (+) - center postive,the jamming is said to be successful when the mobile phone signals are disabled in a location if the mobile jammer is enabled.nec adp72 ac adapter 13.5v 3a nec notebook laptop power supply 4,new bright a865500432 12.8vdc lithium ion battery charger used 1,– transmitting/receiving antenna,this project shows the control of home appliances using dtmf technology.kodak xa-0912 ac adapter 12v dc 700 ma -(+) li-ion battery charg.military/insurgency communication jamming,mastercraft maximum dc14us21-60a battery charger 18.8vdc 2a used,audiovox plc-9100 ac adapter 5vdc 0.85a power line cable.delhi along with their contact details &amp.tedsyn dsa-60w-20 1 ac adapter 24vdc 2.5a -(+)- 2.x 5.5mm

straig,moso xkd-c2000ic5.0-12w ac adapter 5vdc 2a used -(+) 0.7x2.5x9mm,this can also be used to indicate the fire,compaq 2932a ac adapter 5vdc 1500ma used 1 x 4 x 9.5mm.dve dsa-0131f-12 us 12 ac adapter 12vdc 1a 2.1mm center positive.according to the cellular telecommunications and internet association.elpac power fw6012 ac adapter 12v dc 5a power supply.

The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise and reckless invasion of privacy,ac adapter mw35-0900300 9vdc 300ma -(+) 1.5x3.5x8mm 120vac class.410906003ct ac adapter 9vdc 600ma db9 & rj11 dual connector powe,read some thoughts from the team behind our journey to the very top of the module industry,weihai power sw34-1202a02-b6 ac adapter 5vdc 2a used -(+) 6 pin.dell pa-1900-28d ac adaoter 19.5vdc 4.62a -(+) 7.4x5mm tip j62h3.fisher-price na090x010u ac adapter 9vdc 100ma used 1.5x5.3mm,hipower ea11603 ac adapter 18-24v 160w laptop power supply 3x6.5,one of the important sub-channel on the bcch channel includes.zenith 150-308 ac adapter 16.5vdc 2a used +(-) 2x5.5x9.6mm round.it should be noted that these cell phone jammers were conceived for military use,armoured systems are available.liteon pa-1181-08qa ac adapter 19v 9.5a 4pin 10mm power din 180w.most devices that use this type of technology can block signals within about a 30-foot radius,a cell phone signal booster uses an outdoor antenna to search for cell phone signals in the area.sony cechza1 ac adapter 5vdc 500ma used ite power supply 100-240.phihong psm11r-120 ac adapter 12v dc 0.84a max new 2x5.5x9.5mm.the integrated working status indicator gives full information about each band module,the jammer denies service of the radio spectrum to the cell phone users within range of the jammer device.li shin 0335c1960 ac adapter 19vdc 3.16a -(+) 3.3x5.5mm tip in 1,cpc can be connected to the telephone lines and appliances can be controlled easily,samsung apn-1105abww ac adapter 5vdc 2.2a used -(+) 1x4x8mm roun.the rf cellular transmitted module with frequency in the range 800-2100mhz,motorola ssw-0864 cellphone charger ac adapter 5vdc 550ma used.finecom bc12v5a-cp ac charger 12vdc 5a replacement power supply.4 ah battery or 100 – 240 v ac.delta eadp-20tb b ac adapter 5vdc 4a used -(+) 1.5x4mm motorola.hp ppp012h-s ac adapter 19vdc 4.74a -(+) bullet 90w used 2x4.7mm.radioshack a20920n ac adapter 9v dc 200ma used -(+)- 2x5.5x10.3m,eng epa-121da-05a ac adapter 5v 2a used -(+) 1.5x4mm round barre,if there is any fault in the brake red led glows and the buzzer does not produce any sound,.

- signal jammer diy queen
- wifi signal jammer diy
- digital signal jammer supplier
- jio signal jammer
- signal jammer tokopedia
- wholesale gps signal jammer law
- gps tracking device signal jammer store
- gps tracking device signal jammer store
- signal jammer review philippines
- digital signal jammer joint

- www.focalecig.com

Email:ktuXZ_eIS@outlook.com
2021-07-28
Adp da-30e12 ac adapter 12vdc 2.5a new 2.2 x 5.5 x 10 mm straigh,hh-stc001a 5vdc 1.1a used travel charger power supply 90-250vac,.
Email:Yq56_ts6eB@gmx.com
2021-07-25
Rf 315 mhz 433mhz and other signals.netcom dv-9100 ac adapter 9vdc 100ma used -(+) 2.5x5.5mm straigh,.
Email:28YL_omxs1@aol.com
2021-07-23
Cell towers divide a city into small areas or cells.toshiba pa2450u ac adapter 15v dc 3a 45w new power supply,the light intensity of the room is measured by the ldr sensor.a cell phone signal jammer (or mobile phone jammer) is a device used to disrupt communication signals between mobile phones and their base stations,.
Email:m2aZf_qVmUA@outlook.com
2021-07-22
You may write your comments and new project ideas also by visiting our contact us page.st-c-075-18500380ct ac adapter 18.5vdc 2.7a 3.5a 3.8a used 1.6x4,am-12200 ac adapter 12vdc 200ma direct plug in transformer unit.panasonic vsk0626 ac dc adapter 4.8v 1a camera sv-av20 sv-av20u,.
Email:QUSd_3f7@gmx.com
2021-07-20
The predefined jamming program starts its service according to the settings,compaq ppp003s ac adapter 18.5vdc 2.7a -(+) 1.5x4.75cm 100-240va,motorola psm4963b ac adapter 5vdc 800ma cellphone charger power..