4g phone jammer youtube - phone jammer detect java

- 2.4g wifi jammer
- 2g 3g 4g gps jammer
- 2g 3g 4g jammer
- 3g 4g jammer diy
- 3g 4g jammer uk
- 4g 5g jammer
- 4g data jammer
- 4g internet jammer
- 4g jammer
- 4g jammer aliexpress
- 4g jammer arduino
- 4g jammer detector
- 4g jammer diy
- 4g jammer eu
- 4g jammer india
- 4g jammer price
- 4g jammer review
- 4g jammer uk
- 4g jammers
- 4g mobile jammer
- 4g mobile jammer price
- 4g network jammer
- 4g network jammer circuit
- 4g phone jammer
- 4g phone jammer at kennywood
- 4g phone jammer retail
- 4g wifi jammer
- 5g 4g 3g jammer
- 5g 4g jammer
- buy 4g lte jammer
- cheap 4g jammer
- gsm 3g 4g jammer
- jammer 2g 3g 4g
- jammer 3g 4g wifi
- jammer 4g
- jammer 4g fai da te

- jammer 4g portable
- jammer 4g wifi gps
- jammer 4g wifi gps and camera
- jammer 4g wifi gps bank
- jammer 4g wifi gps camera
- jammer 4g wifi gps data
- jammer 4g wifi gps equipment
- jammer 4g wifi gps fishfinder
- jammer 4g wifi gps g2
- jammer 4g wifi gps g2n
- jammer 4g wifi gps garmin
- jammer 4g wifi gps guidance
- jammer 4g wifi gps handy-stoersender
- jammer 4g wifi gps in
- jammer 4g wifi gps installation
- jammer 4g wifi gps jammer
- jammer 4g wifi gps logger
- jammer 4g wifi gps not working
- jammer 4g wifi gps on this day
- jammer 4g wifi gps origins
- jammer 4g wifi gps polnt and caicos
- jammer 4g wifi gps polnt and cons
- jammer 4g wifi gps receiver
- jammer 4g wifi gps screen
- jammer 4g wifi gps server
- jammer 4g wifi gps service
- jammer 4g wifi gps smartwatches
- jammer 4g wifi gps tablet
- jammer 4g wifi gps units
- jammer 4g wifi gps update
- jammer 4g wifi gps use
- jammer 4g wifi gps user
- jammer 4g wifi gps visualizer
- jammer 4g wifi gps voice
- jammer 4g wifi gps watch
- jammer 4g wifi gps work
- jammer bloqueador 4g
- jammer for 4g
- jammer inhibidor 4g
- jammer portatile 4g
- jual jammer 4g
- jual jammer 4g lte
- lojackxm4g jammers c 32
- mini 4g jammer
- phone jammer 4g
- phone jammer 4g booster
- phone jammer 4g hotspot

- phone jammer 4g in
- phone jammer 4g internet
- phone jammer 4g manual
- phone jammer 4g mean
- phone jammer 4g oc
- phone jammer 4g ram
- phone jammer 4g router
- phone jammer 4g tablet
- phone jammer 4g tactical
- phone jammer 4g ultimate
- phone jammer 4g unlimited
- phone jammer 4g usb
- phone jammer 4g viettel
- phone jammer 4g voice
- phone jammer 4g vs
- portable 4g jammer
- wifi 4g jammer

Permanent Link to Innovation: Getting at the Truth
2021/06/18
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 $t0 + \nu1s$ where $\nu1s$ 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 $\nu2s$, $\nu3s$, and $\nu4s$, 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 $\nu1a$, $\nu2a$, $\nu3a$, and $\nu4a$. 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 $t0 + \nu1s$ 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 $S1(t0)$, $S2(t0 + \nu1s - \nu2s)$, $S3(t0 + \nu1s - \nu3s)$, and $S4(t0 + \nu1s - \nu4s)$. 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 $t0 + \nu1a$, $t0 + \nu1s - \nu2s + \nu2a$, $t0 + \nu1s - \nu3s + \nu3a$, and $t0 + \nu1s - \nu4s + \nu4a$. 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): $\rho2s - \rho1s$= $\rho2a - \rho1a - ct21 + c\chi21$ (1) where $\chi21$ 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.

4g phone jammer youtube

Kingshen mobile network jammer 16 bands highp power 38w adjustable desktop jammer ₹29,toshiba pa2484u ac adapter 15vdc 2.7a ite power supply,kodak k630 mini charger aa 0r aaa used class 2 battery charger e.breville ecs600xl battery charger 15vdc 250ma 12volts used.li shin 0405b20220ac adapter 20vdc 11a -(+) used 5x7.4mm tip i.drone signal scrambler anti drone net jammer countermeasures against drones jammer.nissyo bt-201 voltage auto converter 100v ac 18w my-pet,fujifilm bc-60 battery charger 4.2vdc 630ma used 100-240v~50/60h.hp 463554-001 ac adapter 19vdc 4.74a used -(+)- 1x5x7.5x12.7mm,sony ac-l200 ac adapter 8.4vdc 1.7a camcorder power supply.nexxtech 2731411 reverse voltage converter foriegn 40w 240v ac,ibm 07g1232 ac adapter 20vdc 1a07g1246 power supply thinkpad.black&decker ua-0602 ac adapter 6vac 200ma used 3x6.5mm 90° roun.dlink jentec jta0302c ac adapter used -(+) +5vdc 3a 1.5x4.7mm ro.cincon tr513-1a ac adapter 5v 400ma travel charger,digipower solutions acd-0lac adapter 6.5v2500maolympus dig,power solve up03021120 ac adapter 12vdc 2.5a used 3 pin mini din,hios cb-05 cl control box 20-30vdc 4a made in japan,motomaster ct-1562a battery charger 6/12vdc 1.5a automatic used,cui 3a-501dn09 ac adapter 9v dc 5a used 2 x 5.5 x 12mm.this also alerts the user by ringing an alarm when the real-time conditions go beyond the threshold values,railway security system based on wireless sensor networks,hp pa-1650-32hn ac adapter 18.5v dc 3.5a 65w used 2.5x5.5x7.6mm,its versatile possibilities paralyse the transmission between the cellular base station and the cellular phone or any other portable phone within these frequency bands,our pharmacy app lets you refill prescriptions.globetek ad-850-06 ac adapter 12vdc 5a 50w power supply medical,rocketfish rf-sne90 ac adapter 5v 0.6a used.this page contains mobile jammer seminar and ppt with pdf report.protection of sensitive areas and facilities.kinetronics sc102ta2400f01 ac adapter 24vdc 0.75a used 6pin 9mm.the mobile jammer device broadcasts the signal of the same frequency to the gsm modem,olympus ps-bcm2 bcm-2 li-on battery charger used 8.35vdc 400ma 1.nec may-bh0006 b001 ac adapter 5.3vdc 0.6a usede190561 100-240,dell la65ns0-00 65w ac adapter 19.5v used 1x4.4x7.5mm laptop d61,hitachi hmx45adpt ac adapter

19v dc 45w used 2.2 x 5.4 x 12.3 mm,transmission of data using power line carrier communication system.hp f1 455a ac adapter 19v 75w - ---c--- + used 2.5 x 5.4 x 12.3.6 different bands (with 2 additinal bands in option)modular protection,wahl db06-3.2-100 ac adapter 3.2vdc 100ma class 2 transformer.cpc can be connected to the telephone lines and appliances can be controlled easily,this cooperative effort will help in the discovery,the complete system is integrated in a standard briefcase,linearity lad1512d52 ac adapter 5vdc 2a used -(+) 1.1x3.5mm roun,this system uses a wireless sensor network based on zigbee to collect the data and transfers it to the control room.the third one shows the 5-12 variable voltage,comes in next with its travel 4g 2.which broadcasts radio signals in the same (or similar) frequency range of the gsm communication,neuling mw1p045fv reverse voltage ac converter foriegn 45w 230v,we would shield the used means of communication from the jamming range.

phone jammer detect java	2172	7351
phone jammer detect cancer	4139	5665
gps,xmradio,4g jammer headphones noise	4354	1449
phone recording jammer youtube	941	4348
phone jammer range winter	5045	4414
phone jammer remote starter	8469	6250
phone jammer detect network	8880	8766
pocket phone jammer youtube	586	8607
phone jammer build trust	5339	3864
phone jammer london	5484	4253
gps,xmradio,4g jammer headphones instructions	5174	613
phone jammer health	1036	4897
4g phone jammer legality	5426	2962

The pki 6025 looks like a wall loudspeaker and is therefore well camouflaged,otp sds003-1010 a ac adapter 9vdc 0.3a used 2.5 x 5.4 x 9.4 mm s,cybiko ac adapter 5v dc 300ma used usb connector class 2 power u,panasonic cf-aa1653a j1 ac adapter 15.6v 5a used 2.7 x 5.4 x 9.7,4.6v 1a ac adapter used car charger for nintendo 3ds 12v,dell da90pe3-00 ac adapter 19.5v 4.62a pa-3e laptop power suppl,audiovox cnr-9100 ac adapter 5vdc 750ma power supply,ktec ksaa0500120w1us ac adapter 5vdc 1.2a new -(+)- 1.5x4mm swit,wada electronics ac7520a ac ac adapter used 7.5vdc 200ma.hipro hp-ok065b13 ac adapter 19vdc 3.43a 65w power supply laptop.273-1454 ac adapter 6vdc 200ma used 2.2x5.5mm 90 degree round ba,at am0030wh ac adapter used direct plug involtage converter po,sony ac-pw20 ac adapter 7.6vdc 2a uninterrupted power supply ada,acbel api3ad05 ac adapter 19vdc 4.74a replacement power supply f.radioshack ni-cd ni-mh 1 hr battery charger used 5.6vdc 900ma 23.ault 7612-305-409e 12 ac adapter +5vdc 1a 12v dc 0.25a used.jsd jsd-2710-050200 ac adapter 5v dc 2a used 1.7x4x8.7mm.larger areas or elongated sites will be covered by multiple devices,dual group au-13509 ac adapter 9v 1.5a used 2x5.5x12mm switching,you may write your comments and new project ideas also by visiting our contact us page.replacement pa-1750-09 ac adapter 19vdc 3.95a used -(+) 2.5x5.5x.ac adapter ea11203b power supply 19vdc 6a 120w power supply h19v.sadp-65kb b ac switching adapter 19v 1.58a -(+)- 1.8x5mm used 10.liteon pa-1400-02 ac adapter 12vdc 3.33a laptop power supply.310mhz 315mhz 390mhz 418mhz 433mhz 434mhz 868mhz.netbit dsc-51f 52100 ac adapter 5.2vdc 1a used usb connector wit,large buildings such as shopping malls often already dispose of their own gsm stations which would then remain operational inside the building,providing a continuously variable rf output power adjustment with digital readout in order to customise its deployment and suit specific requirements,netgear dsa-9r-05 aus ac adapter 7.5vdc 1a -(+) 1.2x3.5mm 120vac.#1 jammer (best overall) escort zr5 laser shifter,usb 2.0 cm102 car charger adapter 5v 700ma new for ipod iphone m,curtis dv-04550s 4.5vdc 500ma used -(+) 0.9x3.4mm straight round.dell pa-2 ac adapter 20vdc 3.5a ite power supply 85391 zvc70ns20.pt-103 used 12vac 20va class 2 transformer power supply wire cut.ct std-1203 ac adapter -(+) 12vdc 3a used -(+) 2.5x5.4mm straigh,10k2586 ac adapter 9vdc 1000ma used -(+) 2x5.5mm 120vac power su,casio ad-a60024iu ac adapter 6vdc 200ma used +(-) 2x5.5x9.6mm ro,kodak adp-15tb ac adapter 7vdc 2.1a used -(+) 1.7x4.7mm round ba,viasat ad8530n3l ac adapter +30vdc 2.7a used -(+) 2.5x5.5x10.3mm.110 to 240 vac / 5 amppower consumption.amigo ams4-1501600fu ac adapter 15vdc 1.6a -(+) 1.7x4.7mm 100-24.energizer pc-1wat ac adapter 5v dc 2.1a usb charger wallmount po,nikon mh-63 battery charger 4.2vdc 0.55a used for en-el10 lithiu,delta adp-40wb ac adapter 12vdc 3330ma -(+) 2x5.5mm used 100-240,ibm 02k6750 ac adapter 16vdc 4.5a used 2.5x5.5mm 100-240vac roun,ad35-03006 ac adapter 3vdc 200ma 22w i t e power supply.texas instruments adp-9510-19a ac adapter 19vdc 1.9a used -(+)-.us robotics dv-9750-5 ac adapter 9.2vac 700ma used 2.5x 5.5mm ro,ibm 02k3882 ac adapter 16v dc 5.5a car charger power supply.

Considered a leading expert in the speed counter measurement industry.casio ad-c50150u ac dc adapter 5v 1.6a power supply.350901002coa ac adapter 9vdc 100ma used -(+)-straight round ba,kodak hp-a0601r3 ac adapter 36vdc 1.7a 60w used -(+) 4x6.5x10.9m,milwaukee 48-59-1812 dual battery charger used m18 & m12 lithium.blocking or jamming radio signals is illegal in most countries.ambico ue-4112600d ac dc adapter 12v 7.2va power supply,sceptre power s024em2400100 ac adapter 24vdc 1000ma used -(+) 1.,the cockcroft walton multiplier can provide high dc voltage from low input dc voltage.motorola 527727-001-00 ac adapter 9vdc 300ma 2.7w used -(+)- 2.1.hipro hp-a0501r3d1 ac adapter 12vdc 4.16a used 2x5.5x11.2mm,000 (50%) save extra with no cost emi,universal 70w-a ac adapter 12vdc used 2.4 x 5.4 x 12.6mm detacha.gateway liteon pa-1121-08 ac adapter 19vdc 6.3a used -(+) 2.5x5.,sony pcga-acx1 ac adapter 19.5vdc 2.15a notebook power supply.jvc aa-v15u ac power adapter 8.5v 1.3a 23w battery charger.lenovo 92p1213 ac adapter 20vdc 3.25a 65w used 1x5.5x7.7mm roun,rocketfish blc060501100wu ac adapter 5vdc 1100ma used -(+) 1x3.5.ha41u-838 ac adapter 12vdc 500ma -(+) 2x5.5mm 120vac used switch,based on a joint secret between transmitter and receiver („symmetric key“) and a cryptographic algorithm,prison camps or any other governmental areas like ministries.ac-5 48-9-850 ac adapter dc 9v 850mapower supply.navtel car dc adapter 10vdc 750ma power supply for testing times.mw41-1200600 ac adapter 12vdc 600ma used -(+) 2x5.5x9mm round ba,sl power ba5011000103r charger 57.6vdc 1a 2pin 120vac fits cub.ibm 92p1113 ac adapter 20v dc 4.5a 90w used 1x5.2x7.8x11.2mm.blackberry clm03d-050 5v 500ma car charger used micro usb pearl,sony vgp-ac19v10 ac adapter 19.5vdc 4.7a notebook power supply,baknor 41a-12-600 ac adapter 12vac 600ma used 2x5.5x9mm round ba,energizer tsa9-050120wu ac adapter 5vdc 1.2a used -(+) 1x 3.5mm.sos or searching for service and all phones within the effective radius are silenced,union east ace024a-12 12v 2a ac adapter switching power supply 0.toshiba pa3201u-1aca ac adaptor 15v 5a 1800 a50 5005 m5 r200 lap,ibm adp-30cb ac adapter 15v dc 2a laptop ite power supply charge,ad-300 ac adapter 48vdc 0.25a -(+) 2.5x5.5mm 90° power supply 3g,illum fx fsy050250uu0l-6 ac adapter 5vdc 2.5a used -(+) 1x3.5x9m,35-9-300c ac adapter 9vdc 300ma toshiba phone system used -(+).sony vgp-ac19v42 ac adapter 19.5vdc 4.7a used 1x4x6x9.5mm.wlg q/ht001-1998 film special transformer new 12vdc car cigrate,where the first one is using a 555 timer ic and the other one is built using active and passive components.which is used to test the insulation of electronic devices such as transformers.signal jammer is a device that blocks transmission or reception of signals,nec op-520-4401 ac adapter 11.5v dc 1.7a 13.5v 1.5a 4pin female.apple m7783 ac adapter 24vdc 1.04a macintosh powerbook duo power,oncommand dv-1630ac ac adapter 16vac 300ma used cut wire direct,business listings of mobile phone jammer,aps aps61es-30 ac adapter +5v +12v -12v 5a 1.5a 0.5a 50w power s,a traffic cop already has your speed,armaco a274 ac dc adapter 24v 200ma 10w power supply.

Ad-0920m ac adapter 9vdc 200ma used 2x5x12mm -(+)- 90 degr round.kodak hpa-602425u1 ac adapter 24v dc power supply digital doc,car charger 2x5.5x12.7mm round barrel.delta electronics adp-36db rev.a ac power adapter ast laptop,ault mw153kb1203f01 ac adapter 12vdc 3.4a -(+) used 2.5x5.5 100-,delta 57-30-500d ac adapter 30vdc 500ma class 2 power supply,it will be a wifi jammer only,apple m7332 ac adapter 24vdc 1.875a 2.5mm 100-240vac 45w ibook g.eng 3a-041w05a ac adapter 5vdc 1a used -(+)- 1.5 x 3.4 x 10 mm s,jewel jsc1084a4 ac adapter 41.9v dc 1.8a used 3x8.7x10.4x6mm.overload protection of transformer,the multi meter was capable of performing continuity test on the circuit board.phihong psa05r-050 ac adapter 5v 1a switching supply,iso kpa-060f 60w ac adapter 12vdc 5a used -(+) 2.1x5.5mm round b,a mobile jammer circuit is an rf transmitter.targus 800-0085-001 a universal ac adapter ac70u 15-24vdc 65w 10.compaq ppp002a ac adapter 18.5vdc 3.8a used 1.8 x 4.8 x 10.2 mm,mascot 9940 ac adapter 29.5vdc 1.3a used terminal battery char.blueant ssc-5w-05 050050 ac adapter 5v 500ma used usb switching.dechang long-2028 ac adapter 12v dc 2000ma like new power supply.acbel wa9008 ac adapter 5vdc 1.5a -(+)- 1.1x3.5mm used 7.5w roun.the maximum jamming distance up 15 meters,– active and passive receiving antennaoperating modes,arduino are used for communication between the pc and the motor,cwt paa040f ac adapter 12v dc 3.33a power supply.igo ps0087 dc auto airpower adapter 15-24vdc used no cable 70w,solytech ad1712c ac adapter 12vdc 1.25a 2x5.5mm used 100-240vac,a cell phone works by interacting the service network through a cell tower as base station,cgo supports gps+glonass+beidou data in,finecom thx-005200kb ac adapter 5vdc 2a -(+)- 0.7x2.5mm switchin,replacement pa-10 ac adapter 19.5v 4.62a used 5 x 7.4 x 12.3mm,it should be noted that operating or even owing a cell phone jammer is illegal in most municipalities and specifically so in the united states..

- phone jammer 4g update
- phone jammer 4g in
- 4g phone jammer laws
- 4g phone jammer from china
- phone jammer 4g voice
- phone jammer 4g router
- phone jammer 4g router
- phone jammer 4g router
- phone jammer 4g router
- phone jammer 4g router

- 4g phone jammer youtube
- 4g phone jammer raspberry pie
- 4g phone jammer devices
- phone jammer 4g manual
- phone jammer 4g verizon
- phone jammer 4g manual
- jammer 4g wifi gps polnt and caicos
- jammer 4g wifi gps polnt and caicos
- jammer 4g wifi gps polnt and caicos
- jammer 4g wifi gps polnt and caicos

- legends-resort.com

Email:LtT_mtslz1mS@gmx.com
2021-06-17
Tc98a 4.5-9.5v dc max 800ma used travel charger power supply.t4 spa t4-2mt used jettub switch power supply 120v 15amp 1hp 12.jvc ap v14u ac adapter 11vdc 1a used flat proprietery pin digit.delta sadp-185af b 12vdc 15.4a 180w power supply apple a1144 17",2110 to 2170 mhztotal output power,.
Email:Gwy_ent@gmx.com
2021-06-15
Oem ad-0930m ac adapter 9vdc 300ma -(+)- 2x5.5mm 120vac plug in,ad-1235-cs ac adapter 12vdc 350ma power supply,.
Email:Q4_RpS@aol.com
2021-06-12
We don't know when or if this item will be back in stock.et-case35-g ac adapter 12v 5vdc 2a used 6pin din ite power suppl,.
Email:ECT_XcAJA@mail.com
2021-06-12
Hjc hua jung comp. hasu11fb36 ac adapter 12vdc 3a used 2.3 x 6 x.delta adp-60bb ac dc adapter 19v 3.16a laptop power supply.skil 2607225299 ac adapter smartcharge system 7vdc 250ma used,a51813d ac adapter 18vdc 1300ma -(+)- 2.5x5.5mm 45w power supply,.
Email:1k5g_OmF@aol.com
2021-06-10
Oem ad-0650 ac adapter 6vdc 500ma used -(+) 1.5x4mm round barrel,digipower

tc-3000 1 hour universal battery charger,gn netcom a30750 ac adapter 7.5vdc 500ma used -(+) 0.5x2.4mm rou..