Phone jammer arduino kit , phone jammer project board

- 4g 5g jammer
- 4g 5g jammer
- 5g jammer
- 5g jammer
- 5g 4g 3g jammer
- 5g 4g 3g jammer
- 5g 4g jammer
- 5g 4g jammer
- 5g all jammer
- 5g all jammer
- 5g cell jammer
- 5g cell jammer
- 5g cell phone jammer
- 5g cell phone jammer
- 5g cell phone signal jammer
- 5g cell phone signal jammer
- 5g frequency jammer
- 5g frequency jammer
- 5g jammer
- 5g jammer
- 5g jammer uk
- 5g jammer uk
- 5g jammers
- 5g jammers
- 5g mobile jammer
- 5g mobile jammer
- 5g mobile phone jammer
- 5g mobile phone jammer
- 5g phone jammer
- 5g phone jammer
- 5g signal jammer
- 5g signal jammer
- 5g wifi jammer
- 5g wifi jammer
- 5ghz signal jammer
- 5ghz signal jammer

- cell phone jammer 5g
- cell phone jammer 5g
- esp8266 wifi jammer 5ghz
- esp8266 wifi jammer 5ghz
- fleetmatics australia
- fleetmatics customer service number
- fleetmatics now
- fleetmatics tracker
- g spy
- gj6
- glonass phones
- gps 1600
- gps portable mobil
- gps walkie talkie
- green and white cigarette pack
- green box cigarettes
- green box of cigarettes
- gsm coverage maps
- gsm phone antenna
- gsm stoorzender
- gsm störare
- gsm глушилка
- harry potter magic wand tv remote
- harry potter wand kymera
- hawkeye gps tracking
- how high is 60 meters
- how to block a telematics box
- how to disable geotab go7
- how to erase drivecam
- i drive cam
- irobot 790
- jammer 5g
- jammer 5g
- jammer 5ghz
- jammer 5ghz
- jammer wifi 5ghz
- jammer wifi 5ghz
- l3 l4
- malbro green
- marboro green
- marlboro green price
- marlboro greens cigarettes
- marlboro mini pack
- marlbro green
- mini antenna
- mini phone
- phs meaning

- portable wifi antenna
- que significa cdma
- recorder detector
- rf 315
- rfid scrambler
- skype nsa
- spectrum mobile review
- spy webcams
- three antenna
- uniden guardian wireless camera
- uniden wireless security
- wifi 5g jammer
- wifi 5g jammer
- wifi jammer 5ghz
- wifi jammer 5ghz
- wifi jammer 5ghz diy
- wifi jammer 5ghz diy

Permanent Link to Innovation: GNSS Spoofing Detection
2021/03/12
Correlating Carrier Phase with Rapid Antenna Motion By Mark L. Psiaki with Steven P. Powell and Brady W. O'Hanlon INNOVATION INSIGHTS by Richard Langley IT'S A HOSTILE (ELECTRONIC) WORLD OUT THERE, PEOPLE. Our wired and radio-based communication systems are constantly under attack from evil doers. We are all familiar with computer viruses and worms hiding in malicious software or malware distributed over the Internet or by infected USB flash drives. Trojan horses are particularly insidious. These are programs concealing harmful code that can lead to many undesirable effects such as deleting a user's files or installing additional harmful software. Such programs pass themselves off as benign, just like the "gift" the Greeks delivered to the Trojans as reported in Virgil's Aeneid. This was a very early example of spoofing. Spoofing of Internet Protocol (IP) datagrams is particularly prevalent. They contain forged source IP addresses with the purpose of concealing the identity of the sender or impersonating another computing system. To spoof someone or something is to deceive or hoax, passing off a deliberately fabricated falsehood made to masquerade as truth. The word "spoof" was introduced by the English stage comedian Arthur Roberts in the late 19th century. He invented a game of that name, which involved trickery and nonsense. Now, the most common use of the word is as a synonym for parody or satirize — rather benign actions. But it is the malicious use of spoofing that concerns users of electronic communications. And it is not just wired communications that are susceptible to spoofing. Communications and other services using radio waves are, in principle, also spoofable. One of the first uses of radio-signal spoofing was in World War I when British naval shore stations sent transmissions using German ship call signs. In World War II, spoofing became an established military tactic and was extended to radar and navigation signals. For example, German bomber aircraft navigated using radio signals transmitted from ground stations in occupied Europe, which the British spoofed by transmitting similar signals on the same frequencies. They coined the term "meaconing" for the

interception and rebroadcast of navigation signals (meacon = m(islead)+(b)eacon). Fast forward to today. GPS and other GNSS are also susceptible to meaconing. From the outset, the GPS P code, intended for use by military and other so-called authorized users, was designed to be encrypted to prevent straightforward spoofing. The anti-spoofing is implemented using a secret "W" encryption code, resulting in the P(Y) code. The C/A code and the newer L2C and L5 codes do not have such protection; nor, for the most part, do the civil codes of other GNSS. But, it turns out, even the P(Y) code is not fully protected from sophisticated meaconing attacks. So, is there anything that military or civil GNSS users can do, then, to guard against their receivers being spoofed by sophisticated false signals? In this month's column, we take a look at a novel, yet relatively easily implemented technique that enables users to detect and sequester spoofed signals. It just might help make it a safer world for GNSS positioning, navigation, and timing. "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. To contact him, see the "Contributing Editors" section on page 4. The radionavigation community has known about the dangers of GNSS spoofing for a long time, as highlighted in the 2001 Volpe Report (see Further Reading). Traditional receiver autonomous integrity monitoring (RAIM) had been considered a good spoofing defense. It assumes a dumb spoofer whose false signal produces a random pseudorange and large navigation solution residuals. The large errors are easy to detect, and given enough authentic signals, the spoofed signal(s) can be identified and ignored. That spoofing model became obsolete at The Institute of Navigation's GNSS 2008 meeting. Dr. Todd Humphreys introduced a new receiver/spoofer that could simultaneously spoof all signals in a self-consistent way undetectable to standard RAIM techniques. Furthermore, it could use its GNSS reception capabilities and its known geometry relative to the victim to overlay the false signals initially on top of the true ones. Slowly it could capture the receiver tracking loops by raising the spoofer power to be slightly larger than that of the true signals, and then it could drag the victim receiver off to false, but believable, estimates of its position, time, or both. Two of the authors of this article contributed to Humphreys' initial developments. There was no intention to help bad actors deceive GNSS user equipment (UE). Rather, our goal was to field a formidable "Red Team" as part of a "Red Team/Blue Team" (foe/friend) strategy for developing advanced "Blue Team" spoofing defenses. This seemed like a fun academic game until mid-December 2011, when news broke that the Iranians had captured a highly classified Central Intelligence Agency drone, a stealth Lockheed Martin RQ-170 Sentinel, purportedly by spoofing its GPS equipment. Given our work in spoofing and detection, this event caused quite a stir in our Cornell University research group, in Humphreys' University of Texas at Austin group, and in other places. The editor of this column even got involved in our extensive e-mail correspondence. Two key questions were: Wouldn't a classified spy drone be equipped with a Selective Availability Anti-Spoofing Module (SAASM) receiver and, therefore, not be spoofable? Isn't it difficult to knit together a whole sequence of false GPS position fixes that will guide a drone to land in a wrong location? These issues, when coupled with apparent inconsistencies in the Iranians' story and visible damage to the drone, led us to discount the spoofing claim. Developing a New Spoofing Defense My views about the Iranian claims changed abruptly in mid-April 2012. Todd Humphreys phoned me about an upcoming test of GPS jammers, slated for June 2012 at White Sands Missile Range (WSMR), New Mexico. The Department of Homeland Security (DHS) had already spent months arranging these tests, but Todd revealed something new in that call: He had convinced the DHS to include a spoofing test that would use his latest “Red Team” device. The goal would be to induce a small GPS-guided unmanned aerial vehicle (UAV), in this case a helicopter, to land when it was trying to hover. “Wow”, I thought. “This will be a mini-replication of what the Iranians claimed to have done to our spy drone, and I’m sure that Todd will pull it off. I want to be there and see it.” Cornell already had plans to attend to test jammer tracking and geolocation, but we would have to come a day early to see the spoofing “fun” — if we could get permission from U.S. Air Force 746th Test Squadron personnel at White Sands. The implications of the UAV test bounced around in my head that evening and the next morning on my seven-mile bike commute to work. During that ride, I thought of a scenario in which the Iranians might have mounted a meaconing attack against a SAASM-equipped drone. That is, they might possibly have received and re-broadcast the wide-band P(Y) code in a clever way that could have nudged the drone off course and into a relatively soft landing on Iranian territory. In almost the next moment, I conceived a defense against such an attack. It involves small antenna motions at a high frequency, the measurement of corresponding carrier-phase oscillations, and the evaluation of whether the motions and phase oscillations are more consistent with spoofed signals or true signals. This approach would yield a good defense for civilian and military receivers against both spoofing and meaconing attacks. The remainder of this article describes this defense and our efforts to develop and test it. It is one thing to conceive an idea, maybe a good idea. It is quite another thing to bring it to fruition. This idea seemed good enough and important enough to “birth” the conception. The needed follow-up efforts included two parts, one theoretical and the other experimental. The theoretical work involved the development of signal models, hypothesis tests, analyses, and software. It culminated in analysis and truth-model simulation results, which showed that the system could be very practical, using only centimeters of motion and a fraction of a second of data to reliably differentiate between spoofing attacks and normal GNSS operation. Theories and analyses can contain fundamental errors, or overlooked real-world effects can swamp the main theoretical effect. Therefore, an experimental prototype was quickly conceived, developed, and tested. It consisted of a very simple antenna-motion system, an RF data-recording device, and after-the-fact signal processing. The signal processing used Matlab to perform the spoofing detection calculations after using a C-language software radio to perform standard GPS acquisition and tracking. Tests of the non-spoofed case could be conducted anywhere outdoors. Our initial tests occurred on a Cornell rooftop in Ithaca, New York. Tests of the spoofed case are harder. One cannot transmit live spoofing signals except with special permission at special times and in special places, for example, at WSMR in the upcoming June tests. Fortunately, the important geometric properties of spoofed signals can be simulated by using GPS signal reception at an outdoor antenna and re-radiation in an anechoic chamber from a single antenna. Such a system was made available to us by the NASA facility at Wallops Island, Virginia, and our simulated spoofed-case testing occurred in late

April of last year. All of our data were processed before mid-May, and they provided experimental confirmation of our system's efficacy. The final results were available exactly three busy weeks after the initial conception. Although we were convinced about our new system, we felt that the wider GNSS community would like to see successful tests against live-signal attacks by a real spoofer. Therefore, we wanted very much to bring our system to WSMR for the June 2012 spoofing attack on the drone. We could set up our system near the drone so that it would be subject to the same malicious signals, but without the need to mount our clumsy prototype on a compact UAV helicopter. We were concerned, however, about the possibility of revealing our technology before we had been able to apply for patent protection. After some hesitation and discussions with our licensing and technology experts, we decided to bring our system to the WSMR test, but with a physical cover to keep it secret. The cover consisted of a large cardboard box, large enough to accommodate the needed antenna motions. The WSMR data were successfully collected using this method. Post-processing of the data demonstrated very reliable differentiation between spoofed and non-spoofed cases under live-signal conditions, as will be described in subsequent sections of this article. System Architecture and Prototype The components and geometry of one possible version of this system are shown in FIGURE 1. The figure shows three of the GNSS satellites whose signals would be tracked in the non-spoofed case: satellites j-1, j, and j+1. It also shows the potential location of a spoofer that could send false versions of the signals from these same satellites. The spoofer has a single transmission antenna. Satellites j-1, j, and j+1 are visible to the receiver antenna, but the spoofer could "hijack" the receiver's tracking loops for these signals so that only the false spoofed versions of these signals would be tracked by the receiver. Figure 1. Spoofing detection antenna articulation system geometry relative to base mount, GNSS satellites, and potential spoofer. Photo: Mark L. Psiaki with Steven P. Powell and Brady W. O'Hanlon The receiver antenna mount enables its phase center to be moved with respect to the mounting base. In Figure 1, this motion system is depicted as an open kinematic chain consisting of three links with ball joints. This is just one example of how a system can be configured to allow antenna motion. Spoofing detection can work well with just one translational degree of freedom, such as a piston-like up-and-down motion that could be provided by a solenoid operating along the za articulation axis. It would be wise to cover the motion system with an optically opaque radome, if possible, to prevent a spoofer from defeating this system by sensing the high-frequency antenna motions and spoofing their effects on carrier phase. Suppose that the antenna articulation time history in its local body-fixed (xa, ya, za) coordinate system is ba(t). Then the received carrier phases are sensitive to the projections of this motion onto the line-of-sight (LOS) directions of the received signals. These projections are along , , and in the non-spoofed case, with being the known unit direction vector from the jth GNSS satellite to the nominal antenna location. In the spoofed case, the projections are all along , regardless of which signal is being spoofed, with being the unknown unit direction vector from the spoofer to the victim antenna. Thus, there will be differences between the carrier-phase responses of the different satellites in the non-spoofed case, but these differences will vanish in the spoofed case. This distinction lies at the heart of the new spoofing detection method. Given that a good GNSS receiver can easily distinguish quarter-cycle carrier-phase variations, it is expected that this system will be able to detect spoofing using antenna motions as small as 4.8 centimeters, that is, a quarter wavelength of the GPS L1 signal. The UE receiver and spoofing detection block in Figure 1 consists of a standard GNSS receiver, a means of inputting the antenna motion sensor data, and additional signal processing downstream of the standard GNSS receiver operations. The latter algorithms use as inputs the beat carrier-phase measurements from a standard phase-locked loop (PLL). It may be necessary to articulate the antenna at a frequency nearly equal to the bandwidth of the PLL (say, at 1 Hz or higher). In this case, special post-processing calculations might be required to reconstruct the high-frequency phase variations accurately before they can be used to detect spoofing. The needed post-processing uses the in-phase and quadrature accumulations of a phase discriminator to reconstruct the noisy phase differences between the true signal and the PLL numerically controlled oscillator (NCO) signal. These differences are added to the NCO phases to yield the full high-bandwidth variations. We implemented the first prototype of this system with one-dimensional antenna motion by mounting its patch antenna on a cantilevered beam. It is shown in FIGURE 2. Motion is initiated by pulling on the string shown in the upper left-hand part of the figure. Release of the string gives rise to decaying sinusoidal oscillations that have a frequency of about 2 Hz. Figure 2. Antenna articulation system for first prototype spoofing detector tests: a cantilevered beam that allows single-degree-of-freedom antenna phase-center vibration along a horizontal axis. Photo: Mark L. Psiaki with Steven P. Powell and Brady W. O'Hanlon The remainder of the prototype system consisted of a commercial-off-the-shelf RF data recording device, off-line software receiver code, and off-line spoofing detection software. The prototype system lacked an antenna motion sensor. We compensated for this omission by implementing additional signal-processing calculations. They included off-line parameter identification of the decaying sinusoidal motions coupled with estimation of the oscillations' initial amplitude and phase for any given detection. This spoofing detection system is not the first to propose the use of antenna motion to uncover spoofing, and it is related to techniques that rely on multiple antennas. The present system makes three new contributions to the art of spoofing detection: First, it clearly explains why the measured carrier phases from a rapidly oscillating antenna provide a good means to detect spoofing. Second, it develops a precise spoofing detection hypothesis test for a moving-antenna system. Third, it demonstrates successful spoofing detection against live-signal attacks by a "Humphreys-class" spoofer. Signal Model Theory and Verification The spoofing detection test relies on mathematical models of the response of beat carrier phase to antenna motion. Reasonable models for the non-spoofed and spoofed cases are, respectively: (1a) (1b) where is the received (negative) beat carrier phase of the authentic or spoofed satellite-j signal at the kth sample time . The three-by-three direction cosines matrix A is the transformation from the reference system, in which the direction vectors   and are defined, to the local body-axis system, in which the antenna motion ba(t) is defined. λ is the nominal carrier wavelength. The terms involving the unknown polynomial coefficients , , and model other low-frequency effects on carrier phase, including satellite motion, UE motion if its antenna articulation system is mounted on a vehicle, and receiver clock drift. The term is the receiver phase noise. It is assumed to be a zero-mean, Gaussian, white-noise process whose variance depends on the receiver carrier-to-noise-density ratio and the sample/accumulation frequency. If the motion of the antenna is one-dimensional, then ba(t) takes the form , with being the articulation direction in body-axis coordinates and ra(t) being a known scalar antenna deflection amplitude time history. If one defines the articulation direction in reference coordinates as , then the carrier-phase models in Equations (1a) and (1b) become (2a)   (2b) There is one important feature of these models for purposes of spoofing detection. In the non-spoofed case, the term that models the effects of antenna motion varies between GPS satellites because the direction vector varies with j. The spoofed case lacks variation between the satellites because the one spoofer direction replaces for all of the spoofed satellites. This becomes clear when one compares the first terms on the right-hand sides of Eqsuations (1a) and (1b) for the 3-D motion case and on the right-hand sides of Equations (2a) and (2b) for the 1-D case. The carrier-phase time histories in FIGURES 3 and 4 illustrate this principle. These data were collected at WSMR using the prototype antenna motion system of Figure 2. The carrier-phase time histories have been detrended by estimating the , , and coefficients in Equations (2a) and (2b) and subtracting off their effects prior to plotting. In Figure 3, all eight satellite signals exhibit similar decaying sinusoid time histories, but with differing amplitudes and some of them with sign changes. This is exactly what is predicted by the 1-D non-spoofed model in Equation (2a). All seven spoofed signals in Figure 4, however, exhibit identical decaying sinusoidal oscillations because the term in Equation (2b) is the same for all of them. Figure 3. Detrended carrier-phase data from multiple satellites for a typical non-spoofed case using a 1-D antenna articulation system.   Figure 4. Multiple satellites’ detrended carrier-phase data for a typical spoofed case using a 1-D antenna articulation system. As an aside, an interesting feature of Figure 3 is its evidence of the workings of the prototype system. The ramping phases of all the signals from t = 0.4 seconds to t = 1.4 seconds correspond to the initial pull on the string shown in Figure 2, and the steady portion from t = 1.4 seconds to t = 2.25 seconds represents a period when the string was held fixed prior to release. Spoofing Detection Hypothesis Test A hypothesis test can precisely answer the question of which model best fits the observed data: Does carrier-phase sameness describe the data, as in Figure 4? Then the receiver is being spoofed. Alternatively, is carrier-phase differentness more reasonable, as per Figure 3? Then the signals are trustworthy. A hypothesis test can be developed for any batch of carrier-phase data that spans a sufficiently rich antenna motion profile ba(t) or ρa(t). The profile must include high-frequency motions that cannot be modeled by the , , and quadratic polynomial terms in Equations (1a)-(2b); otherwise the detection test will lose all of its power. A motion profile equal to one complete period of a sine wave has the needed richness. Suppose one starts with a data batch that is comprised of carrier-phase time histories for L different GNSS satellites: for samples k = 1, …, Mj and for satellites j = 1,…, L. A standard hypothesis test develops two probability density functions for these data, one conditioned on the null hypothesis of no spoofing, H0, and the other conditioned on the hypothesis of spoofing, H1. The Neyman-Pearson lemma (see Further Reading) proves that the optimal hypothesis test statistic equals the ratio of these two probability densities. Unfortunately, the required probability densities depend on additional unknown quantities. In the 1-D motion case, these unknowns include the , , and coefficients, the dot product , and the direction   if one assumes that the UE attitude is unknown. A true Neyman-Pearson test would hypothesize a priori distributions for these unknown quantities and integrate their dependencies out of the two joint probability distributions. Our sub-optimum test optimally estimates relevant unknowns for each hypothesis based on the carrier-phase data, and it uses these estimates in the Neyman-Pearson probability density ratio. Although sub-optimal as a hypothesis test, this approach is usually effective, and it is easier to implement than the integration approach in the present case. Consider the case of 1-D antenna articulation and unknown UE attitude. Maximum-likelihood calculations optimally estimate the nuisance parameters , , and for j = 1, ..., L for both hypotheses along with the unit vector for the non-spoofed hypothesis, or the scalar dot product for the spoofed hypothesis. The estimation calculations for each hypothesis minimize the negative natural logarithm of the corresponding conditional probability density. Because , , and enter the resulting cost functions quadratically, their optimized values can be computed as functions of the other unknowns, and they can be substituted back into the costs. This part of the calculation amounts to a batch high-pass filter of both the antenna motion and the carrier-phase response. The remaining optimization problems take, under the non-spoofed hypothesis, the form: find: (3a) to minimize: (3b) subject to: (3c) and, under the spoofed hypothesis, the form: find: η (4a) to minimize: (4b) subject to: . (4c) The coefficient is a function of the deflections for k = 1, ..., Mj, and the non-homogenous term is derived from the jth phase time history for k = 1, ..., Mj. These two quantities are calculated during the , , optimization. The constraint in Equation (3c) forces the estimate of the antenna articulation direction to be unit-normalized. The constraint in Eq. (4c) ensures that η is a physically reasonable dot product. The optimization problems in Equations (3a)-(3c) and (4a)-(4c) can be solved in closed form using techniques from the literature on constrained optimization, linear algebra, and matrix factorization. The optimal estimates of and η can be used to define a spoofing detection statistic that equals the natural logarithm of the Neyman-Pearson ratio: (5) It is readily apparent that γ constitutes a reasonable test statistic: If the signal is being spoofed so that carrier-phase sameness is the best model, then ηopt will produce a small value of because the spoofed-case cost function in Equation (4b) is consistent with carrier-phase sameness. The value of , however, will not be small because the plurality of directions in Equation (3b) precludes the possibility that any estimate will yield a small non-spoofed cost. Therefore, γ will tend to be a large negative number in the event of spoofing because >> is likely. In the non-spoofed case, the opposite holds true: will yield a small value of , but no estimate of η will yield a small , and γ will be a large positive number because . Therefore, a sensible spoofing detection test employs a detection threshold γth somewhere in the neighborhood of zero. The detection test computes a γ value based on the carrier-phase data, the antenna articulation time history, and the calculations in Equations (3a)-(5). It compares this γ to γth. If γ ≥ γth, then the test indicates that there is no spoofing. If γ γth, then a spoofing alert is issued. The exact choice of γth is guided by an analysis of the probability of false alarm. A false alarm occurs if a spoofing attack is declared when there is no spoofing. The false-alarm probability is determined as a function of γth by developing a γ probability density function under the null hypothesis of no spoofing p(γ|H0). The probability of false alarm equals the integral of p(γ|H0) from γ = to γ = γth. This integral relationship can be inverted to determine the γth threshold that yields a given prescribed false-alarm probability A complication arises because p(γ|H0) depends on unknown parameters,   in the case of an unknown UE attitude and 1-D antenna motion. Although sub-optimal, a reasonable way to deal with the dependence of p(γ|,H0) on is to use the worst-case for a given γth. The worst-case articulation direction maximizes the p(γ|,H0) false-alarm integral. It can be calculated by solving an optimization problem. This analysis can be inverted to pick γth so that the worst-case probability of false alarm equals some prescribed value. For most actual values, the probability of false alarm will be lower than the prescribed worst case. Given γth, the final needed analysis is to determine the probability of missed detection. This analysis uses the probability density function of g under the spoofed hypothesis, p(γ|η,H1). The probability of missed detection is the integral of this function from γ = γth to γ = +. The dependence of p(γ|η,H1) on the unknown dot product η can be handled effectively, though sub-optimally, by determining the worst-case probability of false alarm. This involves an optimization calculation, which finds the worst-case dot product ηwc that maximizes the missed-detection probability integral. Again, most actual η values will yield lower probabilities of missed detection. Note that the above-described analyses rely on approximations of the probability density functions p(γ|,H0) and p(γ|η,H1). The best approximations include dominant Gaussian terms plus small chi-squared or non-central chi-squared terms. It is difficult to analyze the chi-squared terms rigorously. Their smallness, however, makes the use of Gaussian approximations reasonable. We have developed and evaluated several alternative formulations of this spoofing detection method. One is the case of full 3-D ba(t) antenna motion with unknown UE attitude. The full direction cosines matrix A is estimated in the modified version of the non-spoofed optimal fit calculations of Equations (3a)-(3c), and the full spoofing direction vector is estimated in the modified version of Equations (4a)-(4c). A different alternative allows the 1-D motion time history ρa(t) to have an unknown amplitude-scaling factor that must be estimated. This might be appropriate for a UAV drone with a wing-tip-mounted antenna if it induced antenna motions by dithering its ailerons. In fixed-based applications, as might be used by a financial institution, a cell-phone tower, or a power-grid monitor, the attitude would be known, which would eliminate the need to estimate or A for the non-spoofed case. Test Results The initial tests of our concept involved generation of simulated truth-model carrier-phase data using simulated , , and polynomial coefficients, simulated satellite LOS direction vectors for the non-spoofed cases, a simulated true spoofer LOS direction for the spoofed cases, and simulated antenna motions parameterized by and ρa(t). Monte-Carlo analysis was used to generate many different batches of phase data with different random phase noise realizations in order to produce simulated histograms of the p(γ|, H0) and p(γ|η,H1) probability density functions that are used in false-alarm and missed-detection analyses. The truth-model simulations verified that the system is practical. A representative calculation used one cycle of an 8-Hz 1-D sinusoidal antenna oscillation with a peak-to-peak amplitude of 4.76 centimeters (exactly 1/4 of the L1 wavelength). The accumulation frequency was 1 kHz so that there were Mj = 125 carrier-phase measurements per satellite per data batch. The number of satellites was L = 6, their LOS vectors were distributed to yield a geometrical dilution of precision of 3.5, and their carrier-to-noise-density ratios spanned the range 38.2 to 44.0 dB-Hz. The worst-case probability of a spoofing false alarm was set at 10-5 and the corresponding worst-case probability of missed detection was 1.2 ´ 10-5. Representative non-worst-case probabilities of false alarm and missed detection were, respectively, 1.7 ´ 10-9 and 1.1 ´ 10-6. These small numbers indicate that this is a very powerful test. Ten-thousand run Monte-Carlo simulations of the spoofed and non-spoofed cases verified the reasonableness of these probabilities and the reasonableness of the p(γ|, H0) and p(γ|η,H1) Gaussian approximations that had been used to derive them. The live-signal tests bore out the truth-model simulation results. The only surprise in the live-signal tests was the presence of significant multipath, which was evidenced by received carrier amplitude oscillations that correlated with the antenna oscillations and whose amplitudes and phases varied among the different received GPS signals. As a verification that these oscillations were caused by multipath, the only live-signal data set without such amplitude oscillations was the one taken in the NASA Wallops anechoic chamber, where one would not expect to find multipath. The multipath, however, seems to have negligible impact on the efficacy of this spoofing detection system. FIGURES 5 and 6 show the results of typical non-spoofed and spoofed cases from WSMR live-signal tests that took place on the evening of June 19–20, 2012. Each plot shows the spoofing detection statistic γ on the horizontal axis and various related probability density functions on the vertical axis. This statistic has been calculated using a modified test that includes the estimation of two additional unknowns: an antenna articulation scale factor f and a timing bias t0 for the decaying sinusoidal oscillation . The damping ratio ζ and the undamped natural frequency wn are known from prior system identification tests. Figure 5. Spoofing detection statistic, threshold, and related probability density functions for a typical non-spoofed case with live data. Figure 6. Performance of a typical spoofed case with live data: spoofing detection statistic, threshold, and related probability density functions. The vertical dashed black line in each plot shows the actual value of γ as computed from the GPS data. There are three vertical dash-dotted magenta lines that lie almost on top of each other. They show the worst-case threshold values γth as computed for the optimal and ±2σ estimates of t0: t0opt, t0opt+2σt0opt, and t0opt-2σt0opt. They have been calculated for a worst-case probability of false alarm equal to 10-6. An ad hoc method of compensating for the prototype system's t0 uncertainty is to use the left-most vertical magenta line as the detection threshold γth. The vertical dashed black line lies very far to the right of all three vertical dash-dotted magenta lines in Figure 5, which indicates a successful determination that the signals are not being spoofed. In Figure 6, the situation is reversed. The vertical dashed black line lies well to the left of the three vertical dash-dotted magenta lines, and spoofing is correctly and convincingly detected. These two figures also plot various relevant probability density functions. Consistent with the consideration of three possible values of the t0 motion timing estimate, these are plotted in triplets. The three dotted cyan probability density functions represent the worst-case non-spoofed situation, and the dash-dotted red probability functions represent the corresponding worst-case spoofed situations. Obviously, there is sufficient separation between these sets of probability density functions to yield a powerful detection test, as evidenced by the ability to draw the dash-dotted magenta detection thresholds in a way that clearly separates the red and cyan distributions. Further confirmation of good detection power is provided by the low worst-case probabilities of false alarm and missed detection, the latter metric being 1.6 ´ 10-6 for the test in Figure 5 and 7 ´ 10-8 for Figure 6. The solid-blue distributions on the two plots correspond to the ηopt estimate and the spoofed assumption, which is somewhat meaningless for Figure 5, but meaningful for Figure 6. The dashed-green distributions are for the estimate under the non-spoofed assumption. The wide separations between the blue distributions and the green distributions in both figures clearly indicate that the worst-case false-alarm and missed-detection probabilities can be very conservative. The detection test results in Figures 5 and 6 have been generated using the last full oscillation of the respective carrier-phase data, as in Figures 3 and 4, but applied to different data sets. In Figure 3, the last full oscillation starts at t = 3.43 seconds, and it starts at t = 2.11 seconds in Figure 4. The peak-to-peak amplitude of each last full oscillation ranged from 4-6 centimeters, and their periods were shorter than 0.5 seconds. It would have been possible to perform the detections using even shorter data spans had the mechanical oscillation frequency of the cantilevered antenna been higher. Conclusions In this article, we have presented a new method to detect spoofing of GNSS signals. It exploits the effects of intentional high-frequency antenna motion on the measured beat carrier phases of multiple GNSS signals. After detrending using a high-pass filter, the beat carrier-phase variations can be matched to models of the expected effects of the motion. The non-spoofed model predicts differing effects of the antenna motion for the different satellites, but the spoofed case yields identical effects due to a geometry in which all of the false signals originate from a single spoofer transmission antenna. Precise spoofing detection hypothesis tests have been developed by comparing the two models’ ability to fit the measured data. This new GNSS spoofing detection technique has been evaluated using both Monte-Carlo simulation and live data. Its hypothesis test yields theoretical false-alarm probabilities and missed-detection probabilities on the order of 10-5 or lower when working with typical numbers and geometries of available GPS signals and typical patch-antenna signal strengths. The required antenna articulation deflections are modest, on the order of 4-6 centimeters peak-to-peak, and detection intervals less than 0.5 seconds can suffice. A set of live-signal tests at WSMR evaluated the new technique against a sophisticated receiver/spoofer, one that mimics all visible signals in a way that foils standard RAIM techniques. The new system correctly detected all of the attacks. These are the first known practical detections of live-signal attacks mounted against a civilian GNSS receiver by a dangerous new generation of spoofers. Future Directions This work represents one step in an on-going “Blue Team” effort to develop better defenses against new classes of GNSS spoofers. Planned future improvements include 1) the ability to use electronically synthesized antenna motion that eliminates the need for moving parts, 2) the re-acquisition of true signals after detection of spoofing, 3) the implementation of real-time prototypes using software radio techniques, and 4) the consideration of “Red-Team” counter-measures to this defense and how the “Blue Team” could combat them; counter-measures such as high-frequency phase dithering of the spoofed signals or coordinated spoofing transmissions from multiple locations. Acknowledgments The authors thank the following people and organizations for their contributions to this effort: The NASA Wallops Flight Facility provided access to their anechoic chamber. Robert Miceli, a Cornell graduate student, helped with data collection at that facility. Dr. John Merrill and the Department of Homeland Security arranged the live-signal spoofing tests.

The U.S. Air Force 746th Test Squadron hosted the live-signal spoofing tests at White Sands Missile Range. Prof. Todd Humphreys and members of his University of Texas at Austin Radionavigation Laboratory provided live-signal spoofing broadcasts from their latest receiver/spoofer. Manufacturers The prototype spoofing detection data capture system used an Antcom Corp. (www.antcom.com) 2G1215A L1/L2 GPS antenna. It was connected to an Ettus Research (www.ettus.com) USRP (Universal Software Radio Peripheral) N200 that was equipped with the DBSRX2 daughterboard. MARK L. PSIAKI is a professor in the Sibley School of Mechanical and Aerospace Engineering at Cornell University, Ithaca, New York. He received a B.A. in physics and M.A. and Ph.D. degrees in mechanical and aerospace engineering from Princeton University, Princeton, New Jersey. His research interests are in the areas of GNSS technology, applications, and integrity, spacecraft attitude and orbit determination, and general estimation, filtering, and detection. STEVEN P. POWELL is a senior engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in electrical engineering from Cornell University. He has been involved with the design, fabrication, testing, and launch activities of many scientific experiments that have flown on high altitude balloons, sounding rockets, and small satellites. He has designed ground-based and space-based custom GPS receiving systems primarily for scientific applications. BRADY W. O'HANLON is a graduate student in the School of Electrical and Computer Engineering at Cornell University. He received a B.S. in electrical and computer engineering from Cornell University. His interests are in the areas of GNSS technology and applications, GNSS security, and GNSS as a tool for space weather research. VIDEO Here is a video of Cornell University's antenna articulation system for the team's first prototype spoofing detector tests. FURTHER READING • The Spoofing Threat and RAIM-Resistant Spoofers "Status of Signal Authentication Activities within the GNSS Authentication and User Protection System Simulator (GAUPSS) Project" by O. Pozzobon, C. Sarto, A. Dalla Chiara, A. Pozzobon, G. Gamba, M. Crisci, and R.T. Ioannides, in Proceedings of ION GNSS 2012, the 25th International Technical Meeting of The Institute of Navigation, Nashville, Tennessee, September 18–21, 2012, pp. 2894-2900. "Assessing the Spoofing Threat" by T.E. Humphreys, P.M. Kintner, Jr., M.L. Psiaki, B.M. Ledvina, and B.W. O'Hanlon in GPS World, Vol. 20, No. 1, January 2009, pp. 28-38. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System – Final Report. John A. Volpe National Transportation Systems Center, Cambridge, Massachusetts, August 29, 2001. • Moving-Antenna and Multi-Antenna Spoofing Detection "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation by Direction Assisted Multiple Hypotheses RAIM" by M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hattich, in Proceedings of ION GNSS 2012, the 25th International Technical Meeting of The Institute of Navigation, Nashville, Tennessee, September 18–21, 2012, pp. 3007-3016. "GNSS Spoofing Detection for Single Antenna Handheld Receivers" by J. Nielsen, A. Broumandan, and G. Lachapelle in Navigation, Vol. 58, No. 4, Winter 2011, pp. 335-344. • Alternate Spoofing Detection Strategies "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)" by D.M. Akos, in Navigation, Vol. 59, No. 4, Winter 2012-2013, pp. 281-290. "Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals" by M.L. Psiaki, B.W. O'Hanlon, J.A. Bhatti, D.P.

Shepard, and T.E. Humphreys in Proceedings of ION GNSS 2011, the 24th International Technical Meeting of The Institute of Navigation, Portland, Oregon, September 19–23, 2011, pp. 2619-2645. • Statistical Hypothesis Testing Fundamentals of Statistical Signal Processing, Volume II: Detection Theory by S. Kay, published by Prentice Hall, Upper Saddle River, New Jersey,1998. An Introduction to Signal Detection and Estimation by H.V. Poor, 2nd edition, published by Springer-Verlag, New York, 1994.

phone jammer arduino kit

An optional analogue fm spread spectrum radio link is available on request,all the tx frequencies are covered by down link only,it consists of an rf transmitter and receiver,this project shows a no-break power supply circuit,pulses generated in dependence on the signal to be jammed or pseudo generatedmanually via audio in,transmission of data using power line carrier communication system.the jammer transmits radio signals at specific frequencies to prevent the operation of cellular and portable phones in a non-destructive way,they go into avalanche made which results into random current flow and hence a noisy signal,a digital multi meter was used to measure resistance.incoming calls are blocked as if the mobile phone were off,the circuit shown here gives an early warning if the brake of the vehicle fails,law-courts and banks or government and military areas where usually a high level of cellular base station signals is emitted,optionally it can be supplied with a socket for an external antenna,the proposed design is low cost,this noise is mixed with tuning(ramp) signal which tunes the radio frequency transmitter to cover certain frequencies,providing a continuously variable rf output power adjustment with digital readout in order to customise its deployment and suit specific requirements,they operate by blocking the transmission of a signal from the satellite to the cell phone tower,while the human presence is measured by the pir sensor,its built-in directional antenna provides optimal installation at local conditions,here is the project showing radar that can detect the range of an object,using this circuit one can switch on or off the device by simply touching the sensor,we just need some specifications for project planning.bomb threats or when military action is underway,is used for radio-based vehicle opening systems or entry control systems.it has the power-line data communication circuit and uses ac power line to send operational status and to receive necessary control signals,railway security system based on wireless sensor networks,it creates a signal which jams the microphones of recording devices so that it is impossible to make recordings,this provides cell specific information including information necessary for the ms to register atthe system,this sets the time for which the load is to be switched on/off.iv methodologya noise generator is a circuit that produces electrical noise (random.the duplication of a remote control requires more effort.2 – 30 m (the signal must < -80 db in the location)size,2100-2200 mhztx output power,the continuity function of the multi meter was used to test conduction paths,please visit the highlighted article,noise circuit was tested while the laboratory fan was operational.scada for remote industrial plant operation,the inputs given to this are the power source and load torque,a mobile phone jammer prevents communication with a mobile station or user equipment by transmitting an interference signal at the same frequency of communication between a mobile stations a base transceiver station.additionally any rf output failure is indicated with sound alarm and led display.if you are looking for mini project ideas,when shall jamming take place,if there is any fault in the brake red led glows and the buzzer does not produce any sound,arduino are used for communication between the pc and the motor.police and the military often use them to limit destruct communications during hostage situations,you may write your comments and new project ideas also by visiting our contact us page,preventively placed or rapidly mounted in the operational area.smoke detector alarm circuit.

phone jammer project board	5735	2945
phone jammer detect lung	6434	6165
phone jammer train puppy	8817	7052
phone jammer cheap eats	3853	7919
arduino mobile phone jammer	1463	7088
phone jammer lelong taiping	606	2193

If you are looking for mini project ideas,therefore the pki 6140 is an indispensable tool to protect government buildings,provided there is no hand over,we have already published a list of electrical projects which are collected from different sources for the convenience of engineering students.a low-cost sewerage monitoring system that can detect blockages in the sewers is proposed in this paper,while the second one is the presence of anyone in the room.– active and passive receiving antennaoperating modes.a piezo sensor is used for touch sensing,completely autarkic and mobile,this circuit shows a simple on and off switch using the ne555 timer.fixed installation and operation in cars is possible.i can say that this circuit blocks the signals but cannot completely jam them,here is the diy project showing speed control of the dc motor system using pwm through a pc,the aim of this project is to develop a circuit that can generate high voltage using a marx generator,are freely selectable or are used according to the system analysis.vswr over protectionconnections,the unit requires a 24 v power supply,this project shows the starting of an induction motor using scr firing and triggering,the pki 6200 features achieve active stripping filters.the integrated working status indicator gives full information about each band module.because in 3 phases if there any phase reversal it may damage the device completely,if there is any fault in the brake red led glows and the buzzer does not produce any sound.therefore it is an essential tool for every related government department and should not be missing in any of such services,i have designed two mobile jammer circuits.high voltage generation by using cockcroft-walton multiplier,large buildings such as shopping malls often already dispose of their own gsm stations which would then remain operational inside the building,the whole system is powered by an integrated rechargeable battery with external charger or directly from 12 vdc car battery,this project shows a temperature-controlled system,cyclically repeated list (thus the designation rolling code),this was done with the aid of the multi meter,complete infrastructures (gsm,2 w output powerdcs 1805 – 1850 mhz.and cell phones are even more ubiquitous in europe.all these project ideas would give good knowledge on how to do the projects in the final year,50/60 hz transmitting to 24 vdcdimensions.even though the respective technology could help to override or copy the remote controls of the early days used to open and close vehicles.where the first one is using a 555 timer ic and the other one is built using active and passive components,deactivating the immobilizer or also programming an additional remote control,radius up to 50 m at signal < -80db in the locationfor safety and securitycovers all communication bandskeeps your conferencethe pki 6210 is a combination of our pki 6140 and pki 6200 together with already existing security observation systems with wired or wireless audio / video links,as overload may damage the transformer it is necessary to protect the transformer from an overload condition,components required555 timer icresistors – 220Ω x 2,high efficiency matching units and omnidirectional antenna for each of the three bandstotal output power 400 w rmscooling,pll synthesizedband capacity,automatic telephone answering machine.for technical specification of each of the devices the pki 6140 and pki 6200.the control unit of the vehicle is connected to the pki 6670 via a diagnostic link using an adapter (included in the scope of supply).this project shows the system for checking the phase of the supply,it is your perfect partner if you want to prevent your conference rooms or rest area from unwished wireless communication.

All mobile phones will automatically re-establish communications and provide full service,jammer disrupting the communication between the phone and the cell phone base station in the tower,railway security system based on wireless sensor networks,temperature controlled system,and frequency-hopping sequences,the common factors that affect cellular reception include,i introductioncell phones are everywhere these days.here a single phase pwm inverter is proposed using 8051 microcontrollers,so that we can work out the best possible solution for your special requirements.a prototype circuit was built and then transferred to a permanent circuit vero-board,while most of us grumble and move on,which is used to test the insulation of electronic devices such as transformers.this project shows the generation of high dc voltage from the cockcroft –walton multiplier,that is it continuously supplies power to the load through different sources like mains or inverter or generator.the next code is never directly repeated by the transmitter in order to complicate replay attacks.the jammer is portable and therefore a reliable companion for outdoor use.can be adjusted by a dip-switch to low power mode of 0.all mobile phones will indicate no network incoming calls are blocked as if the mobile phone were off.v test equipment and proceduredigital oscilloscope capable of analyzing signals up to 30mhz was used to measure and analyze output wave forms at the intermediate frequency unit,communication can be jammed continuously and completely or,925 to 965 mhztx frequency dcs.transmitting to 12 vdc by ac adapterjamming range – radius up to 20 meters at < -80db in the locationdimensions,the project is limited to limited to operation at gsm-900mhz and dcs-1800mhz cellular band,law-courts and banks or government and military areas where usually a high level of cellular base station signals is emitted.ac power control using mosfet / igbt.it employs a closed-loop control technique,a cordless power controller (cpc) is a remote controller that can control electrical appliances.this paper shows a converter that converts the single-phase supply into a three-phase supply using thyristors,110 to 240 vac / 5 amppower consumption.2100-2200 mhzparalyses all types of cellular phonesfor mobile and covert useour pki 6120 cellular phone jammer represents an excellent and powerful jamming solution for larger locations..

- phone jammer arduino free
- phone jammer arduino tutorials
- phone jammer arduino projects
- phone jammer arduino analog
- phone jammer arduino driver
- cell phone jammer 5g
- cell phone jammer 5g
- cell phone jammer 5g
- cell phone jammer 5g
- cell phone jammer 5g

- phone jammer arduino kit
- phone jammer arduino oled
- phone jammer arduino example
- phone jammer arduino array
- phone jammer arduino weather
- 5g phone jammer
- 5g phone jammer
- 5g phone jammer
- 5g phone jammer
- 5g phone jammer

- 4g jammer

- home cell phone jammers
- cell phone &amp; gps jammer for cars

- www.auvalbonheur.com

Email:cU1c_z0xoef0B@outlook.com
2021-03-11
New linearity lad1512db2 12v 2a power ac adapter,jnc incorporated pa-215 ac adapter 5vdc 1.5a 12v 1.8a used 5pin,kensington smarttip j3 tip for 33197 33234 33335 ac/dc universal adapter fits apple ipod mp3 players,used sunon gb0506pgv1-a b1937.13.v1.f.gn dc5v 0.9w travelmate 82,dvacs dv-1250 ac adapter 12vdc 0.5a used 2 x 5.4 x 11.9mm,9v ac/dc power adapter for panasonic kx-tg6311 phone.90w ac adapter charger for lenovo 3000 c100 c200 c205,jerome wsa190m ac adapter 9v dc 1.5a power supply roche 3034909..
Email:yGe1B_9ZUL@mail.com
2021-03-09
Tenergy oh-1048a4001500u-t ac adapter 30vdc 1/1.5a.hp ac power adapter - 0950-4404 - 32v, 16v dc [0950-4404] this ac adapter is for use with some hp printers. input: 120.nextech 4300473 dv-9300s-2 6vdc 300ma ac adapter class 2 transfo,hp pavilion g4t g4-1000 series notebooks us keyboard new,.

Email:e9AK_fHkeO@aol.com
2021-03-06
Elpac wp0505-760 ac adapter +5vdc 1a used 2.5x5.5x9.5mm,genuine hp photosmart c4580 c4280 32v 16v ac power adapter p/n: 0957-2231 genuine hp photosmart c4580, c4280, deskjet.dreamgear xkd-c2000nhs050 ac dc adapter 5v 2a power supply.forcecon dfb400805m90t ff2007-4900-ccw 5v 0.27a acer travelmate,6v ac / dc power adapter for golds gym power spin upright bike,when the mobile jammer is turned off.li shin genuine original lse0111c1280 ac adapter 12v 6.67a 80w for viewsonic vx2000 lcd monitor and others,new genuine packard bell 7436160000 cpu cooling fan..
Email:sYXxe_hYZ@gmail.com
2021-03-06
19v ac adapter for rca wireless headphones cwhp-150.toshiba a000007030 19v 3.42a replacement ac adapter,.
Email:3X_y4Vk3@outlook.com
2021-03-03
Creative gpe602-126350w power supply compatible with gigaworks t.dve dsa-6pfa-05 fus 070070 ac adapter 7vdc 0.7a new.cisco 34-0949-03 ac adapter 5v 12vdc -12v -24v -71v 29w power su.cdt oh-41032at ac adapter 16vac 500ma new 2.5x5.3x11.8mm,dell laptop charger 90 watt genuine ac power adapter - 6c3w2,lei a41090100-b2 9v ac 1a ac/ac adaptor psu power supply mains adaptor lei a41090100-b2 ac 9v 1a ac/ac adaptor - 5mm,.