How to make an rf jammer - how to work hidden camera

- 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 GNSS Lies, GNSS Truth
2021/03/14
Photo: Mark L. Psiaki, Brady W. O'Hanlon, Steven P. Powell, Jahshan A. Bhatti, Todd E. Humphreys, and Andrew Schofield Spoofing Detection with Two-Antenna Differential Carrier Phase By Mark L. Psiaki, Brady W. O'Hanlon, Steven P. Powell, Jahshan A. Bhatti, Todd E. Humphreys, and Andrew Schofield A new method detects spoofing attacks that are resistant to standard RAIM technique and can sense an attack in a fraction of a second without external aiding. The signal-in-space properties used to detect spoofing are the relationships of the signal arrival directions to the vector that points from one antenna to the other. A real-time implementation succeeded against live-signal spoofing attacks aboard a superyacht, the White Rose of Drachs shown above, cruising in international waters. Read more about "Red Team, White Team, Blue Team" below. Concerns about spoofing of open-service GNSS signals inspired early work on simple receiver-autonomous integrity monitoring (RAIM) methods based on the consistency of the navigation solution. Work on new classes of defense techniques began in earnest after the demonstration of a powerful spoofer that is undetectfable by simple pseudorange-based RAIM methods. There has been a sense of urgency to solve the spoofing problem since the Iranians captured a classified U.S. drone in 2011 and made unsubstantiated claims to have spoofed its GPS. Two dramatic field demonstrations of the spoofer developed by author Humphreys and colleagues at the University of Texas, Austin, heightened interest in spoofing detection: one involved deception of a small airborne unmanned autonomous vehicle (UAV), causing it to dive towards the ground; another sent a superyacht off course without raising any alarms on its bridge. One class of spoofing detection methods uses encrypted signals, their known relationships to the open-service signals, and after-the-fact availability of encryption information. Such techniques require a high-bandwidth communication link between the potential victim of a spoofing attack and a trusted source of after-the-fact encryption information, and may involve significant latency between attack and detection.

Another class of methods uses advanced RAIM-type techniques. Instead of considering only pseudorange consistency, these RAIM techniques examine additional signal characteristics such as absolute power levels, distortion of the PRN code correlation function along the early/late axis, the possible existence of multiple distinct correlation peaks in signal-acquisition-type calculations, and other signal or receiver characteristics. Such methods are relatively simple to implement because they do not require much additional hardware, if any, but some of these strategies can have trouble distinguishing between multipath and spoofing or between jamming and spoofing. A third class proposes the addition of Navigation Message Authentication bits. These are encrypted parts of the low-rate navigation data message. Such techniques require modification of the navigation data message and can allow long latencies between the onset of a spoofing attack and its detection. A fourth class exploits the differing signal-in-space geometry of spoofed signals in comparison to true GNSS signals. All spoofed signals typically arrive from the same direction, but true signals arrive from a multiplicity of directions. Some of these methods use receiver antenna motion to achieve direction-of-arrival sensitivity. Others use an array of two or more receiver antennas. The most powerful of these detection strategies exploit models of the effects on carrier-phase data of antenna motion or antenna-array geometry. This knowledge may be partial because an unknown antenna-array attitude may need to be determined as part of the detection calculation. Their power derives from the high degree of accuracy with which a typical GNSS receiver can measure beat carrier phase. Goals. This research follows on moving-antenna/carrier-phase-based spoofing detection work. One of our goals has been to remove the necessity for moving parts by using two antennas and processing their carrier-phase data. A second goal has been to achieve real-time operation. An earlier prototype moving-antenna system (see “GNSS Spoofing Detection,” GPS World, June 2013) used post-processing and completed its spoofing detection calculations days or weeks after the recording of wide-band RF data during live-signal attacks. A third goal has been to test this system against actual live-signal spoofing attacks to prove its real-time capabilities and evaluate its performance during the two phases of an attack: the initial signal capture and the post-capture drag-off to erroneous position and timing fixes. Two-Antenna System Architecture The system consists of two GNSS patch antennas, GPS receiver hardware and software, and spoofing detection signal-processing hardware and software. Figure 1 shows two versions. The left-hand version connects its two patch antennas to an RF switch. The single analog RF output of the switch is input to a GNSS receiver that is standard in all respects, except for two features. First, it controls the RF switch or, at least, has access to the switching times. Second, it employs a specialized phase-locked loop (PLL) that can track the beat carrier phase of a given signal through the phase jumps that occur at the switching times. The right-hand version connects each antenna to an independent GPS receiver, likely connected to a common reference oscillator. Figure 1. Two configurations:, the RF-switched-signal/single-receiver configuration (left) and the two-receiver configuration (right). The last element of each system is a spoofing detection signal-processing unit. Its inputs are the single-differenced beat carrier phases of all tracked signals, with differences taken between the two antennas. In the switched antenna system, each difference is deduced by the specialized PLL. In the two-receiver system, the single-differences are calculated

explicitly from each receiver's beat carrier-phase observables. Except for the final spoofing detection unit, the two-receiver system on the right-hand side of Figure 1 is already available commercially. Typical applications are CDGPS-based attitude/heading determination. Thus, this is the easiest version to implement. This system could include more than two antennas. A multi-antenna system could have a dedicated RF front-end and a dedicated set of receiver channels for each antenna, as on the right of Figure 1. Alternatively, a multi-antenna system could include an RF switch between any one of the multiple antennas at the command of the receiver. The latter design would entail a slight modification to the specialized PLL to track multiple independent phase jumps for the independent antenna switches. Principles. The principles used to detect spoofing can be understood by considering and comparing the signal-in-space and antenna geometries shown in Figure 2, the two-antenna system and three GNSS satellites for a typical non-spoofed case, and Figure 3, a spoofed case. The salient difference is that the different GNSS signals arrive from different directions for the non-spoofed case, namely and . They all arrive from the same direction, the direction of the spoofer , for the spoofed case. For detection purposes, the important geometric feature is the projection of each direction of arrival onto the known separation vector between the two antennas, bBA. This projection has a direct effect on the beat carrier-phase difference between the two antennas. In the non-spoofed case, this effect will vary between the different received signals in ways consistent with the attitude of the vector. In the spoofed case, all of these carrier-phase differences will be identical. The spoofing detection algorithm decides between two hypotheses about the carrier-phase differences, one conjecturing a diversity consistent with authentic signals and the other conjecturing the sameness that is characteristic of spoofed signals. Figure 2. Geometry of two-antenna spoofing detection system and GNSS satellites for non-spoofed case. Figure 3. Spoofed-case geometry of two-antenna spoofing detection system and GNSS spoofer. Hypothesis Test The PDF paper on which this article is based presents the non-spoofed and spoofed signal models that form the basis of a hypothesis test, develops optimal estimation algorithms that fit the observed differential beat carrier phases to the two models, and shows how these estimates and their associated fit error costs can be used to develop a sensible spoofing detection hypothesis test. Download the PDF here. Offline and Live-Signal Testing We tested a prototype version of the two-antenna system as depicted on the righthand side of Figure 1. The antennas connect to two independent RF front-ends that run off of the same reference oscillator. These RF front-ends provide input to two independent receivers that track each signal using a delay-lock loop (DLL) and a PLL. Figures 4 and 5 show system elements: two GPS patch antennas mounted on a single ground plane with a spacing of 0.14 meters, two RF front-ends — universal software radio peripherals (USRPs) — with a common ovenized crystal oscillator. Digital signal-processing functions are implemented in real-time software radio receivers (SWRX) running in parallel on a Linux laptop, written in C++. Spoofing detection calculations are performed on the same laptop using algorithms encoded in Matlab. Figure 4. The two antennas of the prototype spoofing detection system mounted on a common ground plane. Figure 5. Signal processing hardware of the prototype spoofing detection system. A key feature of this architecture is the ability of its real-time software radios' C++ code to call the spoofing detector's Matlab tic function and to pass

carrier-phase and other relevant data to the tic function. This feature served to shorten the implementation and test cycle for the prototype system by eliminating the need to translate the original Matlab versions of the spoofing detection algorithms into C++. This enabled rapid re-tuning and redesign of the spoofing detection calculations, exploited during the course of live-signal testing. The Matlab package displays real-time signal authentication information. Figure 6 shows the version of the display used for this study's culminating live-signal tests. All displays are updated in real time. The upper left, upper right, and lower left plots scroll along their horizontal time axes to keep the most recent 4.5 minutes of data available. The lower right compass updates each time a new spoofing detection calculation is performed. The green dots in the upper left plot indicate that the time between spoofing detections, Δtspf , is nominally 1 second, though sometimes the gap is longer due to lack of a sufficient number of validated single-differenced carrier phases to carry out the calculation. Thus, the nominal update time for all of the plots in this display is 1 second. Faster updates are possible with the Matlab software, but Δtspf was deemed sufficiently fast for this study's experiments. The most important panel in Figure 6 is the upper left spoofing detection statistic time history. The magenta plus signs on the plot show the spoofing detection threshold chosen for this case, γth. The computed γ values are plotted as green o's if they lie above γth and as red asterisks if they lie below. If γ is above γth, the message "GPS Signals Authenticated" is displayed on the plot; if below, the message switches to the spoofing alert: "GPS SPOOFING ATTACK DETECTED!" Figure 6. Spoofing detector real-time display. Clockwise from top left: the spoofing detection statistic time history γ(t); four diagnostic time histories that include time histories of the number of satellites used for spoofing detection L(t) (blue asterisks), their corresponding GDOP(t) values (magenta o's), the time increment between spoofing detection tests Δtspf(t) (green dots), and the compass heading ψ(t) as determined from the two-antenna non-spoofed-case solution (black dots); Compass display; and time history of GPS PRN number availability. The other three panels proved helpful in diagnosing system performance. A low L value (near 4) or a high GDOP value in the upper right panel indicated poorer reliability of the spoofing detection calculations. A correct compass heading in the absence of spoofing provided a check on the system. During spoofing attacks, the compass heading became jumpy, thereby providing another possible indicator of inauthentic signals. The vertical scale of the lower left panel lists the possible GPS PRN numbers. The presence of a green or red dot at the level corresponding to a given PRN number indicates that one or both receivers is seeing something from that satellite at the corresponding time. If the dot is red, then the returned data are incomplete or are deemed to be insufficiently validated for use in the spoofing detection calculation. If the dot is green, then the data from that PRN have been used in the detection that has been carried out at that time. Another feature of the prototype spoofing detection system is its ability to record the wide-band RF data from its two antennas. For each spoofing scenario, the raw samples from both USRPs were recorded while the real-time software receiver was performing its signal-processing operations and while the real-time spoofing detector was doing its calculations. These recorded data streams will allow off-line analysis and testing of a re-tuned or completely redesigned spoofing detection system. Red Team Receiver/Spoofer. The UT Austin spoofer's attack strategy overlays the spoofed signal on top of the true signals, ramps up the

power to capture the receiver tracking loops, and finally drags the pseudorange, beat carrier phase, and carrier Doppler shift off from their true values to spoofed values. Figure 7 shows the pseudorange part of a spoofing attack: cross-correlation of the receiver's PRN code replica with the total received signal (blue solid curve); the receiver's early, prompt, and late correlations (red dots); and the spoofer signal (black dash-dotted curve). In the top plot, the spoofer has zero power, and the receiver sees only the true signal. The second and third plots show the spoofer ramping up its power while maintaining its false signal in alignment with the true signal. The spoofer power in the middle/third plot is sufficient to capture control of the three red dots of the receiver's DLL. In the fourth and fifth plots, the spoofer initiates and continues a pseudorange drag-off, an intentional falsification of the pseudorange as measured by the victim receiver's DLL. Figure 7. Receiver/spoofer attack sequence as viewed from a channel's code offset cross-correlation function. Spoofer signal: black dash-dotted curve; sum of spoofer and true signals: blue solid curve; receiver early, prompt, and late correlation points: red dots. The spoofer performs drag-off simultaneously on all spoofed channels in a vector spoofing attack that maintains consistency of all spoofed pseudoranges. After the initiation of drag-off, the victim receiver computes a wrong position, a wrong true time, or both, but the residual pseudorange errors in its navigation solution remain small. Therefore, this type of attack is not detectable by traditional pseudorange-based RAIM calculations. The receiver spoofer hardware consists of a GNSS reception antenna, the receiver spoofer signal-processing unit, and the spoofer transmission antenna (Figure 8). Figure 8a. Receiver/spoofer hardware: GPS reception antenna on ship's rear upper deck. Figure 8b. Receiver/spoofer hardware: directional transmission antenna pointed at the ship's GPS antenna and the detector antenna pair near the defended ship's antenna. The orientation of the spoofing transmission antenna, combined with its remote location from the receiver/spoofer's reception antenna, ensured that the spoofer did not self-spoof. Figure 8c. Receiver/spoofer hardware: spoofer electronics, located amidships. The receiver/spoofer requires tuning of its transmission power levels. If the power is too high, its spoofing attacks will be too obvious. A very high transmitted power could also saturate the front-end electronics of the intended victim, causing it to jam the system rather than spoof it. If transmitted power is too low, it will not capture the victim's tracking loops, and its spoofing attack will fail. The proper power level depends on the gain patterns of the spoofer transmission antenna and the victim receiver antenna and on their relative geometry. Attack Test Scenarios. Three sets of tests were conducted to develop and evaluate the spoofing detection system. The first tests started by recording wideband RF GPS L1 data using USRPs. These data were post-processed in two software receivers that recorded the outputs of their signal tracking loops. Afterwards, the Matlab spoofing detection calculations were run using the recorded tracking loop data as inputs. These preliminary tests at Cornell and Austin proved the efficacy of the spoofing detection algorithms. They did not, however, test system performance during the transition from non-spoofed to spoofed signals that takes place at the initiation of a spoofing attack. The second set of tests was carried out using the first real-time version of the system, after the Matlab spoofing detection calculations were repackaged into a tic function and linked to the C++ real-time software receivers. This set of tests also was unable to probe the system's performance at the onset of a

spoofing attack, before the signal drag-off. The final set of tests was conducted aboard the White Rose of Drachs in the Mediterranean's international waters. The power adjustment tests on June 27 needed a means to decide whether a given attack had captured the tracking loops of the ship's GPS receiver. The strategy for confirming capture was to perform a noticeable drag-off after the initial attack. We settled on a vertical drag-off as providing the most obvious indication of a successful capture. Successful attacks dragged the receiver's reported altitude as high as 5,000 meters. The tests that evaluated spoofer and spoofing detector antenna placements relative to the ship's GPS antenna were also important to achieving sensible results. Various placements were tried. The most successful relative geometry is depicted in Figure 8. The placement of the detector antennas relative to the defended antenna is atypical of likely real-world detection scenarios. It is expected that a real-world spoofing detector will be integral with the defended GNSS receiver. The culminating live-signal attack involved a 50-minute spoofing scenario in which the attacker took the ship — apparently — from the Adriatic to the coast off of Libya. The scenario's long distance and short duration required a mid-course speed in excess of 900 knots. This spoofing scenario was designed in the simplest possible way, by taking a straight-line course in WGS-84 Cartesian coordinates from the true location to the spoofed location off of Libya. This course took the spoofed yacht position across the Italian and Sicilian land masses and below the Earth's surface to a maximum depth of more than 23 kilometers. Obviously, the White Rose was physically unable to execute this maneuver. Its crew would not have needed spoofing detection to realize that its GPS receiver was returning false readings. The main points of this last test were to dramatize the potential errors that can be caused by a spoofer and to check whether the spoofing detector could continue to function under these drastic conditions. Figure 9 highlights this unusual scenario with two displays from the ship's bridge, photographed during the attack. The GPS display shows the speed, 621 kn (knots), and the altitude, 7376 m. The chart display shows the yacht on (or rather, below) dry land and halfway across the "insole" of Italy's boot. It also shows a tremendously long velocity vector, extending beyond the chart. Figure 9a. The ship's bridge GPS receiver display during the Libya spoofing scenario. Figure 9b. The GPS-driven chart during the Libya spoofing scenario. Spoofing Detection Test Results Various signal output time histories (Figure 10) illustrate the attack sequence and suggest means to evaluate the spoofing detection system. The upper panel plots the fractional portions of the two-antenna spoofing detector's single-differenced beat carrier-phase time histories, $\Delta\phi 1BA$, …, $\Delta\phi LBA$ for the L = 7 tracked PRN numbers 16, 18, 21, 22, 27, 29, and 31. The middle panel plots the amplitude time history of the 100 Hz prompt [I;Q] accumulation vector for PRN 16, as received at Antenna A of the detection system. The bottom panel plots the PRN 16 carrier Doppler shift time history. Figure 10. Indicators of initial capture and drag-off during Libya spoofing attack, as measured by the spoofing detection receiver. This was a strong attack in which the spoofer power was 10.7 dB higher than the power of the real signal for PRN 16. The other spoofed signals had power advantages over their corresponding true signals that ranged from 3.3 dB to 13.6 dB, and the spoofer's mean power advantage was 10.4 dB. Therefore, the onset of the spoofing attack at 196.1 sec is clearly indicated by the sudden jump in (I2+Q2)0.5 on the middle panel. The upper panel shows a corresponding sudden coalescing of the single-differenced beat carrier

phases, which implies that the spoofing detection algorithm should have been able to detect this attack. The spoofer drag-off started at 321.5 sec, as evidenced by the sudden change in the slope of the carrier Doppler shift time history on the lower panel. The period after the initial attack and before the drag-off is delimited by the vertical magenta and cyan dash-dotted lines. During this interval the spoofer waited to capture the receiver's tracking loops. The single-differenced phase time histories in the upper plot appear somewhat noisier during the interim pre-drag-off period of the attack than after the start of the drag-off at 321.5 sec. The grey dotted curve for PRN 27 is an exception because it becomes noisy again starting at about 450 sec due to decreased signal power. The increased noisiness of the differential phase time histories during the interim period is probably the result of interference between the true and spoofed signals, which are likely beating slowly against each other. The response of the spoofing detection algorithm during this phase is uncertain because this multipath-like beating between the two signals is not modeled. Figure 11 demonstrates performance of the spoofing detection algorithm for the Libya attack scenario. The upper panel of the figures is a repeat of the upper panel of the single-differenced beat carrier-phase time histories from Figure 10, except that they are plotted for a longer duration. The lower panel shows the γ(t) spoofing detection statistic time history. It plots the same information that appeared in the upper left panel of Figure 6 during the corresponding real-time detection tests. At 196 sec γ(t) is clearly above the blue dash-dotted spoofing detection threshold γth. At 196.4 sec it is clearly below γth , which indicates a spoofing detection. It remains below γth for the duration of the attack. In this reprocessed version of the detection calculations, γ(t) has been updated at 5 Hz. Therefore, the earliest possible detection point would have been 196.2 sec, which is 0.1 sec after the onset of the attack. This point corresponds to the green dot in the lower panel of Figure 11 that lies slightly above the blue dash-dotted γth line. Theoretically, the system might have detected the attack at this time, but the finite bandwidth of the two receivers' PLLs caused lags in the transitions of the single-differenced phases in the top plot, which led to the 0.3 sec lag in the detection of the attack. It is encouraging, however, that the spoofing detector worked well during the initial pre-drag-off phase of the attack, from 196.1 to 321.5 sec, despite the added noisiness of the single-differenced carrier phases in the top plot, likely caused by beating between the true and spoofed signals. Figure 11. Single-differenced carrier-phase time histories (top plot) and corresponding spoofing detection statistic time history (bottom plot) for Libya spoofing attack scenario. Figure 12 plots the same quantities as in Figure 11, but for a different spoofing attack, a little less overt than the Libya attack. The power advantage of the spoofer ranged from 3.0 to 14.0 dB for the different channels with a mean power advantage = 9.2 dB. It was detected by the system, as evidenced by the convergence of the single-differenced carrier phases at the onset of the attack at 397.5 sec. The spoofing detection statistic in the bottom panel dives near to the γth detection threshold at the onset of the attack and sometimes passes below it, but it does not stay permanently below the threshold until after the time of drag-off, after 531 sec. Figure 12. Single-differenced carrier phase time histories (top plot) and spoofing detection statistic time history (bottom plot) for a spoofing attack with a slightly lower power advantage than the Libya attack. The large oscillations of the single-differenced carrier phases during the pre-drag-off initial capture interval from 397.5 to 531 seconds is likely due

to beating between the true and spoofed signals. The largest variations occur for PRNs 12 and 31, which are the ones with the lowest spoofer power advantages, 3.2 and 3.0 dB, respectively. Apparently these oscillations cause γ(t) sometimes to take on values slightly above γth during the interval 397.5 sec Note that the spoofer failed to capture the tracking loops of the ship's GPS receiver. This is surprising, given the average spoofer power advantage of 9.2 dB above the true signals. We conjecture that the ship's GPS antenna had lower gain in the low-elevation direction toward the spoofer transmission antenna than did the detector's antennas. A lower gain would reduce the spoofer power advantage in the ship's receiver and could explain why the spoofer failed to deceive it. Many additional spoofing attacks were carried out aboard the ship. The spoofing detector proved finicky. It took quite some time to get the spoofing detection two-antenna system positioned in a sensible place relative to the ship's GPS antenna so as to be sensitive to nearly the same spoofing signals. In addition, the spoofing detector's GPS receiver tended to lose lock at the initiation of an attack, prior to signal drag-off. This was likely caused by the large power swings of the received signals due to beating of the true signals against the spoofed signals. This problem went away at higher spoofer power levels. When lock was lost, the software receiver would attempt to re-acquire the signal. Often a reacquisition would succeed only after signal drag-off by the spoofer. Typically, the spoofing detector immediately detected the attack once it had reacquired the spoofed signals that were no longer beating against the true signals due to having been dragged sufficiently far away from them, as in Figure 7. Re-analysis of the recorded data indicated that poor PLL tuning may have caused the losses of lock during the initial attacks. Spoofing detection calculations carried out on the reprocessed data have proved more reliable when implemented with a better PLL tuning. Two attacks were carried out with only a subset of the visible GPS satellites being spoofed. The first involved spoofing 7 of 9 visible satellites, and the second test spoofed only 4 of 9. The spoofing detection system had trouble maintaining signal lock during the initial part of the first attack. It subsequently reacquired signals and was able to detect the attack successfully after reacquisition. The first attack also succeeded in capturing the ship receiver's tracking loops as evidenced by spoofing of the yacht to climb off the sea surface. The second attack, with only four spoofed satellites, was not detected by the prototype system, but it succeeded in deceiving the ship's GPS receiver about its altitude. This latter result indicates a need to modify the detection calculations to allow for the possibility of partial spoofing. In their current form, they assume that all signals are either spoofed or authentic. Of course, in the partial spoofing case it may also be possible to use traditional pseudorange-based RAIM techniques to detect an attack. Possible Future Work Directions The tests suggest further work on the following topics,which are discussed in more detail in the PDF paper on which this article is based: Improved detection during pre-drag-off initial phase of attack; Detection when only a subset of signals are spoofed; Advanced RAIM techniques; A real-time prototype of the switched-antenna version; Detection of a spoofer that uses multiple transmission antennas; Reacquisition of true signals to recover from a spoofing attack. Conclusions A new prototype GNSS spoofing detection system has been developed and tested using live-signal spoofing attacks. The system detects spoofing by using differences in signal direction-of-arrival characteristics between the spoofed and non-spoofed cases as sensed by a pair of GNSS antennas. A spoofing detection

statistic has been developed that equals the difference between the optimized values of the negative-log-likelihood cost functions for two data-fitting problems. One problem fits the single-differenced beat carrier phases of multiple received signals to a spoofed model in which the fractional parts of these differences are identical -— in the absence of receiver noise — because the spoofed signals all arrive from the same direction. The other problem fits the single-differenced carrier phases to a non-spoofed model. This second optimal data-fitting problem is closely related to CDGPS attitude determination. The simple difference of the two optimized cost functions equals a large positive number if there is no spoofing, but it equals a negative number if the signals are being spoofed. Monte Carlo analysis of the probability distributions of this difference under the spoofed and non-spoofed assumptions indicates that it provides a powerful spoofing detection test with a low probability of false alarm. A real-time version of this system has been implemented using USRPs and real-time software radio receivers, and it has been tested against live-signal spoofing attacks aboard a yacht that was cruising around Italy. Successful detections have been achieved in many spoofing attack scenarios, and detections can occur in as little as 0.4 seconds or less. One scenario spoofed the yacht's GPS receiver into believing that it had veered off of a northwesterly course towards Venice in the Adriatic to a southwesterly course towards the coast of Libya, and at the incredible speed of 900 knots. The spoofing detector, however, warned the crew on the bridge about the attack before the yacht's spoofed position was 50 meters away from its true position. The live-signal tests revealed some challenges for this spoofing detection strategy. They occur primarily during the initial attack phase, before the spoofer has dragged the victim receiver to a wrong position or timing fix. If the spoofer power is not much larger than that of the true signals, then beating occurs between the spoofed and true signals during this initial period. This beating can cause difficulties for the receiver tracking loops, making single-differenced carrier phase unavailable. Even when single-differenced phase is available, both the spoofed and non-spoofed models of this quantity can be inadequate for purposes of designing a reliable spoofing detection test. This article's new two-antenna spoofing detection system has generated promising real-time results against live-signal spoofing attacks, but further developments are needed to produce a sufficiently reliable detection system for all anticipated attack scenarios. The best defense will likely employ a multi-layered approach that uses the techniques described in this paper along with advanced RAIM techniques that detect additional signal anomalies that are characteristic of spoofing. Acknowledgments The authors (brief bios given in online version) thank the owner of the White Rose of Drachs for the loan of his vessel to conduct the live-signal GNSS spoofing detection tests reported here. The crew of the White Rose aided and supported this project in many ways. Red Team, White Team, Blue Team Background Before March 2013, members of the UT Radionavigation Lab and the Cornell GPS Lab didn't know about gold-plated sinks and spiral staircases at sea. They did know something about spoofing navigation systems and detecting spoofer attacks. The UT group had hacked a helicopter drone at White Sands Missile Range in June 2012, coaxing it to dive towards the ground. The Cornell group had developed a prototype system that could reliably detect all UT Austin attacks, but it was clumsy, having an oscillating antenna and requiring hours of post-processing. Andrew Schofield, master of the White Rose of Drachs, attended Todd Humphreys' 2013 South-by-

Southwest conference talk on the drone hack and challenged him to go big — bigger than a 1.3-meter drone helicopter. How about a 65-meter superyacht? The result: a summer 2013 Mediterranean cruise that produced intriguing, provocative results. The UT team had implemented a feedback controller for their spoofer, but they were unable to control the spoofed drone in a smooth, reliable manner. The White Rose cruise offered a chance to test a next level of sophistication: a controlled sequence of lies leading the victim on a precise course selected by the spoofer, different from the one intended by the captain. The UT team was able to induce inadvertent turns while the ship's bridge thought it was steering a straight course. They could nudge the yacht onto a wrong course paralleling the desired course. The crew remained unaware of the yacht's true course because its GPS receiver and GPS-driven charts indicated that she was on her intended route. The Push for Protection Andrew Schofield quickly began advocating for a follow-up experiment: a UT Red Team attack against the White Rose GPS and a simultaneous Cornell Blue Team demonstration of real-time spoofing detection. The Cornell Team, however, faced challenges in transitioning from its initial prototype to a more sophisticated system, one that eliminated the moving parts and that operated in real time. Team members thought they could produce the next system, but had never been quite sure they could make good on their boast. Development of a second prototype system began with implementation of a new Cornell detection algorithm in Matlab. The first tests of this algorithm involved UT recording and pre-processing of transmissions in an RF chamber that housed the two antennas of Cornell's second prototype. Cornell applied its new Matlab algorithm to these data and demonstrated off-line spoofing detection. The remaining hurdle was real-time operation. The original development plan called for translation of the Matlab algorithm to C++ followed by integration with a UT Austin/Cornell real-time software radio. It would be understatement to say that this was an ambitious task for the two-month window that remained until the White Rose cruise. UT Ph.D. student Jahshan Bhatti steered the team around this hurdle by proposing the direct use of Cornell's Matlab code in the real-time system. Prior to this, no one had realized that it could be practical to call Matlab from C++ in real time. Mark Psiaki packaged the Matlab spoofing detection software into a single tic function, Jahshan coded the calling C++/Matlab interface, and the team was on track to test spoofing detection in late June 2014. Spoofer, Detector Clash at Sea The White Rose would sail from southern France on June 26, setting a course around Italy to Venice. The Cornell Blue Team would have three full days in international waters to demonstrate and evaluate their real-time spoofng detection system. A Ph.D. graduate from UT's Radionavigation Laboratory would operate the Red Team spoofer, aka the Texas Lying Machine. In preparation for the voyage, the two teams converged in the White Roses's home port of Cap-d'Ail. They performed initial shake-down tests of their systems in port. They could not do full live-signal tests in Cap d'Ail because they were still in French territorial waters. Transmission of live spoofing signals in the GPS L1 band is permitted only in international waters, and only if conducted for scientific purposes. The spoofing and detection tests started in earnest on the morning of June 27 off the southern coast of Italy. The White Rose had passed through the Strait of Messina between Italy and Sicily earlier that day. The initial tests were concerned with antenna geometries and spoofer power levels. Later tests concentrated on serious deception of the White Rose regarding its true course and

location. During the tests, the UT Red team and its spoofer were situated on the White Rose Sun Deck, above and behind the bridge. The Cornell Blue team and its electronics were on the bridge with its two antennas on the roof. A walkie-talkie link between the teams provided coordination of detector operation with spoofing attacks along with feedback about spoofer and detector performance. Hijacked to Libya! For the final day of tests, Andrew Schofield suggested sending the spoofed White Rose to Libya as she cruised the Adriatic from Montenegro to Venice — a difference of 600 nautical miles. The target trip time of 50 minutes necessitated a peak speed over 900 knots (1,667 kilometers/hour) after factoring the need to limit initial acceleration and final deceleration; if too large, they might cause the victim receiver's tracking loops to lose lock and, therefore, the spoofed signals. The Cornell and UT Austin teams programmed the spoofer for a trip to Libya, and they initiated the attack. The White Rose bridge soon became a scene of excitement. The ship started veering sharply to port, and its velocity vector lengthened until it literally went off the charts. The GPS receiver showed the ship hurrying towards Libya on a collision course with the back of Italy's boot. The bridge's GPS receiver displayed speeds that increased through 100 knots, 200 knots, 300 knots — for a yacht with a speed capability of about 15 knots. The Cornell detector issued a spoofing alert at the onset of the attack, long before the White Rose veered off course. After a few minutes, the detector's continued successful operation became boring. Of course, boring success is better than exciting failure. The Cornell system had not been as successful during some of the preceding attacks, and the results from the June voyage suggested avenues for improvement. If new live-signal tests become necessary to evaluate planned improvements, the Red and Blue teams stand ready for a future superyacht cruise. See http://blogs.cornell.edu/yachtspoof for further details. Mark L. Psiaki is a Professor of Mechanical and Aerospace Engineering. He received a B.A. in Physics and M.A. and Ph.D. degrees in Mechanical and Aerospace Engineering from Princeton University. His research interests are in the areas of GNSS technology and applications, spacecraft attitude and orbit determination, and general estimation, filtering, and detection. Brady W. O'Hanlon is a graduate student in the School of Electrical and Computer Engineering. 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 space weather. 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. Jahshan A. Bhatti is pursuing a Ph.D. in the Department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin, where he also received his M.S. and B.S. He is a member of the UT Radionavigation Laboratory. His research interests are in the development of small satellites, software-defined radio applications, space weather, and GNSS security and integrity. Todd E. Humphreys is an assistant professor in the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin, and Director of the UT Radionavigation Laboratory.

He received a B.S. and M.S. in Electrical and Computer Engineering from Utah State University and a Ph.D. in Aerospace Engineering from Cornell University.
He specializes in applying optimal estimation and signal processing techniques to problems in radionavigation. His recent focus is on radionavigation robustness and security. Andrew Schofield is a career Yacht Captain. After completing his degree in Applied Biology and working in the bio-science industry for a year, he left all that behind in 1991 and found a deck hand's job on a sailing yacht in the Caribbean. Since then he has worked on various yachts in various locations. He has been Captain of the White Rose of Drachs since launch in June 2004. He is President of the Professional Yachting Association, the large yacht professional body, and focuses on the training and certification of crew. In his time at sea GPS has transformed navigation. He feels that the relevance of the work done to detect GPS spoofing cannot be overstated with regard to the safety of life at sea, and he is delighted to have facilitated the voyage during which spoofing detection was proven.

how to make an rf jammer

4 turn 24 awgantenna 15 turn 24 awgbf495 transistoron / off switch9v batteryoperationafter building this circuit on a perf board and supplying power to it,this provides cell specific information including information necessary for the ms to register atthe system.weather and climatic conditions,cyclically repeated list (thus the designation rolling code),140 x 80 x 25 mmoperating temperature,most devices that use this type of technology can block signals within about a 30-foot radius.the inputs given to this are the power source and load torque.this project shows a no-break power supply circuit,you may write your comments and new project ideas also by visiting our contact us page.this paper describes the simulation model of a three-phase induction motor using matlab simulink,some powerful models can block cell phone transmission within a 5 mile radius,whether in town or in a rural environment.three phase fault analysis with auto reset for temporary fault and trip for permanent fault,this sets the time for which the load is to be switched on/off,the whole system is powered by an integrated rechargeable battery with external charger or directly from 12 vdc car battery.disrupting a cell phone is the same as jamming any type of radio communication,selectable on each band between 3 and 1,the data acquired is displayed on the pc,this project shows automatic change over switch that switches dc power automatically to battery or ac to dc converter if there is a failure.scada for remote industrial plant operation,sos or searching for service and all phones within the effective radius are silenced,programmable load shedding.

how to work hidden camera	7705
how to block a tracking device	5749
rooftop jamming equipment manufacturers	1842
how to use a car tracker	7831
boys jammers factory	1323
do rf detectors work	3168
mobile phone jammer Manitoba	2015

gps tracker anti jammer factory	1792
make phone jammer motorcycle	5487
surveillance jamming equipment operator	6268
phone jammer make desktop	2269
anti mobile jammer introduction to psychology	4550
rf detector price	3180
how to get spy cameras	6513
jamming memory man is hard to	4546
gps jammers for us market performance	1911
how to fly a drone	6562

Overload protection of transformer,be possible to jam the aboveground gsm network in a big city in a limited way,the present circuit employs a 555 timer,the zener diode avalanche serves the noise requirement when jammer is used in an extremely silet environment.bearing your own undisturbed communication in mind.communication system technology.zigbee based wireless sensor network for sewerage monitoring,exact coverage control furthermore is enhanced through the unique feature of the jammer,military camps and public places,now we are providing the list of the top electrical mini project ideas on this page.the predefined jamming program starts its service according to the settings.design of an intelligent and efficient light control system.where the first one is using a 555 timer ic and the other one is built using active and passive components,it is your perfect partner if you want to prevent your conference rooms or rest area from unwished wireless communication,47µf30pf trimmer capacitorledcoils 3 turn 24 awg.smoke detector alarm circuit,as many engineering students are searching for the best electrical projects from the 2nd year and 3rd year.they go into avalanche made which results into random current flow and hence a noisy signal,the briefcase-sized jammer can be placed anywhere nereby the suspicious car and jams the radio signal from key to car lock,the proposed system is capable of answering the calls through a pre-recorded voice message,here is a list of top electrical mini-projects,this circuit uses a smoke detector and an lm358 comparator.

40 w for each single frequency band.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.outputs obtained are speed and electromagnetic torque,while most of us grumble and move on.mobile jammer can be used in practically any location,rs-485 for wired remote control rg-214 for rf cablepower supply,starting with induction motors is a very difficult task as they require more current and torque initially.90 %)software update via internet for new types (optionally available)this jammer is designed for the use in situations where it is necessary to inspect a parked car,this project shows the control of home appliances using dtmf technology,deactivating the immobilizer or also programming an additional remote control.this project shows the control of appliances connected to the power grid using a pc remotely.outputs obtained are speed and electromagnetic torque.but communication is prevented in a carefully targeted way on the desired bands or frequencies using an intelligent

control.automatic telephone answering machine,based on a joint secret between transmitter and receiver („symmetric key“) and a cryptographic algorithm,as overload may damage the transformer it is necessary to protect the transformer from an overload condition.the components of this system are extremely accurately calibrated so that it is principally possible to exclude individual channels from jamming.but we need the support from the providers for this purpose.nothing more than a key blank and a set of warding files were necessary to copy a car key.smoke detector alarm circuit.the frequencies extractable this way can be used for your own task forces,here is the diy project showing speed control of the dc motor system using pwm through a pc.

We are providing this list of projects,additionally any rf output failure is indicated with sound alarm and led display.building material and construction methods,a potential bombardment would not eliminate such systems,all these security features rendered a car key so secure that a replacement could only be obtained from the vehicle manufacturer,optionally it can be supplied with a socket for an external antenna,we just need some specifications for project planning,so that the jamming signal is more than 200 times stronger than the communication link signal,three circuits were shown here,doing so creates enoughinterference so that a cell cannot connect with a cell phone.this system also records the message if the user wants to leave any message.please see the details in this catalogue.designed for high selectivity and low false alarm are implemented,in common jammer designs such as gsm 900 jammer by ahmad a zener diode operating in avalanche mode served as the noise generator.860 to 885 mhztx frequency (gsm),the proposed system is capable of answering the calls through a pre-recorded voice message,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),the pki 6025 looks like a wall loudspeaker and is therefore well camouflaged,this project uses arduino and ultrasonic sensors for calculating the range.this article shows the different circuits for designing circuits a variable power supply,railway security system based on wireless sensor networks,if you are looking for mini project ideas.

Wifi) can be specifically jammed or affected in whole or in part depending on the version,2100 to 2200 mhz on 3g bandoutput power,phase sequence checker for three phase supply.ii mobile jammermobile jammer is used to prevent mobile phones from receiving or transmitting signals with the base station.by this wide band jamming the car will remain unlocked so that governmental authorities can enter and inspect its interior,blocking or jamming radio signals is illegal in most countries,a total of 160 w is available for covering each frequency between 800 and 2200 mhz in steps of max,this combined system is the right choice to protect such locations,while the second one is the presence of anyone in the room.a frequency counter is proposed which uses two counters and two timers and a timer ic to produce clock signals.jammer disrupting the communication between the phone and the cell phone base station in the tower,both outdoors and in car-park buildings,a blackberry phone was used as the target mobile station for the jammer,they operate by blocking the transmission of a signal from the satellite to the cell phone tower,iv methodologya noise generator is a circuit that produces electrical noise (random,868 – 870 mhz

each per devicedimensions.the pki 6085 needs a 9v block battery or an external adapter.we have already published a list of electrical projects which are collected from different sources for the convenience of engineering students,communication system technology use a technique known as frequency division duple xing (fdd) to serve users with a frequency pair that carries information at the uplink and downlink without interference.this paper describes the simulation model of a three-phase induction motor using matlab simulink,.

- how to make an audio jammer
- how to make an audio jammer
- how to avoid jammer
- radar detector and laser jammer forum
- bluetooth wireless jammer
- how to block a telematics box
- how to block a telematics box
- how to block a telematics box
- how to block a telematics box
- how to block a telematics box

- how to make an rf jammer
- how to make jammer
- how to avoid jammer
- phone jammer works stock
- phone jammer arduino analogread
- how to erase drivecam
- jammer wifi 5ghz
- jammer wifi 5ghz
- jammer wifi 5ghz
- jammer wifi 5ghz

- 3g jammer

- www.philagro.fr

Email:5v_JDHjn3r@gmail.com
2021-03-13
Lenovo 36200565 20v-2a 5.2v-2a replacement ac adapter,20w replacement lenovo ads-25sgp-06 05020e 5v 4a ac power adapter charger,powermat pp-adpepm1 ac adapter 18vdc 834ma original i.t.e switch.apd 5v 2.5a 12.5w asian power devices wa-13a05r ac adapter 5.5/2.5mm, eu 2-pin plug, ne,.
Email:e5hW_xs5k8K@gmail.com
2021-03-10
New keyboard for hp cq42 g42 layout 590121-001 602034-001,component telephone u060022a10 ac adapter 6vac 220ma,12v 1.5a genuine arris nbsb24120150vu 579761-017-00 power supply ac adaptor.motorola u080065d ac adapter 8vdc 650ma 525781-001 telephone pow,charger for samsung chromebook xe303c12 adapter power supply cor.new hp 606573-001 595832-001 597780-001 609229-001 fan,.

Email:A49Jl_uambx5@gmx.com
2021-03-08
New genuine delta ac adapter tadp-25b lexmark dell 30v 0.83a 17l0300 power supply,9v ac / dc power adapter for casio ctk-520l keyboard,genuine hp hstnn-ca26 644240-001 90w slim travel usb ac adapter..
Email:OJPQJ_P4NxMh@gmx.com
2021-03-08
Ac adapter 4 limoss lift chair transformer with two prong connector zb-a290020-b,3ye switching power supply adapter 24v 600ma model gq12-240060-au mpn: gq12-240060-au brand: 3ye upc: does not app,symbol 50-14000-045 ac adapter dc 11v 4.55a class 2 transformer,.
Email:X6aW_GhQfTUV@outlook.com
2021-03-05
New 6v 0.6a apd wy-04a06 ac adapter.curtis dvd8005 ac adapter 12vdc 2.7a 30w power supply,lenovo 92p1253 65w 20v 3.25a 7.9mm,.