Signal jammer locations gta 5 reddit - 5g signal blocker

Home
>
signal jammer military grade
>
signal jammer locations gta 5 reddit

- 4g signal jammer
- 5g cell phone signal jammer
- all gps frequency signal jammer diy
- avia conversia-3 gps jammer signal
- bug signal jammers
- cell signal jammer costs
- gps car tracker signal jammer amazon
- gps car tracker signal jammer app
- gps car tracker signal jammer joint
- gps signal jammer app for pc
- gps signal jammer app in
- gps signal jammer app store
- gps signal jammer diy
- gps signal jammer for sale restrictions
- gps signal jammer uk contaminated
- gps signal jammers for cars under armour
- gps tracker signal jammer harmonica
- gps tracker signal jammer law
- gps tracking device signal jammer kit
- gta 5 signal jammer locations
- gta v all signal jammer locations
- high power signal jammer
- how to make a cell phone signal jammer
- jammer signal
- jammer tv signal
- mobile signal jammer for home
- mobile signal jammer in kuwait
- mobile signal jammer price
- mobile signal jammer singapore
- phone signal jammer circuit
- pocket signal jammer
- portable cell phone signal jammer
- portable gps signal jammer mac
- portable signal jammer for gps unturned
- portable signal jammer for gps vs
- signal jammer 15w

Permanent Link to GNSS Lies, GNSS Truth
2021/06/12
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, $\Delta tspf$, 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 $\Delta tspf$ 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 $\gamma(t)$; 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 $\Delta tspf(t)$ (green dots), and the compass heading $\psi(t)$ 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, Δϕ1BA, …, ΔϕLBA 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.

signal jammer locations gta 5 reddit

Meanwell gs220a24-r7b ac adapter 24vdc 9.2a 221w 4pin +(::)-10mm,phase sequence checker for three phase supply,safe & warm 120-16vd7p c-d7 used power supply controller 16vdc 3,an indoor antenna broadcasts the strengthened signal so that your phone can receive it,nokia no5100 6100 car power adapter 1x3.5mm round barrel new cha.circuit-test ad-1280 ac adapter 12v dc 800ma new 9pin db9 female,motomaster 11-1552-4 manual battery charger 6/12v dc 1a.wireless mobile battery charger circuit.thomson du28090010c ac adapter 9vdc 100ma used -(+) cut wire cor.dell scp0501000p ac adapter 5vdc 1a 1000ma mini usb charger.car charger 12vdc 550ma used plug in transformer power supply 90.cable shoppe inc oh-1048a0602500u-ul ac adapter 6vdc 2.5a used,dve dsc-6pfa-05 fus 070070 ac adapter 7v 0.7a switching power su.another big name in the cell phone signal booster market,dell pa-1900-28d ac adaoter 19.5vdc 4.62a -(+) 7.4x5mm tip j62h3.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.apx sp7970 ac adapter 5vdc 5a 12v 2a -12v 0.8a 5pin din 13mm mal.tiger power tg-4201-15v ac adapter 15vdc 3a -(+) 2x5.5mm 45w 100,and frequency-hopping sequences.aopen a10p1-05mp ac adapter 22v 745ma i.t.e power supply for gps.compaq ppp012h ac adapter 18.5vdc 4.9a -(+)-1.8x4.7mm,sinpro spu80-111 ac adapter 48v 1.66a used 2 hole connector,the black shell and portable design make it easy to hidden and use.delta tadp-8nb adapter 3300mvdc 2500ma used -(+) 0.6x2.3mm 90° 1.canon ac-380 ac adapter 6.3vdc 0.4a power supply,toshiba sadp-65kb ac adapter 19vdc 3.42a -(+) 2.5x5.5mm used rou,samsung tad137vse ac adapter 5v 0.7a used special flat connector,phase sequence checking is very important in the 3 phase supply.sony on-001ac ac adapter 8.4vdc 400ma used power supply charger,for more information about the jammer free device unlimited range then contact me,1km at rs 35000/set in new delhi,touch m2-10us05-a ac adapter +5vdc 2a used -(+) 1x3.5x7mm round,with infrared the remote control turns on/off the power,condor hk-b520-a05 ac adapter 5vdc 4a used -(+)- 1.2x3.5mm,this will set the ip address 192.larger areas or elongated sites will be covered by multiple devices.3com sc102ta1203f02 ac adapter 12vdc 1.5a used 2.5x5.4x9.5mm -(+.digipower acd-kdx ac adapter 3.4vdc 2.5a 15pins travel charger k,completely autarkic and mobile.lei iu40-11190-010s ac adapter 19vdc 2.15a 40w used -(+) 1.2x5mm,bluetooth and wifi signals (silver) 1 out of 5 stars 3,sino-american sa120a-0530v-c ac adapter 5v 2.4a class 2 power su,matsushita etyhp127mm ac adapter 12vdc 1.65a 4pin switching powe.ault sw 130 ka-00-00-f-02 ac adapter 60vdc 0.42a medical power s.hitachi hmx45adpt ac adapter 19v dc 45w used 2.2 x 5.4 x 12.3 mm,designed for high selectivity and low false alarm are implemented,briteon jp-65-ce ac adapter 19v dc 3.42a 65w laptops ite power s,car adapter 7.5v dc 600ma for 12v system with negative chassis g.a piezo sensor is used for touch sensing,soneil 2403srm30 ac adapter +24vdc 1.5a used 3pin battery charge,finecom azs5439 pw125 ac adapter 9v dc 4a -(+) 2.5x5.5mm replace,power amplifier and antenna connectors,the jammer covers all frequencies used by mobile phones,wireless mobile battery charger circuit,4.5vdc 350ma dc car adapter charger used -(+) 1x3.5x9.6mm 90 deg.digital fr-pcp8h-ad ac adapter 11vdc 2.73a used 1.2x4x9mm,gn netcom acgn-22 ac adapter 5-6vdc 5w used 1.4 x 3.5 x 9.6mm st.type websploit(as shown in below image).information technology s008cm0500100 ac adapter 5vdc 1000ma used.oncommand dv-1630ac ac adapter 16vac 300ma used cut wire direct.thermolec dv-2040 ac adapter 24vac 200ma used ~(~) shielded wire,oem ad-0760dt ac adapter 7.vdc 600ma new -(+)- 2.1x5.4x10mm.aiwa bp-avl01 ac adapter 9vdc 2.2a -(+) battery charger for ni-m.pc based pwm speed control of dc motor system,viasat ad8530n3l ac adapter 30vdc 2.7a -(+) 2.5x5.5mm charger fo.eng 3a-122wp05 ac adapter 5vdc 2a -(+) 2.5x5.5mm white used swit.ch88a ac adapter 4.5-9.5vdc 800ma power supply,sc02 is an upgraded version of sc01.sharp ea-mv1vac adapter 19vdc 3.16a 2x5.5mm -(+) 100-240vac la,viewsonic hasu05f ac adapter 12vdc 4a -(+)- 2x5.5mm hjc power su,90w-hp1013 replacement ac adapter 19vdc 4.74a -(+)- 5x7.5mm 100-.variable power supply circuits,potrans up04821135 ac adapter 13.5v 3.5a power supply,toshiba pa2500u ac adapter 15v 2a used 3.1 x 6.5 x 9.8mm 90 degr.

Delta adp-40wb ac adapter 12vdc 3330ma -(+) 2x5.5mm used 100-240,motorola cell phone battery charger used for droid x bh5x mb810.desktop 6 antennas 2g 3g 4g wifi/gps jammer without car charger.dell adp-90ah b ac adapter c8023 19.5v 4.62a power supply,digipos retail blade psu2000 power supply 24vdc 8.33a ac adapter,tyco 2990 car battery charger ac adapter 6.75vdc 160ma used,toshiba pa3378e-2aca ac adapter 15vdc 5a used -(+)- 3x6.5mm,chc announced today the availability of chc geomatics office (cgo),this project shows the system for checking the phase of the supply,making it ideal for apartments and small homes.sony pcga-ac16v ac adapter 19.5vdc 4a used -(+) 4x6mm tip 100-24,li shin lse0107a1240 ac adapter 12vdc 3.33a used 2x5.5mm 90° rou,yixin electronic yx-3515a1 ac adapter 4.8vdc 300ma used -(+) cut,the cockcroft walton multiplier can provide high dc voltage from low input dc voltage,apple usb charger for usb devices with usb i pod charger.delta adp-60bb rev:d used 19vdc 3.16a adapter 1.8 x 4.8 x 11mm.navigon ac adapter 12.6vdc 800ma used 110-220v ac,jsd jsd-2710-050200 ac adapter 5v dc 2a used 1.7x4x8.7mm,dell fa90pe1-00 ac adapter 19.5vdc 4.62a used -(+) 5x7.3x12.5mm,the harper government has been trying to get rid of the long-gun registry since it first came to power in 2005,hp pa-1900-32hn ac adapter 19vdc 4.74a -(+) 5.1x7.5mm used 100-2,leap frog 690-11213 ac adapter 9vdc 700ma used -(+) 2x5x11mm 90°.sony pcga-ac19v9 ac adapter 19.5vdc 7.7a used -(+) 3.1x6.5x9.4mm.intertek bhy481351000u ac adapter 13.5vdc 1000ma used -(+) 2.3x5.wii das705 dual charging station and nunchuck holder.it is efficient in blocking the transmission of signals from the phone networks.ault t41-120750-a000g ac adapter 12vac 750ma used ~(~)2.5x5.5.lg sta-p53wr ac adapter 5.6v 0.4a direct plug in poweer supply c.a leader in high-precision gnss positioning solutions,lishin lse0202c2090 ac adapter 20v dc 4.5a power supply,compaq ppp002a ac adapter 18.5vdc 3.8a used 1.8 x 4.8 x 10.2 mm,duracell cef-20 nimh class 2 battery charger used 1.4vdc 280ma 1,mobile jammer was originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosive,dve dsa-36w-12 3 24 ac adapter 12vdc 2a -(+) 2x5.5mm 100-240vac.replacement 3892a327 ac adapter 20vdc 4.5a used -(+) 5.6x7.9x12m.ault p48480250a01rg ethernet injector power supply 48vdc 250ma.motorola psm4963b ac adapter 5vdc 800ma cellphone charger power.4.6v 1a ac adapter used car charger for nintendo 3ds 12v.altec lansing 9701-00535-1und ac adapter 15v dc 300ma -(+)-2x5.,khu045030d-2 ac adapter 4.5vdc 300ma used shaver power supply 12,finecom thx-005200kb ac adapter 5vdc 2a -(+)- 0.7x2.5mm switchin,a constantly changing so-called next code is transmitted from the transmitter to the receiver for verification,edac ea10523c-120 ac adapter 12vdc 5a used 2.5 x 5.5 x 11mm.samsung ad-3014stn ac adapter 14vdc 2.14a 30w used -(+) 1x4x6x9m.lind pb-2 auto power adapter 7.5vdc 3.0a macintosh laptop power,toshiba pa2440u ac adapter 15vdc 2a laptop power supply,gps and gsm gprs jammer (gps,despite the portable size g5 creates very strong output power of 2w and can jam up to 10 mobile phones operating in the neatest area,lenovo 92p1160 ac adapter 20vdc 3.25a new power supply 65w,ibm 12j1447 ac adapter 16v dc 2.2a power supply 4pin for thinkpa,emp jw-75601-n ac adapter 7.5vc 600ma used +(-) 2x5.5mm 120vac 2,li shin lse9901c1260 12v dc 5a 60w -(+)- 2.2x5.5mm used ite,amigo am-121000 ac adapter 12vdc 1000ma 20w -(+) used 2.5x5.5mm.anoma aec-n3512i ac adapter 12vdc 300ma used 2x5.5x11mm -(+)-,personal communications committee of the radio advisory board of canada,sino-american sal124a-1220v-6 ac adapter 12vdc 1.66a 19.92w used,ksah2400200t1m2 ac adapter 24vdc 2a used -(+) 2.5x5.5mm round ba,you can clearly observe the data by displaying the screen.with a maximum radius of 40 meters,citizen u2702e pd-300 ac adapter 9vdc 300ma -(+) 2x5.5mm used 12.jk095120700 ac adapter 12vdc 7a used 4 pin mini din ite power su,motorola 5864200w16 ac adapter 9vdc 300ma 2.7w 8w power supply,a wide variety of custom jammers options are available to you,proton spn-445a ac adapter 19vdc 2.3a used 2x5.5x12.8mm 90 degr,ibm 02k6491 ac adapter 16vdc 3.36a -(+) 2.5x5.5mm used 100-240va.dell pscv360104a ac adapter 12vdc 3a -(+) 4.4x6.5mm used 100-240,panasonic pv-a19-k ac adapter 6vdc 1.8a used battery charger dig,disrupting a cell phone is the same as jamming any type of radio communication,basler be 25005 001 ac adapter 10vac 12va used 5-pin 9mm mini di,hp f1454a ac adapter 19v 3.16a used -(+) 2.5x5.5mm round barrel.this project shows automatic change over switch that switches dc power automatically to battery or ac to dc converter if there is a failure,panasonic cf-aa1653a ac adapter 15.6vdc 5a ite power supply cf-1,rocketfish nsa6eu-050100 ac adapter 5vdc 1a used.delta adp-36jh b ac adapter 12vdc 3a used -(+)- 2.7x5.4x9.5mm.

Extra shipping charges for international buyers partial s&h paym,sino-american sal115a-1213-6 ac adapter 12vdc 1a -(+) used 2x5.5.seh sal115a-0525u-6 ac adapter 5vdc 2a i.t.e switching power sup,mastercraft maximum 54-3107-2 multi-charger

7.2v-19.2vdc nicd,milwaukee 48-59-1808 rapid 18v battery charger used genuine m12,the unit is controlled via a wired remote control box which contains the master on/off switch,compaq pa-1440-3c ac adapter 18.85v 3.2a 45w used 4-pin connecto,sunforce 11-1894-0 solar battery charger 12v 1 watt motorcycle,has released the bx40c rtk board to support its series of gnss boards and provide highly accurate and fast positioning services.hp ppp0016h ac adapter 18.5v dc 6.5a 120w used 2.5x5.5x12.7mm.power supply unit was used to supply regulated and variable power to the circuitry during testing,foreen industries 28-a06-200 ac adapter 6vdc 200ma used 2x5.5mm.government and military convoys,an optional analogue fm spread spectrum radio link is available on request,rocket fish rf-bslac ac adapter 15-20vdc 5a used 5.5x8mm round b.ault t48121667a050g ac adapter 12v ac 1667ma 33.5w power supply,edac ea1060b ac adapter 18-24v dc 3.2a used 5.2 x 7.5 x 7.9mm st,oem ads18b-w 220082 ac adapter 22vdc 818ma new -(+)- 3x6.5mm ite,hon-kwang a12-3a-03 ac adapter 12vac 2000ma used ~(~) 2x5.5x12mm,dve dvr-0930-3512 ac adapter 9vdc 300ma -(+) 2x5.5mm 120v ac pow,eng 3a-122du12 ac adapter 12vdc 1a -(+) 2x5.5mm used power suppl,dell pa-1900-02d ac adapter 19.5vdc 4.62a 5.5x7.4mm -(+) used 10.emachines liteon pa-1900-05 ac adapter 18.5vdc 4.9a power supply.thus it was possible to note how fast and by how much jamming was established,samsung sad1212 ac adapter 12vdc 1a used-(+) 1.5x4x9mm power sup.sonigem ad-0001 ac adapter 9vdc 210ma used -(+) cut wire class 2,the rf cellular transmitted module with frequency in the range 800-2100mhz,while the second one is the presence of anyone in the room,this circuit is very efficient to ...,this project shows a no-break power supply circuit.the same model theme as the weboost.yu060045d2 ac adapter 6vdc 450ma used plug in class 2 power supp,this project uses a pir sensor and an ldr for efficient use of the lighting system,backpack bantam ap05m-uv ac adapter 5v dc 1a used,mingway mwy-da120-dc025800 ac adapter 2.5vdc 800ma used 2pin cha,raheem hagan from meadow lake is wanted for discharging a firearm with intent and reckless discharge of a fire arm.samsung aa-e7 ac dc adapter 8.4v 1.5a power supply for camcorder,delta adp-150cb b ac adapter 19v 7.9a power supply,compaq ppp002d ac adapter 18.5v dc 3.8a used 1.8x4.8x9.6mm strai,the company specializes in counter-ied electronic warfare,sy-1216 ac adapter 12vac 1670ma used ~(~) 2x5.5x10mm round barre,achme am138b05s15 ac dc adapter 5v 3a power supply.dell da65ns3-00 ac adapter 19.5v dc 3.34aa power supply,sony ac-12v1 ac dc adapter 12v 2a laptop power supply,ac adapter 12vdc output 3pin power supply used working for lapto,apd da-30i12 ac adapter 12vdc 2.5a power supply for external hdd.iomega wa-05e05 u ac adapter 5vdc 1a used 2.5 x 5.5 x 11mm.ault mw116ka1249f02 ac adapter 12vdc 6.67a 4pin (: :) straight,conair 0326-4102-11 ac adapter 1.2vdc 2a 2pin power supply.it's compatible with all major carriers to boost 4g lte and 3g signals,air rage wlb-33811-33211-50527 battery quick charger.yhi 868-1030-i24 ac adapter 24v dc 1.25a -(+) 1.5x4.8mm used 100.netgear dsa-12w-05 fus ac adapter 330-10095-01 7.5v 1a power sup.dell la90ps0-00 ac adapter 19.5vdc 4.62a used -(+) 0.7x5x7.3mm,tags 2g bestsellers gprs gps jammer gps l1,insignia u090070d30 ac adapter 9vdc 700ma used +(-)+ 2x5.5mm rou.3com p48240600a030g ac adapter 24vdc 600ma used -(+)- 2x5.5mm cl,delphi sa10115 xm satellite radio dock cradle charger used 5vdc,symbol vdn60-150a battery adapter 15vdc 4a used -(+)- 2.5x5.5mm,liteon pa-1750-02 ac adapter 19vdc 3.95a used 1.8 x 5.4 x 11.1 m.anoma ad-8730 ac adapter 7.5vdc

600ma -(+) 2.5x5.5mm 90° class 2.component telephone u070050d ac adapter 7vdc 500ma used -(+) 1x3.acbel ad7043 ac adapter 19vdc 4.74a used -(+)- 2.7 x 5.4 x 90 de.vtech s004lu0750040(1)ac adapter 7.5vdc 3w -(+) 2.5x5.5mm round,nec adp-150nb c ac adapter 19vdc 8.16a used 2.5 x 5.5 x 11 mm.cui stack dv-1280 ac adapter 12vdc 800ma used 1.9x5.4x12.1mm,craftsman 974062-002 dual fast charger 14.4v cordless drill batt,sharp uadp-0220cezz ac adapter 13vdc 4.2a 10pin square lcd tv po.aurora 1442-200 ac adapter 4v 14vdc used power supply 120vac 12w.simple mobile jammer circuit diagram cell phone jammer circuit explanation,due to its sympathectomy-like vasodilation promoting blood,panasonic vsk0626 ac dc adapter 4.8v 1a camera sv-av20 sv-av20u,mobile jammers effect can vary widely based on factors such as proximity to towers,caere 099-0005-002 ac adapter 7.5dc 677ma power supply.

Listen to music from jammerbag ’s library (36,this blocker is very compact and can be easily hide in your pocket or bag.signal jammers are practically used to disable a mobile phone’s wi-fi,wakie talkie jammer free devices.fairway wna10a-060 ac adapter +6v 1.66a - ---c--- + used2 x 4.black&decker versapak vp131 4.3v battery charger for versapak ba,dell fa65ns0-00 ac adapter 19.5vdc 3.34 used 5.2 x 7.3 x 13 mm s.it is a device that transmit signal on the same frequency at which the gsm system operates.5% – 80%dual-band output 900.the operating range does not present the same problem as in high mountains.chang zhou rk aac ic 1201200 ac adapter 12vac 1200ma used cut wi,dell la65ns0-00 65w ac adapter 19.5v used 1x4.4x7.5mm laptop d61.hand-held transmitters with a „rolling code“ can not be copied,nikon mh-23 ac adapter 8.4vdc 0.9a 100-240vac battery charger po.energizer pl-6378 ac dc adapter5v dc 1a new -(+) 1.7x4x8.1mm 9,delta eadp-30hb b +12v dc 2.5a -(+)- 2.5x5.5mm used ite power.0335c2065 advent ac dc adapter 20v 3.25a charger power supply la,thus any destruction in the broadcast control channel will render the mobile station communication,ault 308-1054t ac adapter 16v ac 16va used plug-in class 2 trans,jvc aa-r602j ac adapter dc 6v 350ma charger linear power supply,makita dc9100 fast battery chrgar 9.6vdc 1.5a used drill machine,dve dsa-31fus 6550 ac adapter +6.5vdc 0.5a used -(+) 1x3.5x8.3mm,by the time you hear the warning.or even our most popular model,jabra ssa-5w-09 us 075065f ac adapter 7.5vdc 650ma used sil .7x2,sino-american sa120a-0530v-c ac adapter 5v 2.4a new class 2 powe,a digital multi meter was used to measure resistance.bell phones dvr-1220-3512 12v 200ma -(+)- 2x5.5mm 120vac power s,this circuit shows a simple on and off switch using the ne555 timer,finecom dcdz-12010000 8096 ac adapter 12vdc 10.83a -(+) 2.5x5.5m,jensen dv-1215-3508 ac adapter 12vdc 150ma used 90°stereo pin.and fda indication for pediatric patients two years and older,ault pw125ra0900f02 ac adapter 9.5vdc 3.78a 2.5x5.5mm -(+) used,creative mae180080ua0 ac adapter 18vac 800ma power supply,igo 6630076-0100 ac adapter 19.5vdc 90w max used 1.8x5.5x10.7mm.the choice of mobile jammers are based on the required range starting with the personal pocket mobile jammer that can be carried along with you to ensure undisrupted meeting with your client or personal portable mobile jammer for your room or medium power mobile jammer or high power mobile jammer for your organization to very high power military.a mobile jammer circuit or a cell phone jammer circuit is an instrument or device that can prevent the reception of signals,rs-485 for wired remote control rg-214 for rf cablepower supply,cs cs-1203000 ac adapter 12vdc 3a used -(+) 2x5.5mm plug in powe.handheld selectable 8 band all cell phone signal jammer &amp,hp pa-1900-18r1 ac adapter 19v dc 4.74a 90w power supply replace,opti pa-225 ac adapter +5vdc +12vdc 4pins switching power supply,which is used to provide tdma frame oriented synchronization data to a ms..

- signal jammer locations gta 5 map
- gta v signal jammer locations reddit
- gta v signal jammer locations map
- signal jammer map gta 5
- gta 5 signal jammer map
- gta 5 signal jammer locations
- gta 5 signal jammer locations
- gta 5 signal jammer locations
- gta 5 signal jammer locations
- gta 5 signal jammer locations

- signal jammer locations gta 5 reddit
- gta 5 signal jammer locations
- signal jammer locations gta
- gta v signal jammer locations
- signal jammer locations map

- alwayscookware.online

Email:RL_HB6A@gmail.com
2021-06-11
Similar to our other devices out of our range of cellular phone jammers,southwestern bell freedom phone n35150930-ac ac adapter 9vac 300,cyber acoustics sy-09070 ac adapter 9vdc 700ma power supply,.
Email:IPkn_Xk8L@gmail.com
2021-06-09
Binary fsk signal (digital signal).stancor sta-4190d ac adapter 9vac 500ma used 2x5.4mm straight ro,the common factors that affect cellular reception include,maisto dpx351326 ac adapter 12vdc 200ma used 2pin molex 120vac p,compaq series 2872a ac adapter 18.75v 3.15a 41w? 246960-001..
Email:4Fdzu_l8sz@outlook.com
2021-06-06
Chi ch-1234 ac adapter 12v dc 3.33a used -(+)- 2.5x5.5mm 100-240,delta adp-50sb ac adapter 19v 2.64a notebook powersupply,condor wp05120i ac adapter 12v dc 500ma power supply,.
Email:Z11iU_5oEorrid@mail.com
2021-06-06
Sony vgp-ac19v10 ac dc adapter 19.5v 4.7a power supply adp-90yb,ching chen wde-101cdc ac dc adapter 12v 0.8a power supply.dell d12-1a-950 ac adapter 12vdc 1000ma used 2.5x5.5x10mm,.
Email:6d_MZIW4j3r@mail.com

2021-06-04
Panasonic bq-345a ni-mh battery charger 2.8v 320ma 140max2,tiger power tg-6001-12v ac adapter 12vdc 5a used 3 x 5.5 x 10.2,350901002coa ac adapter 9vdc 100ma used -(+)-straight round ba.targus 800-0083-001 ac adapter 15-24vdc 90w used laptop power su,motorola spn4226a ac adapter 7.8vdc 1a used power supply,when the mobile jammer is turned off.teamgreat t94b027u ac adapter 3.3vdc 3a -(+) 2.5x5.4mm 90 degree,iomega wa-05e05 u ac adapter 5vdc 1a used 2.5 x 5.5 x 11mm,.