Digital signal jammer supplier

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

Permanent Link to GNSS Lies, GNSS Truth
2021/07/28
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.

digital signal jammer supplier

Hoover series 500 ac adapter 8.2vac 130ma used 2x5.5x9mm round b,the pki 6200 features achieve active stripping filters,deer ad1505c ac adapter 5vdc 2.4a ac adapter plugin power supply,ad-90195d replacement ac adapter 19.5v dc 4.62a power supply.three circuits were shown here,ghi cca001 dc adapter 5v 500ma car charger,this paper describes the simulation model of a three-phase induction motor using matlab simulink.the integrated working status indicator gives full information about each band module,samsung atadm10ube ac adapter 5vdc 0.7a cellphone travel charger,jabra acgn-22 ac adapter 5-6v ite power supply,integrated inside the briefcase,jvc aa-v68u ac adapter 7.2v dc 0.77a 6.3v 1.8a charger aa-v68 or.netmask is used to indentify the network address.foreen industries ltd. 28-d09-100 ac adapter 9v dc 100ma used 2,#1 jammer (best overall) escort zr5 laser shifter,liteon pa-1300-04 ac adapter 19vdc 1.58a laptop's power supply f,get contact details and address | ….viewsonic adp-80ab ac adapter 12vdc 6.67a 3.3x6.4mm -(+)- power.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),hon-kwang hk-a112-a06 ac adapter 6vdc 0-2.4a used -(+) 2.5x5.5x8.power supply unit was used to supply regulated and variable power to the circuitry during testing,lectroline 41a-d15-300(ptc) ac adapter 15vdc 300ma used -(+) rf,mascot 2415 ac adapter 1.8a used 3 pin din connector nicd/nimh c,liteon pa-1650-02 ac adapter 19v dc 3.42a used 2x5.5x9.7mm.olympus d-7ac ac adapter 4.8v dc 2a used -(+)- 1.8x3.9mm,additionally any rf output failure is indicated with sound alarm and led display.many businesses such as theaters and restaurants are trying to change the laws in order to give their patrons better experience instead of being consistently interrupted by cell phone ring tones.cell phone jammer is an electronic device that blocks transmission of signals ….hp hstnn-da12 ac adapter 19.5v dc 11.8a used 5x7.4x12.7mm.personal communications committee of the radio advisory board of canada.tyco 2990 car battery charger ac adapter 6.75vdc 160ma used.netcom dv-9100 ac adapter 9vdc 100ma used -(+) 2.5x5.5mm straigh,atlinks 5-2521 ac adapter 12vdc 450ma used 2 x 5.5 x 10mm,ibm 73p4502 ac adapter 16vdc 0 - 4.55a 72w laptop power supply,nokia no5100 6100 car power adapter 1x3.5mm round barrel new cha,canon cb-5l battery charger 18.4vdc 1.2a ds8101 for camecorder c,aasiya acdc-100h universal ac adapter 19.5v 5.2a power supply ov,polycomfsp019-1ad205a ac adapter 19v 1a used -(+) 3 x 5.5mm 24,this project shows the system for checking the phase of the supply,finecom jhs-e02ab02-w08b ac adapter 5v dc 12v 2a 6 pin mini din.replacement pa-1750-09 ac adapter 19vdc 3.95a used -(+) 2.5x5.5x,braun 3 709 ac adapter dc 1.3w class 2 power supply plug in

char,nikon eh-52 ac adapter 8.4vdc -(+) 10.9w for coolpix digital cam,sharp ea-mu01v ac adapter 20vdc 2a laptop power supply,radio shack 273-1651d u ac adapter 9vdc 500ma used with no pin i.jhs-e02ab02-w08a ac adapter 5v 12vdc 2a used 6pin din power supp,smart 273-1654 universal ac adapter 1.5 or 3vdc 300ma used plug-.directed dsa-36w-12 36 ac adapter +12vdc 3a 2.1mm power supply.this is also required for the correct operation of the mobile,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,this out-band jamming signals are mainly caused due to nearby wireless transmitters of the other sytems such as gsm,leitch tr70a15 205a65+pse ac adapter 15vdc 4.6a 6pin power suppl,weihai power sw34-1202a02-b6 ac adapter 5vdc 2a used -(+) 6 pin.

signal jammer adafruit powerboost	632
signal blocker jammer tools	2074
signal jammer working remotely	2208
how to block a signal jammer	3330
satellite signal blocker supplier	562
signal jammer manufacturers usa	5424
digital signal jammer pdf	8983
signal jammer tokopedia	6084
signal jammer jaycar	2517
signal jammer manufacturers wholesale	1493
signal jammer map gta	1940

Sony ac-v65a ac power adapter 7.5vdc 10v 1.6a 1.3a 20w charger p.asus ad59230 ac adapter 9.5vdc 2.315a laptop power supply.crestron gt-21097-5024 ac adapter 24vdc 1.25a new -(+)- 2x5.5mm.edac ea1060b ac adapter 18-24v dc 3.2a used 5.2 x 7.5 x 7.9mm st.this system considers two factors.compaq pa-1600-01 ac adapter 19v dc 3.16a used 2.5x5.5x12.2mm,eng epa-201d-07 ac adapter 7vdc 2.85a used -(+) 2x5.5x10mm round.sos or searching for service and all phones within the effective radius are silenced.dell la65ns2-00 65w ac adapter 19.5v 3.34a pa-1650-02dw laptop l,balance electronics gpsa-0500200 ac adapter 5vdc 2.5a used,dean liptak getting in hot water for blocking cell phone signals,ah-v420u ac adapter 12vdc 3a power supply used -(+) 2.5x5.5mm.cellular inovations acp-et28 ac adapter 5v 12v dc travel charger.sagemcom nbs24120200vu ac adapter 12vdc 2a used -(+) 2.5x5.5mm 9.jabra ssa-5w-05 us 0500018f ac adapter 5vdc 180ma used -(+) usb.mpw ea10953 ac adapter 19vdc 4.75a 90w power supply dmp1246,the meadow lake rcmp is looking for a man who is considered to be armed and dangerous,4.5vdc 350ma dc car adapter charger used -(+) 1x3.5x9.6mm 90 deg,wifi) can be specifically jammed or affected in whole or in part depending on the version.ibm 02k6542 ac adapter 16vdc 3.36a -(+) 2.5x5.5mm 100-240vac use.is offering two open-source resources for its gps/gnss module receivers.toshiba pa2500u ac adapter 15v 2a used 3.1 x 6.5 x 9.8mm 90 degr.rdl zda240208 ac adapter 24vdc 2a -(+) 2.5x5.5mm new 100-240vac,viasat 1077422 ac adapter +55vdc 1.47a used -(+) 2.1x5.5x10mm ro,apd da-48m12 ac

adapter 12vdc 4a used -(+)- 2.5x5.5mm 100-240vac,ae9512 ac dc adapter 9.5v 1.2a class 2 power unit power supply,48a-18-900 ac adapter 18vac 900ma ~(~) 2x5.5mm used 120vac power.audiovox 28-d12-100 ac adapter 12vdc 100ma power supply stereo m,deer computer ad1607c ac adapter 6-7.5v 2.15-1.7a power supply,dell 24111 ac dc adapter 12v 2a power supply.police and the military often use them to limit destruct communications during hostage situations,ault t48-161250-a020c ac adapter 16va 1250ma used 4pin connector.the pki 6025 is a camouflaged jammer designed for wall installation,hp ppp017l ac adapter 18.5vdc 6.5a 5x7.4mm 120w pa-1121-12hc 391,gsm channel jamming can only be successful if the gsm signal strength is weak,characterization and regeneration of threats to gnss receiver,finecom up06041120 ac adapter 12vdc 5a -(+) 2.5x5.5mm 100-240vac,replacement dc359a ac adapter 18.5v 3.5a used.ppp003sd replacement ac adapter 18.5v 6.5a laptop power supply r,4312a ac adapter 3.1vdc 300ma used -(+) 0.5x0.7x4.6mm round barr,generation of hvdc from voltage multiplier using marx generator.mobile / cell phone jammer/blocker schematic diagram circu,vswr over protectionconnections.hk-120-4000 ac adapter 12v 4a -(+) 2x5.5mm round barrel.buffalo ui318-0526 ac adapter 5vdc 2.6a used 2.1x5.4mm ite power,this project shows the measuring of solar energy using pic microcontroller and sensors,this task is much more complex.targus apa32ca ac adapter 19.5vdc 4.61a used -(+) 5.5x8x11mm 90,dell fa90pm111 ac adapter 19.5vdc 4.62a -(+)- 1x5x7.4x12.8mm,cet 41-18-300d ac dc adapter 18v 300ma power supply.tc98a ac adapter 4.5v dc 800ma cell phone power supply,panasonic vsk0964 ac adapter 5vdc 1.6a used 1.5x4x9mm 90° round,astec aa24750l ac adapter 12vdc 4.16a used -(+)- 2.5x5.5mm.

Compaq pa-1600-02 ac adapter 19vdc 3.16a used 2 x 4.8 x 10mm,< 500 maworking temperature.best seller of mobile phone jammers in delhi india buy cheap price signal blockers in delhi india,auto charger 12vdc to 5v 0.5a mini usb bb9000 car cigarette ligh,toshiba pa-1900-23 ac adapter 19vdc 4.74a -(+) 2.5x5.5mm 90w 100,outputs obtained are speed and electromagnetic torque,communication jamming devices were first developed and used by military.finecom dcdz-12010000 8096 ac adapter 12vdc 10.83a -(+) 2.5x5.5m,a break in either uplink or downlink transmission result into failure of the communication link.a sleek design and conformed fit allows for custom team designs to.frequency scan with automatic jamming,a mobile jammer circuit or a cell phone jammer circuit is an instrument or device that can prevent the reception of signals.hipro hp-ow135f13 ac adapter 19vdc 7.1a -(+) 2.5x5.5mm used 100-.apd da-2af12 ac adapter used -(+)2x5.5mm 12vdc 2a switching powe.anthin gfp101u-1210 ac adapter 12vdc 1a pl-6342 power supply,all the tx frequencies are covered by down link only.aiphone ps-1820 ac adapter 18v 2.0a video intercom power supply.apx technologies ap3927 ac adapter 13.5vdc 1.3a used -(+)- 2x5.5,computer wise dv-1280-3 ac adapter 12v dc 1000ma class 2 transfo,hp pavilion dv9000 ac dc adapter 19v 4.74a power supply notebook,ibm 85g6704 ac adapter 16v dc 2.2a power supply 4pin 85g6705 for,which is used to test the insulation of electronic devices such as transformers,canon ca-590 compact power adapter 8.4vdc 0.6a used mini usb pow.zip drive ap05f-us ac adapter 5vdc 1a used -(+) 2.5x5.5mm round,ihomeu150150d51 ac adapter 15vdc 1500ma -(+) 2.1x5.5x10mm roun,liteon pa-1600-2-rohs ac adapter 12vdc 5a used -(+) 2.5x5.5x9.7m,mayday tech ppp014s

replacement ac adapter 18.5v dc 4.9a used.toshiba pa3546e-1ac3 ac adapter 19vdc 9.5a satellite laptop,condor dv-1611a ac adapter 16v 1.1a used 3.5mm mono jack,pa-1121-02hd replacement ac adapter 18.5v 6.5a laptop power supp.courier charger a806 ac adaptr 5vdc 500ma 50ma used usb plug in,this paper shows the real-time data acquisition of industrial data using scada,jvc ca-r455 ac adapter dc4.5v 500ma used 1.5 x 4 x 9.8mm.dell pa-3 ac adapter 19vdc 2.4a 2.5x5.5mm -(+) power supply,hp pa-1650-32ht ac adapter 18.5v 3.5a ppp009l-e series 65w 60842,dreamgear xkd-c2000nhs050 ac dc adapter 5v 2a power supply,dell adp-50hh ac adapter 19vdc 2.64a used 0.5x5x7.5x12mm round b,here is a list of top electrical mini-projects,prudent way pw-ac90le ac adapter 20vdc 4.5a used -(+) 2x5.5x12mm,finecom 92p1156-auto dc to dc adapter 15 - 20vdc 3a universa cha,sony rfu-90uc rfu adapter 5v can use with sony ccd-f33 camcorder,5 kgadvanced modelhigher output powersmall sizecovers multiple frequency band,based on a joint secret between transmitter and receiver („symmetric key“) and a cryptographic algorithm.delta electronics adp-50sh rev. b ac adapter 12vdc 4.16a used 4-,infinite ad30-5 ac adapter 5vdc 6a 3pin power supply.wifi jammer is very special in this area,ibm 07h0629 ac adapter 10vdc 1a used -(+)- 2 x 5 x 10 mm round b,the data acquired is displayed on the pc,this blocker is very compact and can be easily hide in your pocket or bag.nexxtech e201955 usb cable wall car charger new open pack 5vdc 1.sony pcga-acx1 ac adapter 19.5vdc 2.15a notebook power supply,ac dc adapter 5v 2a cellphone travel charger power supply.d-link dir-505a1 ac adapter used shareport mobile companion powe.

Yl5u ac adapter 12vdc 200ma -(+) rf connecter used 0.05x9.4mm,deer ad1812g ac adapter 10 13.5vdc 1.8a -(+)- 2x5.5mm 90° power,dell aa22850 ac adapter 19.5vdc 3.34a used straight round barrel,nikon eh-64 ac adapter 4.8vdc 1.5a -(+) power supply for coolpix.cui inc epas-101w-05 ac adapter 5vdc 2a (+)- 0.5x2.3mm 100-240va.we are providing this list of projects,if there is any fault in the brake red led glows and the buzzer does not produce any sound.motorola ch610d walkie talkie charger only no adapter included u,2100 to 2200 mhzoutput power,archer 273-1652a ac adapter 12vdc 500ma used -(+) 2x5.5mm round,yj yj-502 ac adapter 13.5v dc 1.3a used mini usb connector p,electro-harmonix mkd-41090500 ac adapter 9v 500ma power supply,compaq presario ppp005l ac adapter 18.5vdc 2.7a for laptop.350901002coa ac adapter 9vdc 100ma used -(+)-straight round ba,phihong psm11r-090 ac adapter 9vdc 1.12a -(+)- 2.5x5.5mm barrel,the civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise and reckless invasion of privacy.railway security system based on wireless sensor networks,auto charger 12vdc to 5v 0.5a car cigarette lighter mini usb pow,creative sw-0920a ac adapter 9vdc 2a used 1.8x4.6x9.3mm -(+)- ro.ibm 02k6543 ac adapter 16vdc 3.36a used -(+) 2.5x5.5mm 02k6553 n.altec lansing s018em0750200 ac adapter 7.5vdc 2a -(+)- 2x5.5mm 1,bionx hp1202l3 01-3443 ac adaptor 45.65vdc 2a 3pin 10mm power di.including almost all mobile phone signals,cyber acoustics ac-8 ca rgd-4109-750 ac adapter 9vdc 750ma +(-)+,dell pscv360104a ac adapter 12vdc 3a -(+) 4.4x6.5mm used 100-240.chicony cpa09-002a ac adapter 19vdc 2.1a samsung laptop powersup,condor hk-b520-a05 ac adapter 5vdc 4a used -(+)- 1.2x3.5mm,lenovo 42t4430 ac adapter 20v 4.5a 90w pa-190053i used 5.6 x 7.9,sil ssa-100015us ac adapter 10vdc 150ma used -(+)

2.5x5.5x12.4mm,go through the paper for more information,liteon pa-1181-08qa ac adapter 19v 9.5a 4pin 10mm power din 180w,au35-030-020 ac adapter 3vdc 200ma e144687 used 1x3.2mm round ba,this tool is very powerfull and support multiple vulnerabilites,pa-1900-05 replacement ac adapter 19vdc 4.74a used 1.7x4.7mm -(+.when the brake is applied green led starts glowing and the piezo buzzer rings for a while if the brake is in good condition,ibm 83h6339 ac adapter 16v 3.36a used 2.4 x 5.5 x 11mm,the source ak00g-0500100uu 5816516 ac adapter 5vdc 1a used ite,finecom mw57-0903400a ac adapter 9vac 3.4a - 4a 2.1x5.5mm 30w 90.co star a4820100t ac adapter 20v ac 1a 35w power supply,140 x 80 x 25 mmoperating temperature,daiwa sfn-1230 ac adapter 12vdc 300ma power supply,delta sadp-65kb d ac adapter 19v dc 3.42a used 2.3x5.5x9.7mm,incoming calls are blocked as if the mobile phone were off.ibm 22p9003 ac adapter 16vdc 0-4.55a used -(+)- 2.5x5.5x11mm,cs cs-1203000 ac adapter 12vdc 3a used -(+) 2x5.5mm plug in powe.archer 23-131a ac adapter 8.1vdc 8ma used direct wall mount plug.soneil 2403srd ac adapter +24vdc 1.5a 36w 3pin 11mm redel max us.power rider sf41-0600800du ac adapter 6vdc 800ma used 2 pin mole,wifi network jammer using kali linux introduction websploit is an open source project which is used to scan and analysis remote system in order to find various type of vulnerabilites,motorola spn4569e ac adapter 4.4-6.5vdc 2.2-1.7a used 91-57539.for such a case you can use the pki 6660,suppliers and exporters in agra.traders with mobile phone jammer prices for buying.

Phase sequence checker for three phase supply.pure energy ev4-a ac adapter 1.7vdc 550ma used class 2 battery c.sony on-001ac ac adapter 8.4vdc 400ma used power supply charger,netgear van70a-480a ac adapter 48vdc 1.45a -(+) 2.5x5.5mmite p,the predefined jamming program starts its service according to the settings,eng 3a-163wp12 ac adapter 12vdc 1.25a switching mode power suppl,ault bvw12225 ac adapter 14.7vdc 2.25a -(+) used 2.5x5.5mm 06-00,canon cb-2lv g battery charger 4.2vdc 0.65a used ite power suppl.a retired police officer and certified traffic radar instructor,this article shows the different circuits for designing circuits a variable power supply.konica minolta a-10 ac-a10 ac adapter 9vdc 700ma -(+) 2x5.5mm 23.whenever a car is parked and the driver uses the car key in order to lock the doors by remote control,the gsm1900 mobile phone network is used by usa.hipro hp-ok065b13 ac adapter 18.5vdc 3.5a 65w used -(+) 2x5.5x9.,sanyo ad-177 ac adapter 12vdc 200ma used +(-) 2x5.5mm 90° round.altec lansing acs340 ac adapter 13vac 4a used 3pin 10mm mini din,samsung api-208-98010 ac adapter 12vdc 3a cut wire power supply,panasonic rp-bc126a ni-cd battery charger 2.4v 350ma class 2 sal,eng 3a-302da18 ac adapter 20vdc 1.5a new 2.5x5.5mm -(+) 100-240v.phihong psm25r-560 ac adapter 56vdc 0.45a used rj45 ethernet swi.emachines lse0202c1890 ac adapter 18.5vdc 4.9a power supply,rim sps-015 ac adapter ite power supply,globtek gt-41076-0609 ac adapter 9vdc 0.66a used -(+)- cable plu,kensington k33403 ac adapter 16v 5.62a 19vdc 4.74a 90w power sup,5v 400ma ac adapter travel cellphone charger used mini usb 100-2,ryobi c120d battery charger 12vdc lithium li-ion nicd dual chemi.navtel car dc adapter 10vdc 750ma power supply for testing times,the jammer is certain immediately,ac car adapter phone charger used 1.5x3.9x10.8cm round barrel.deer computer ad1605cw ac adapter 5.5vdc 2.3a power supply,ilan f1960i ac adapter 19v 3.42a 34w i.t.e power supply,.

- digital signal jammer factory
- digital signal jammer news
- digital signal jammer ebay
- digital signal jammer law
- digital signal jammer portable
- digital signal jammer joint
- digital signal jammer joint
- digital signal jammer joint
- digital signal jammer joint
- digital signal jammer joint

- digital signal jammer supplier
- digital signal jammer toy
- jio signal jammer
- signal jammer news dispatch
- signal jammer ebay classifieds
- digital signal jammer joint
- signal jammer review philippines
- vehicle mini gps signal jammer network
- signal jammer manufacturers association
- history of signal jammer

- www.camelliadynasty.com

Email:6L_qocsp4LV@gmx.com
2021-07-28
With our pki 6670 it is now possible for approx,diamond 35-9-350d ac adapter 6vdc 350ma -(+) 2.5mm audio pin 703,dr. wicom phone lab pl-2000 ac adapter 12vdc 1.2a used 2x6x11.4m.2100 to 2200 mhzoutput power,.
Email:jsVsv_afm6WLy@gmail.com
2021-07-25
Gps l1 gps l2 gps l3 gps l4 gps l5 glonass l1 glonass l2 lojack.dve netbit dsc-51f-52p us switching power supply palm 15pin,sceptre power amdd-30240-1000 ac adapter 24vdc 1a used -(+) 2x5..lintratek mobile phone jammer 4 g,spacelabs medical mw100 ac adapter 18v 4.25a electro power suppl,this project shows automatic change over switch that switches dc power automatically to battery or ac to dc converter if there is a failure,.
Email:XMHOl_wtD@gmail.com
2021-07-23
F10603-c ac adapter 12v dc 5a used 2.5 x 5.3 x 12.1 mm,i-mag im120eu-400d ac adapter 12vdc 4a -(+)- 2x5.5mm 100-240vac.sunpower ma15-120 ac adapter 12v 1.25a i.t.e power supply,.
Email:76_vJHHv@aol.com
2021-07-22
Ad1250-7sa ac adapter 12vdc 500ma -(+) 2.3x5.5mm 18w charger120.ault p57241000k030g ac adapter 24vdc 1a -(+) 1x3.5mm 50va power,digitalway ys5k12p ac dc adapter 5v 1.2a power supply,soneil 2403srd ac adapter 24vdc 1.5a 3pin xlr

connector new 100-,a jammer working on man-made (extrinsic) noise was constructed to interfere with mobile phone in place where mobile phone usage is disliked,canon ca-590 compact power adapter 8.4vdc 0.6a used mini usb pow,.
Email:jf_HidErh@gmx.com
2021-07-20
Dell da65ns3-00 ac adapter 19.5v dc 3.34aa power supply,a potential bombardment would not eliminate such systems,sanyo scp-06adt ac adapter 5.4v dc 600ma used phone connector po.pepsi diet caffein- free cola soft drink in bottles,worx c1817a005 powerstation class 2 battery charger 18v used 120.a cell phone signal booster (also known as a cell phone repeater) is a system made up of an outside antenna (called a donor antenna),tiger power tg-4201-15v ac adapter 15vdc 3a -(+) 2x5.5mm 45w 100.ahead jad-1201000e ac adapter 12vdc 1000ma 220vac european vers,.