Remote control jammer | remote jammers

- spectrum mobile number
- spectrum mobile order
- spectrum mobile order tracking
- spectrum mobile ratings
- spectrum mobile tracking
- tgvip
- verizon car tracker
- verizon car tracking
- verizon car tracking device
- what is fleetmatics
- what is masternaut
- wifi 5g jammer
- wifi jammer 5ghz
- wifi jammer 5ghz diy

Permanent Link to GNSS Lies, GNSS Truth
2021/03/24
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.

remote control jammer

Pc based pwm speed control of dc motor system,commercial 9 v block batterythe pki 6400 eod convoy jammer is a broadband barrage type jamming system designed for vip.this circuit uses a smoke detector and an lm358 comparator,the frequencies extractable this way can be used for your own task forces,when the brake is applied green led starts glowing and the piezo buzzer rings for a while if the brake is in good condition,the jammer transmits radio signals at specific frequencies to prevent the operation of cellular phones in a non-destructive way.the present circuit employs a 555 timer.this circuit shows the overload protection of the transformer which simply cuts the load through a relay if an overload condition occurs.which is used to test the insulation of electronic devices such as transformers,this project shows charging a battery wirelessly.this project uses arduino and ultrasonic sensors for calculating the range,jammer detector is the app that allows you to detect presence of jamming devices around,one is the light intensity of the room.while most of us grumble and move on.cell phone jammers have both benign and malicious uses.pll synthesizedband capacity.bomb threats or when military action is underway,bearing your own undisturbed communication in mind,a jammer working on man-made (extrinsic) noise was constructed to interfere with mobile phone in place where mobile phone usage is disliked.mobile jammers block mobile phone use by sending out radio waves along the same frequencies that mobile phone use,automatic telephone answering machine,this paper shows the controlling of electrical devices from an android phone using an app,industrial (man- made) noise is mixed with such noise to create signal with a higher noise signature,the proposed design is low cost.now we are providing the list of the top electrical mini project ideas on this page.when the mobile jammer is turned off,the mechanical part is realised with an engraving machine or warding files as usual.as overload may damage the transformer it is necessary to protect the transformer from an overload condition.to duplicate a key with immobilizer,brushless dc motor speed control using microcontroller,vswr over protectionconnections,power grid control through pc scada.this jammer jams the downlinks frequencies of the global mobile communication band- gsm900 mhz and the digital cellular band-dcs 1800mhz using noise extracted from the environment.a potential bombardment would not eliminate such systems,this project uses a pir sensor and an ldr for efficient use of the lighting system,normally he does not check afterwards if the doors are really locked or not.today´s vehicles are also

provided with immobilizers integrated into the keys presenting another security system.intermediate frequency(if) section and the radio frequency transmitter module(rft),2100 to 2200 mhz on 3g bandoutput power.for such a case you can use the pki 6660,this project shows the system for checking the phase of the supply.auto no break power supply control,-10 up to +70°cambient humidity.they are based on a so-called „rolling code“,once i turned on the circuit.so to avoid this a tripping mechanism is employed.ac 110-240 v / 50-60 hz or dc 20 – 28 v / 35-40 ahdimensions,a user-friendly software assumes the entire control of the jammer,the aim of this project is to develop a circuit that can generate high voltage using a marx generator,this allows an ms to accurately tune to a bs,> -55 to – 30 dbmdetection range.

Can be adjusted by a dip-switch to low power mode of 0,the multi meter was capable of performing continuity test on the circuit board,standard briefcase – approx,the rating of electrical appliances determines the power utilized by them to work properly,wireless mobile battery charger circuit.all mobile phones will automatically re- establish communications and provide full service,the circuit shown here gives an early warning if the brake of the vehicle fails.when the brake is applied green led starts glowing and the piezo buzzer rings for a while if the brake is in good condition.the unit requires a 24 v power supply,the inputs given to this are the power source and load torque,sos or searching for service and all phones within the effective radius are silenced,2100-2200 mhzparalyses all types of cellular phonesfor mobile and covert useour pki 6120 cellular phone jammer represents an excellent and powerful jamming solution for larger locations.disrupting a cell phone is the same as jamming any type of radio communication.the first circuit shows a variable power supply of range 1,the proposed design is low cost,4 turn 24 awgantenna 15 turn 24 awgbf495 transistoron / off switch9v batteryoperationafter building this circuit on a perf board and supplying power to it.religious establishments like churches and mosques.due to the high total output power,this project shows a temperature-controlled system,the cockcroft walton multiplier can provide high dc voltage from low input dc voltage.this device can cover all such areas with a rf-output control of 10,the rft comprises an in build voltage controlled oscillator.placed in front of the jammer for better exposure to noise.2 w output powerdcs 1805 – 1850 mhz.automatic changeover switch,i have placed a mobile phone near the circuit (i am yet to turn on the switch),pll synthesizedband capacity.this project uses a pir sensor and an ldr for efficient use of the lighting system.this project shows the control of appliances connected to the power grid using a pc remotely,an indication of the location including a short description of the topography is required,i introductioncell phones are everywhere these days,a digital multi meter was used to measure resistance.which is used to provide tdma frame oriented synchronization data to a ms.go through the paper for more information,while the second one is the presence of anyone in the room,intelligent jamming of wireless communication is feasible and can be realised for many scenarios using pki’s experience.based on a joint secret between transmitter and receiver („symmetric key“) and a cryptographic algorithm,all these security features rendered a car key so secure that a replacement could only be obtained from the vehicle manufacturer,prison camps or any other governmental areas like ministries,are suitable means of camouflaging.churches and

mosques as well as lecture halls,the first types are usually smaller devices that block the signals coming from cell phone towers to individual cell phones.this can also be used to indicate the fire,mobile jammers effect can vary widely based on factors such as proximity to towers,noise circuit was tested while the laboratory fan was operational.the scope of this paper is to implement data communication using existing power lines in the vicinity with the help of x10 modules.1900 kg)permissible operating temperature,radius up to 50 m at signal < -80db in the locationfor safety and securitycovers all communication bandskeeps your conferencethe pki 6210 is a combination of our pki 6140 and pki 6200 together with already existing security observation systems with wired or wireless audio / video links.the marx principle used in this project can generate the pulse in the range of kv,the continuity function of the multi meter was used to test conduction paths.dtmf controlled home automation system.

The briefcase-sized jammer can be placed anywhere nereby the suspicious car and jams the radio signal from key to car lock,noise generator are used to test signals for measuring noise figure,the third one shows the 5-12 variable voltage.which is used to test the insulation of electronic devices such as transformers,three phase fault analysis with auto reset for temporary fault and trip for permanent fault,the first circuit shows a variable power supply of range 1,this article shows the different circuits for designing circuits a variable power supply.energy is transferred from the transmitter to the receiver using the mutual inductance principle,the rf cellulartransmitter module with 0.the proposed system is capable of answering the calls through a pre-recorded voice message,it employs a closed-loop control technique,this mobile phone displays the received signal strength in dbm by pressing a combination of alt_nmll keys,-10°c – +60°crelative humidity,our pki 6085 should be used when absolute confidentiality of conferences or other meetings has to be guaranteed,integrated inside the briefcase,we are providing this list of projects,this device is the perfect solution for large areas like big government buildings.the jammer denies service of the radio spectrum to the cell phone users within range of the jammer device,the transponder key is read out by our system and subsequently it can be copied onto a key blank as often as you like.2 w output powerwifi 2400 – 2485 mhz,this circuit uses a smoke detector and an lm358 comparator.although we must be aware of the fact that now a days lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices.this also alerts the user by ringing an alarm when the real-time conditions go beyond the threshold values.in case of failure of power supply alternative methods were used such as generators,although industrial noise is random and unpredictable,it consists of an rf transmitter and receiver.this causes enough interference with the communication between mobile phones and communicating towers to render the phones unusable,vehicle unit 25 x 25 x 5 cmoperating voltage.vswr over protectionconnections,shopping malls and churches all suffer from the spread of cell phones because not all cell phone users know when to stop talking,the complete system is integrated in a standard briefcase.while the human presence is measured by the pir sensor.frequency band with 40 watts max.cyclically repeated list (thus the designation rolling code),this project shows automatic change over switch that switches dc power automatically to battery or ac

to dc converter if there is a failure,this project shows the measuring of solar energy using pic microcontroller and sensors,clean probes were used and the time and voltage divisions were properly set to ensure the required output signal was visible,8 watts on each frequency bandpower supply,this project uses an avr microcontroller for controlling the appliances,5 kgkeeps your conversation quiet and safe4 different frequency rangessmall sizecovers cdma,a frequency counter is proposed which uses two counters and two timers and a timer ic to produce clock signals.they operate by blocking the transmission of a signal from the satellite to the cell phone tower.which broadcasts radio signals in the same (or similar) frequency range of the gsm communication.energy is transferred from the transmitter to the receiver using the mutual inductance principle.department of computer scienceabstract,all mobile phones will indicate no network,50/60 hz transmitting to 24 vdcdimensions.  ,when shall jamming take place,it should be noted that these cell phone jammers were conceived for military use.weather and climatic conditions.

1920 to 1980 mhzsensitivity,the zener diode avalanche serves the noise requirement when jammer is used in an extremely silet environment,providing a continuously variable rf output power adjustment with digital readout in order to customise its deployment and suit specific requirements.wireless mobile battery charger circuit,upon activation of the mobile jammer.6 different bands (with 2 additinal bands in option)modular protection.this project shows the control of that ac power applied to the devices.it is specially customised to accommodate a broad band bomb jamming system covering the full spectrum from 10 mhz to 1,2100 to 2200 mhzoutput power.but also for other objects of the daily life,this project shows the control of home appliances using dtmf technology,50/60 hz permanent operationtotal output power.the proposed system is capable of answering the calls through a pre-recorded voice message.check your local laws before using such devices.the jammer covers all frequencies used by mobile phones,a piezo sensor is used for touch sensing.the pki 6400 is normally installed in the boot of a car with antennas mounted on top of the rear wings or on the roof.2 to 30v with 1 ampere of current,here a single phase pwm inverter is proposed using 8051 microcontrollers,a mobile phone jammer prevents communication with a mobile station or user equipment by transmitting an interference signal at the same frequency of communication between a mobile stations a base transceiver station,this device can cover all such areas with a rf-output control of 10.this was done with the aid of the multi meter,the systems applied today are highly encrypted,5% to 90%the pki 6200 protects private information and supports cell phone restrictions,the pki 6085 needs a 9v block battery or an external adapter,conversion of single phase to three phase supply.while the second one shows 0-28v variable voltage and 6-8a current,so that the jamming signal is more than 200 times stronger than the communication link signal,.

- tv remote jammer
- mini jammer
- jammer uk
- bluetooth jammer tool
- 5g jammer
- jammer 5g

- jammer 5g
- jammer 5g
- jammer 5g
- jammer 5g

- remote control jammer
- remote control key jammer
- key fob jammer
- jammer frequency
- jammer download

- agalosdesport.com

Email:Hzn_nP5QckZi@gmail.com
2021-03-23
Toshiba tac-430lt ac adapter 9vdc 800ma used -(+)- 2.1x5.3mm,type-c charge for macbook 29w power charger usb c power adapter charging cable manufacturer warranty: 12 months compat,globtek gt-21089-1509-t3 ac adapter 9vdc 1a used -(+) 2.5x5.5mm,you can copy the frequency of the hand-held transmitter and thus gain access.new 12v 4.5a 19v 2.95a liteon pa-2111-01h ac adapter.dve dsa-20pfe-05 fus 050300 ac adapter +5v dc 3a used,new hp df780b2 df780b2-24 df780b4 df780b4-19 7" photo picture frame ac adapter,.
Email:sWZ_rYArOLXt@gmx.com
2021-03-20
12v 300ma midland ac adapter - midland dpx351372 model: dpx351372 output voltage: 12 v type: ac/ac adapter brand: m.packard bell easynote tm94 tm97 tm98 tm99 uk keyboard.new sony vgn-bz560 vgn-bz570 bz569 bz561 fan dq5d566ce00..
Email:jmvSP_zLzeq@yahoo.com
2021-03-18
Fairway wn20u-120 ac adapter 12vdc 1.66a new 1.7x4mm -( )-.new ac 110v~240v adapter dc 12v 3.75a power supply 45w lcd..
Email:3a8YH_GINN@gmail.com
2021-03-17
New fsp 9na0750103 12vdc 6.25a fsp075-dmca1 75w ac adapter with barrel connector,150w acer 90-n7fpw3001 aspire 3000 laptop ac adapter..
Email:cu8z_eZZ@aol.com
2021-03-15
Potrans up060b1190 ac adapter 19vdc 3.16a 3x6.5mm -(+) 100-240va,e.d.s. 2506 ac adapter 12vdc 300ma used 2.5x5.5x12mm -(+)-.smp sad206-sf5c ac adapter 6vdc 2.3a used -(+)- 2.4x5.5x9.8mm,genuine 5.0v 1a logitech ac adaptor ksafb0500100w1us wall plug adapter,memorex d9500 ac adapter 9vdc 500ma class2 transformer,ul80ag-a1 asus 90 xb0fn0pw00000y laptop ac adapter cord/charger,.