SCIENCE & TECHNOLOGY RESEARCH INSTITUTE
FOR DEFENCE
MINISTRY OF DEFENCE

STRIDE

Global Positioning System (GPS) Receiver Evaluation Using GPS Simulation

STRIDE

Introduction

GNSS systems:

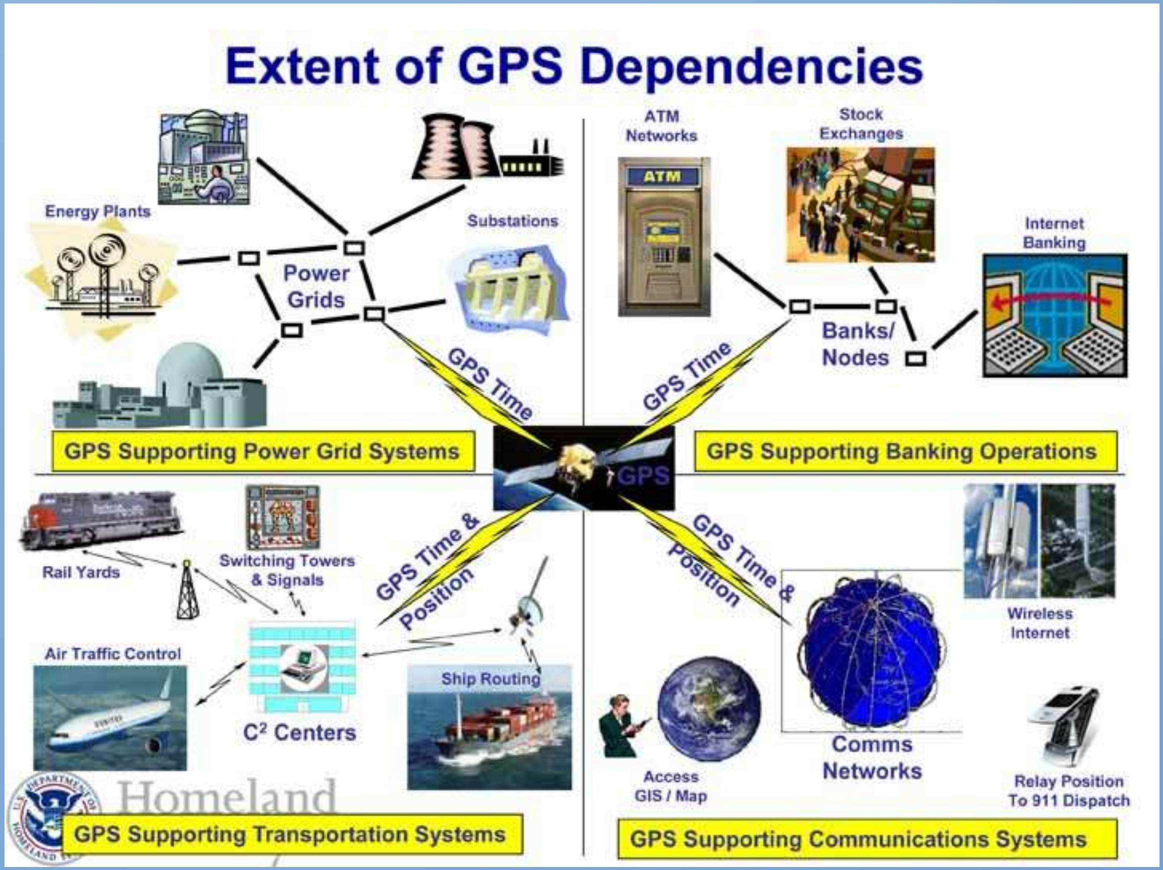
- GPS
  - FOC: April 1995
- GLONASS
  - FOC:
    - January 1996
    - System degradation
    - December 2011
- BeiDou
  - Partially operational (regional stage)
  - FOC: 2020
- Galileo
  - FOC: 2020

FOC: Full operational capability

Introduction

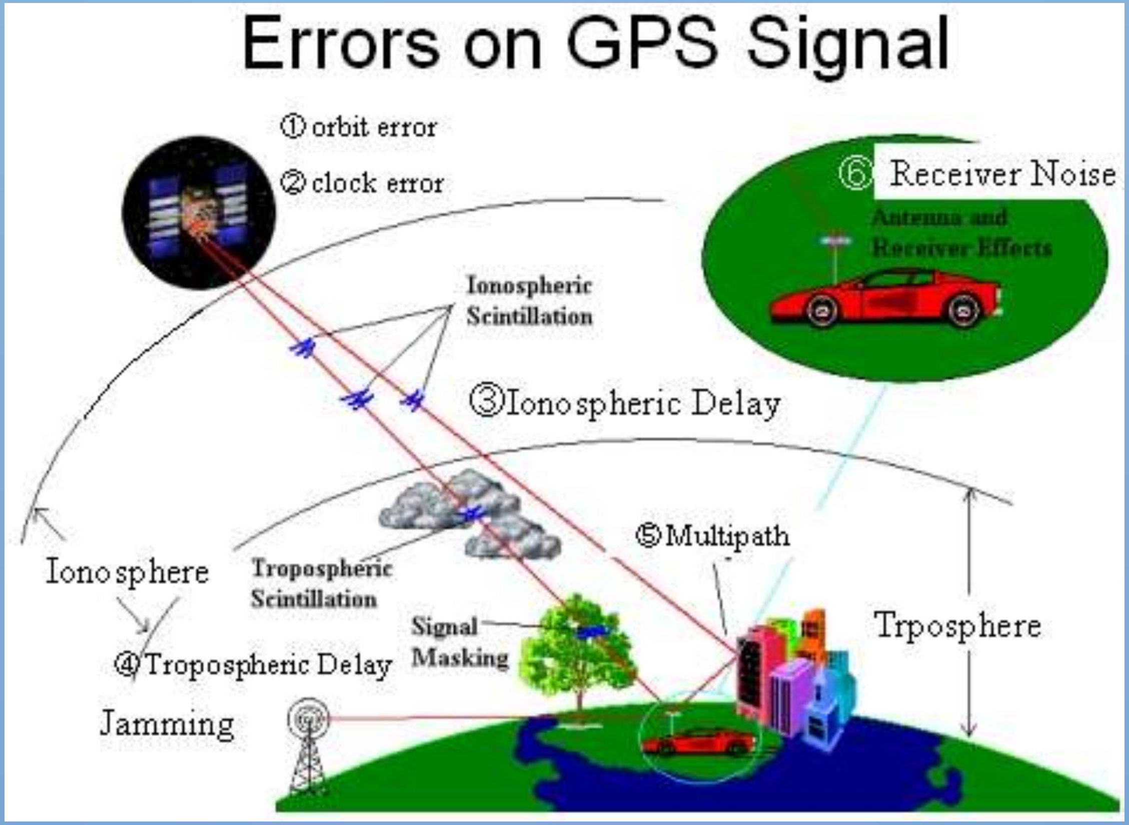
Increasing use for PNT applications:

- ♦Positioning
- ♦Navigation
- ♦Timing



STRIDE

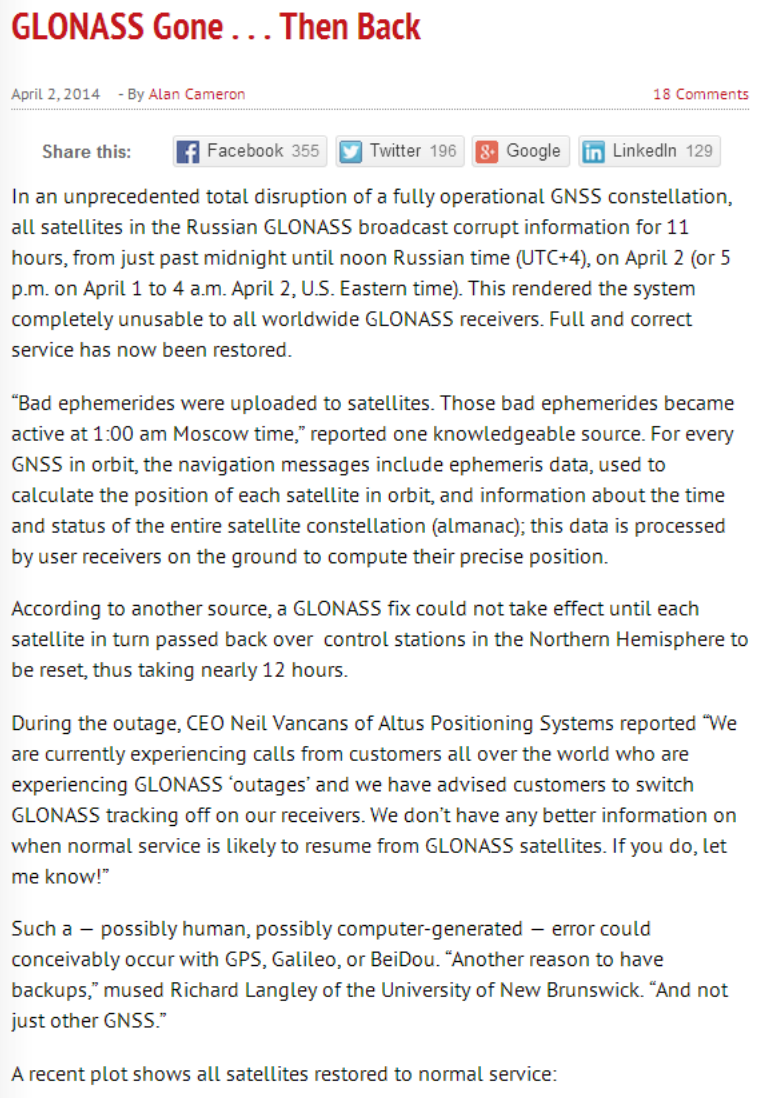
GNSS Vulnerabilities



Source: IranMap.com

STRIDE

GNSS Vulnerabilities



GLONASS Gone . . . Then Back

April 2, 2014 - By Alan Cameron 18 Comments

Share this: Facebook 355 Twitter 196 Google LinkedIn 129

In an unprecedented total disruption of a fully operational GNSS constellation, all satellites in the Russian GLONASS broadcast corrupt information for 11 hours, from just past midnight until noon Russian time (UTC+4), on April 2 (or 5 p.m. on April 1 to 4 a.m. April 2, U.S. Eastern time). This rendered the system completely unusable to all worldwide GLONASS receivers. Full and correct service has now been restored.

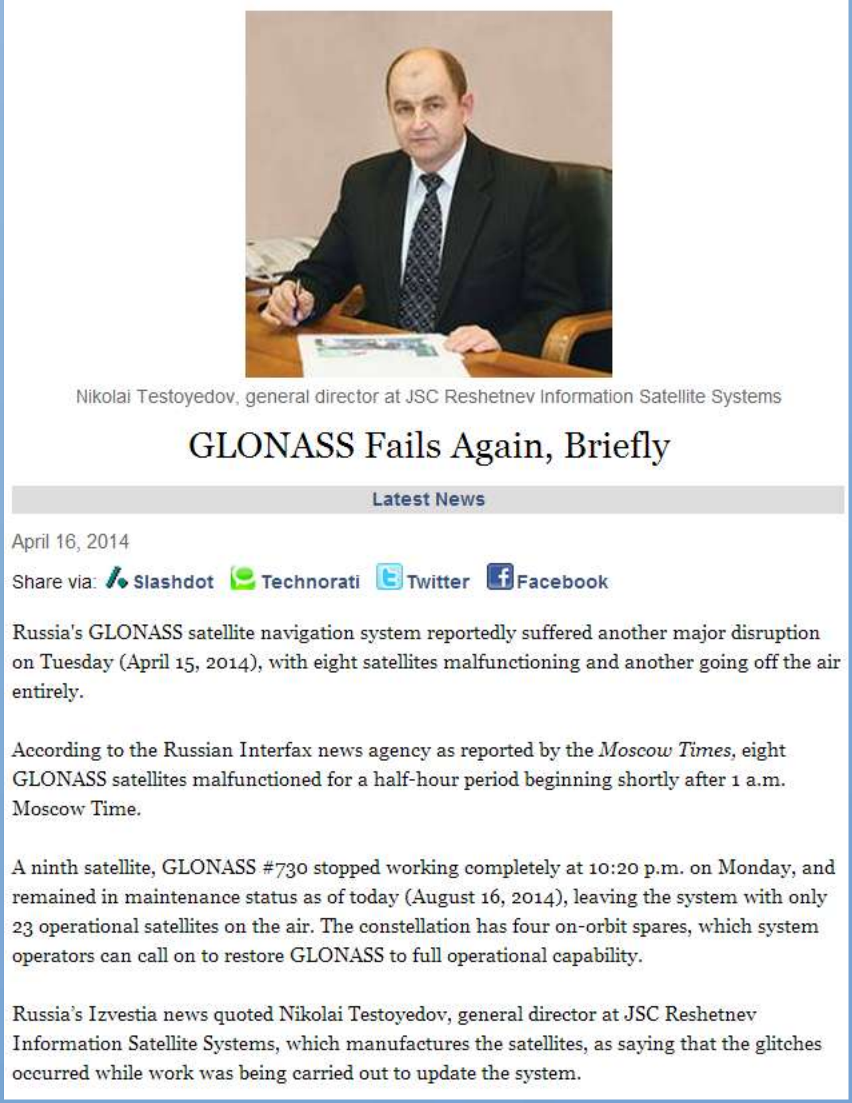
"Bad ephemerides were uploaded to satellites. Those bad ephemerides became active at 1:00 am Moscow time," reported one knowledgeable source. For every GNSS in orbit, the navigation messages include ephemeris data, used to calculate the position of each satellite in orbit, and information about the time and status of the entire satellite constellation (almanac); this data is processed by user receivers on the ground to compute their precise position.

According to another source, a GLONASS fix could not take effect until each satellite in turn passed back over control stations in the Northern Hemisphere to be reset, thus taking nearly 12 hours.

During the outage, CEO Neil Vancans of Altus Positioning Systems reported "We are currently experiencing calls from customers all over the world who are experiencing GLONASS 'outages' and we have advised customers to switch GLONASS tracking off on our receivers. We don't have any better information on when normal service is likely to resume from GLONASS satellites. If you do, let me know!"

Such a — possibly human, possibly computer-generated — error could conceivably occur with GPS, Galileo, or BeiDou. "Another reason to have backups," mused Richard Langley of the University of New Brunswick. "And not just other GNSS."

A recent plot shows all satellites restored to normal service:



Nikolai Testoyedov, general director at JSC Reshetnev Information Satellite Systems

GLONASS Fails Again, Briefly

Latest News

April 16, 2014

Share via: Slashdot Technorati Twitter Facebook

Russia's GLONASS satellite navigation system reportedly suffered another major disruption on Tuesday (April 15, 2014), with eight satellites malfunctioning and another going off the air entirely.

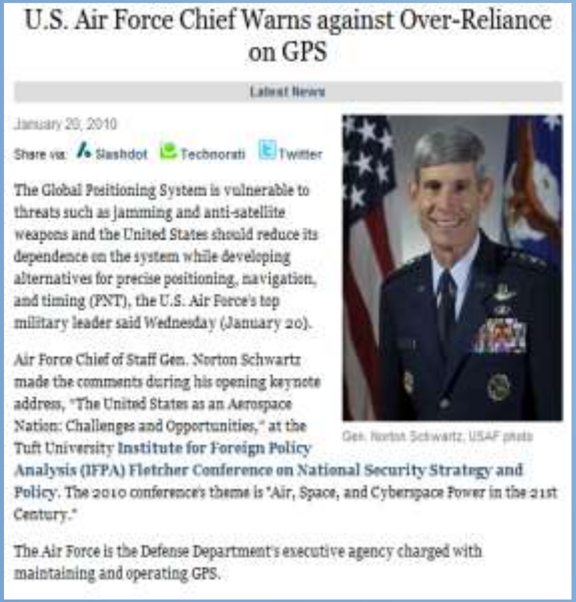
According to the Russian Interfax news agency as reported by the *Moscow Times*, eight GLONASS satellites malfunctioned for a half-hour period beginning shortly after 1 a.m. Moscow Time.

A ninth satellite, GLONASS #730 stopped working completely at 10:20 p.m. on Monday, and remained in maintenance status as of today (August 16, 2014), leaving the system with only 23 operational satellites on the air. The constellation has four on-orbit spares, which system operators can call on to restore GLONASS to full operational capability.

Russia's Izvestia news quoted Nikolai Testoyedov, general director at JSC Reshetnev Information Satellite Systems, which manufactures the satellites, as saying that the glitches occurred while work was being carried out to update the system.

STRIDE

GNSS Vulnerabilities



U.S. Air Force Chief Warns against Over-Reliance on GPS

Latest News

January 20, 2010

Share via: Slashdot Technorati Twitter

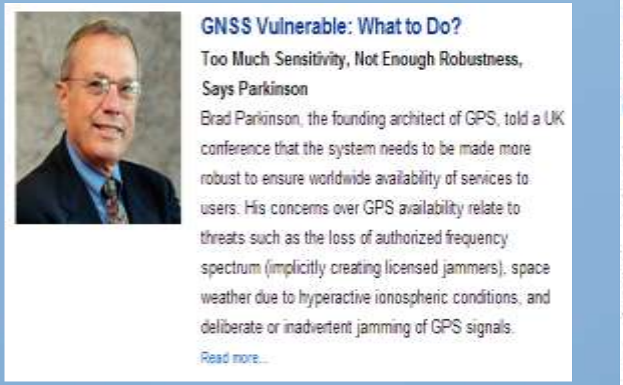
The Global Positioning System is vulnerable to threats such as jamming and anti-satellite weapons and the United States should reduce its dependence on the system while developing alternatives for precise positioning, navigation, and timing (PNT), the U.S. Air Force's top military leader said Wednesday (January 20).

Gen. Norton Schwartz, USAF photo

Air Force Chief of Staff Gen. Norton Schwartz made the comments during his opening keynote address, "The United States as an Aerospace Nation: Challenges and Opportunities," at the Tuft University Institute for Foreign Policy Analysis (IFPA) Fletcher Conference on National Security Strategy and Policy. The 2010 conference's theme is "Air, Space, and Cyberspace Power in the 21st Century."

The Air Force is the Defense Department's executive agency charged with maintaining and operating GPS.

"Another widely-known dependence that creates an exploitable vulnerability is that of GPS. It seems critical to me that the Joint Force should reduce its dependence on GPS-aided precision navigation and timing, allowing it to ultimately become less vulnerable, yet equally precise, and more resilient. The global value of GPS will endure, but our forces must be able to operate in GPS-denied environments in the future”



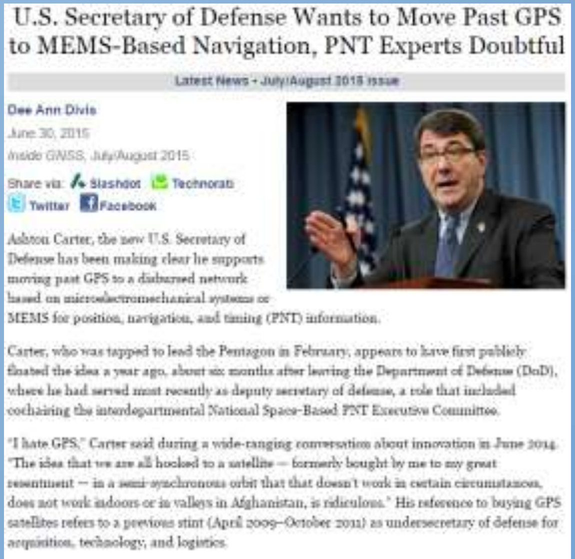
GNSS Vulnerable: What to Do?

Too Much Sensitivity, Not Enough Robustness, Says Parkinson

Brad Parkinson, the founding architect of GPS, told a UK conference that the system needs to be made more robust to ensure worldwide availability of services to users. His concerns over GPS availability relate to threats such as the loss of authorized frequency spectrum (implicitly creating licensed jammers), space weather due to hyperactive ionospheric conditions, and deliberate or inadvertent jamming of GPS signals.

Read more...

“His concerns over GPS availability relate to threats such as the loss of authorized frequency spectrum (implicitly creating licensed jammers), space weather due to hyperactive ionospheric conditions, and deliberate or inadvertent jamming of GPS signals. He warned that GPS is more vulnerable to sabotage or disruption than ever before.”



U.S. Secretary of Defense Wants to Move Past GPS to MEMS-Based Navigation, PNT Experts Doubtful

Latest News • July/August 2015 issue

Dee Ann Divis

June 30, 2015

Inside GNSS, July/August 2015

Share via: Slashdot Technorati Twitter Facebook

Ashton Carter, the new U.S. Secretary of Defense has been making clear he supports moving past GPS to a disbursed network based on microelectromechanical systems or MEMS for position, navigation, and timing (PNT) information.

Carter, who was tapped to lead the Pentagon in February, appears to have first publicly floated the idea a year ago, about six months after leaving the Department of Defense (DoD), where he had served most recently as deputy secretary of defense, a role that included cochairing the interdepartmental National Space-Based PNT Executive Committee.

"I hate GPS," Carter said during a wide-ranging conversation about innovation in June 2014. "The idea that we are all hooked to a satellite — formerly bought by me to my great resentment — in a semi-synchronous orbit that that doesn't work in certain circumstances, does not work indoors or in valleys in Afghanistan, is ridiculous." His reference to buying GPS satellites refers to a previous stint (April 2009–October 2011) as undersecretary of defense for acquisition, technology, and logistics.

“I hate GPS. The idea that we are all hooked to a satellite — formerly bought by me to my great resentment — in a semi-synchronous orbit that that doesn’t work in certain circumstances, does not work indoors or in valleys in Afghanistan, is ridiculous.”

STRIDE

GNSS Receiver Evaluation

- Many designers are working on improving characteristics of GNSS receivers, such as:
  - Lower power consumption
  - Tracking of weak satellite signals
  - Acquisition time
  - Positioning and timing accuracy
  - Radio frequency interference (RFI) interoperability
- Many developers and users still struggle to identify suitable standard tests to objectively verify and evaluate the functionality and performance of GNSS receivers.

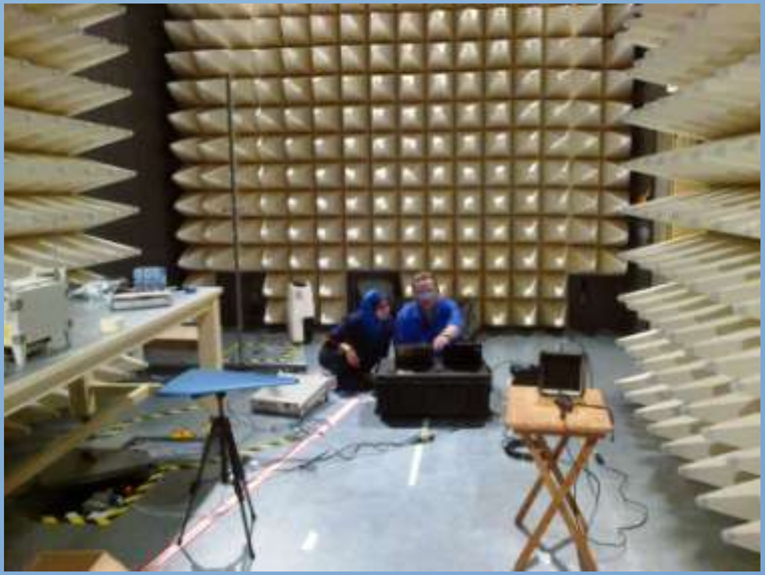
STRIDE

GNSS Receiver Evaluation

Field Evaluation

- Employs live GNSS signals.
- Should be conducted in open area with clear view of the sky.
- Tests scenarios are uncontrollable by users and not repeatable.

GNSS Simulation



- Employs simulated GNSS signals.
- Should be conducted in a RF enclosure (e.g. anechoic chamber).
- Test scenarios are user controllable and repeatable.

Research Theme

Title: Simulation and Modelling of Global
Navigation Satellite System (GNSS)
Vulnerabilities

Research Objectives:

- GNSS simulation will be used to model the effect of the following vulnerabilities on GNSS receiver performances:
  - Radio frequency interference (RFI)
  - Spoofing
  - Ionospheric and tropospheric delays
  - LOS blockage and multipath errors

STRIDE

R&D Projects Conducted

Num.	Project Title	Status	Duration
1	Evaluation of the Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Signals	Internal	November 2009 – June 2010
2	Evaluation of the Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Signals via GPS Simulation	RMK10	January 2011 – May 2012
3	Evaluation of the Effect of Multipath on Global Positioning System (GPS) Signals via GPS Simulation	Internal	January 2013 – January 2014
4	Evaluation of the Effect of Global Positioning System (GPS) Satellite Clock Error via GPS Simulation	Internal	April – September 2014
5	Evaluation of Trade-Off Between Global Positioning System (GPS) Accuracy and Power Saving from Reduction of Number of GPS Receiver Channels	Internal	November 2014 – March 2015
6	Evaluation of the Accuracy of Global Positioning System (GPS) Speed Measurement via GPS Simulation	Internal	May – August 2015
7	Simulation and Modelling of Global Navigation Satellite System (GNSS) Vulnerabilities	Proposed for RMK11	January 2016 – December 2019

STRIDE

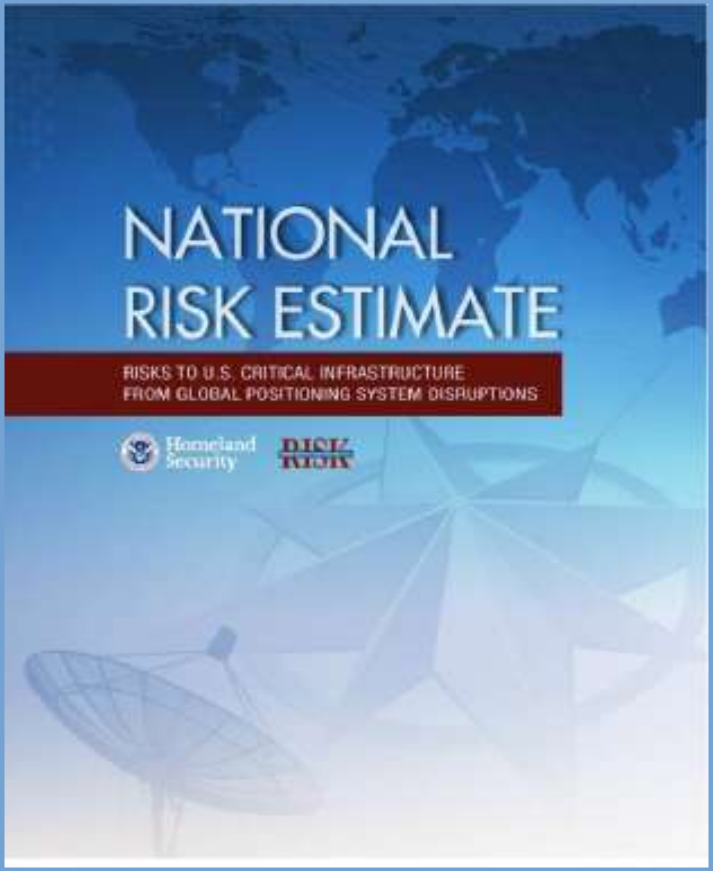
Presentation Outline

- Review of activities conducted on vulnerabilities of GPS to:
  - Radio frequency interference (RFI)
  - Simplistic spoofing
  - Static multipath
  - GPS satellite clock error
  - Power consumption
  - Speed measurement

- Future research direction (RMK11):
  - Intermediate spoofing
  - Dynamic multipath
  - Ionospheric and troposheric delays
  - Extension to other GNSS systems; GLONASS, BeiDou and Galileo

STRIDE

GNSS Jamming & Spoofing



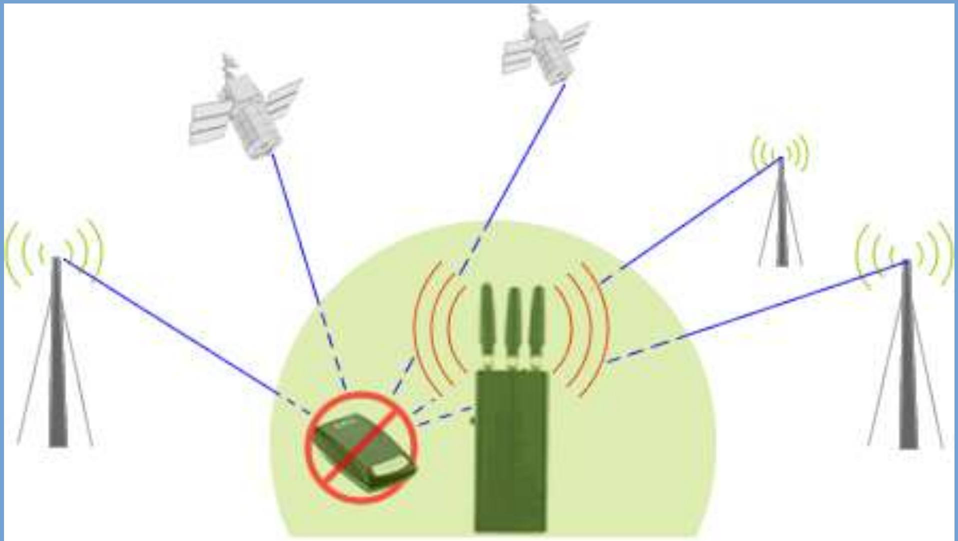
NATIONAL RISK ESTIMATE

RISKS TO U.S. CRITICAL INFRASTRUCTURE FROM GLOBAL POSITIONING SYSTEM DISRUPTIONS

Jamming disruptions are more likely than spoofing incidents - but the latter are of " higher consequence“.

GNSS Jamming

- Jamming: Broadcasting of a strong signal that overrides or obscures the signal being jammed
- GNSS signals that reach the Earth have very low power (10^{-16} – 10^{-13} W = -160 – -130 dBm)
- Renders them highly susceptible to jamming.



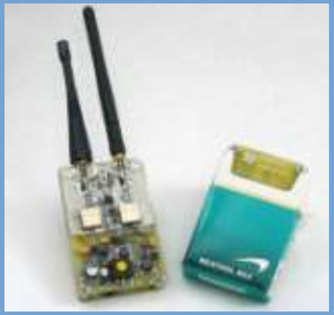
STRIDE

GNSS Jamming

Unintentional (Accidental)

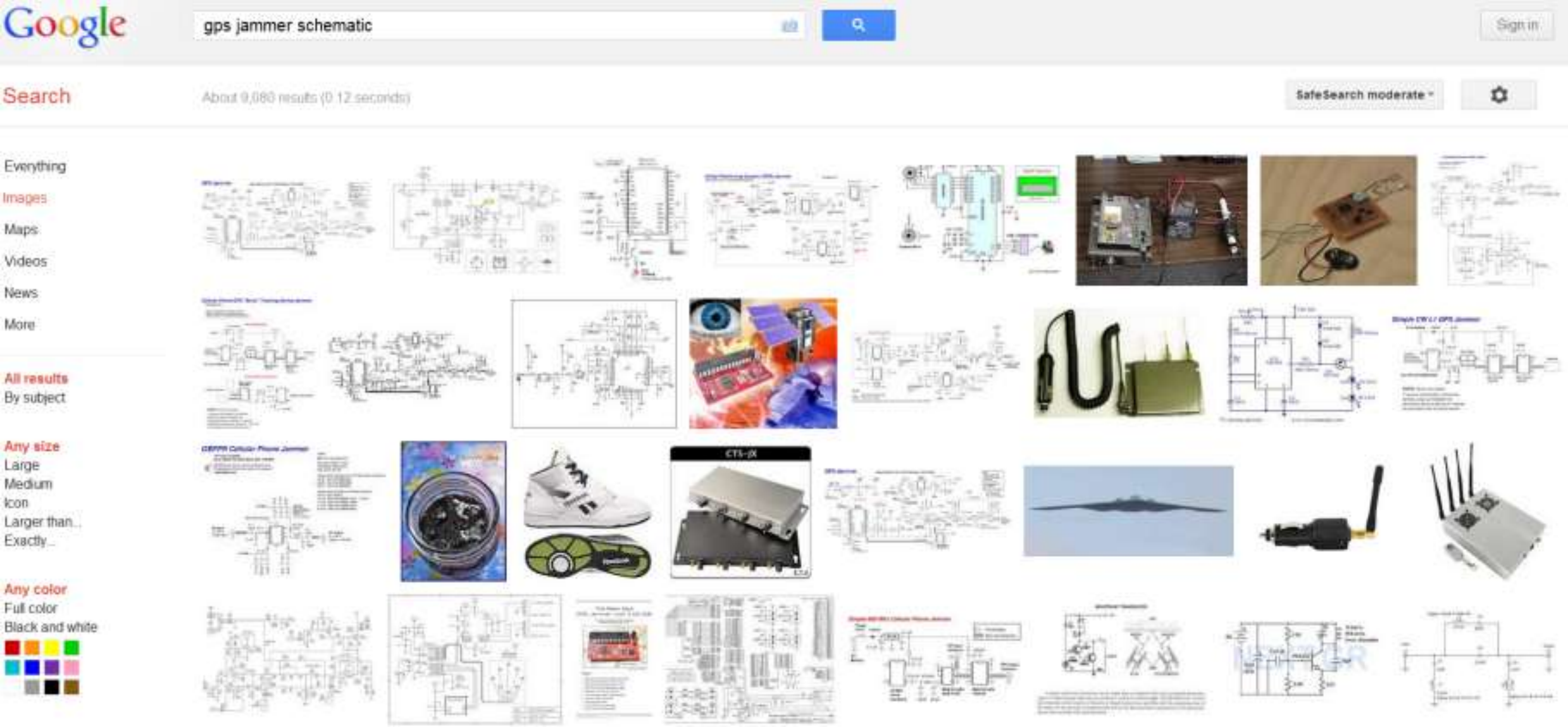
- Broadcast television
- Fixed and mobile VHF transmitters
- Personal electronic devices (PEDs)
- Aeronautical satellite communications
- Mobile satellite services
- Ultra wideband (UWB) radar and communications

Intentional (Deliberate)



STRIDE

GNSS Jamming



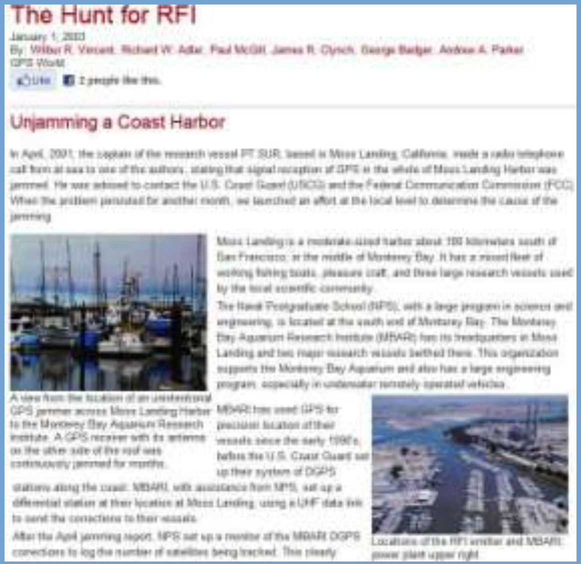
gps jammer schematic

About 9,080 results (0.12 seconds)

SafeSearch moderate

STRIDE

GNSS Jamming



The Hunt for RFI

January 1, 2003
By: Wilbur R. Vincent, Richard W. Adler, Paul McGill, James R. Clynch, George Badger, Andrew A. Parker
GPS World

Like 2 people like this.

Unjamming a Coast Harbor

In April, 2001, the captain of the research vessel PT SUR, based in Moss Landing, California, made a radio telephone call from at sea to one of the authors, stating that signal reception of GPS in the whole of Moss Landing Harbor was jammed. He was advised to contact the U.S. Coast Guard (USCG) and the Federal Communication Commission (FCC). When the problem persisted for another month, we launched an effort at the local level to determine the cause of the jamming.

Moss Landing is a moderate-sized harbor about 100 kilometers south of San Francisco, in the middle of Monterey Bay. It has a mixed fleet of working fishing boats, pleasure craft, and three large research vessels used by the local scientific community.

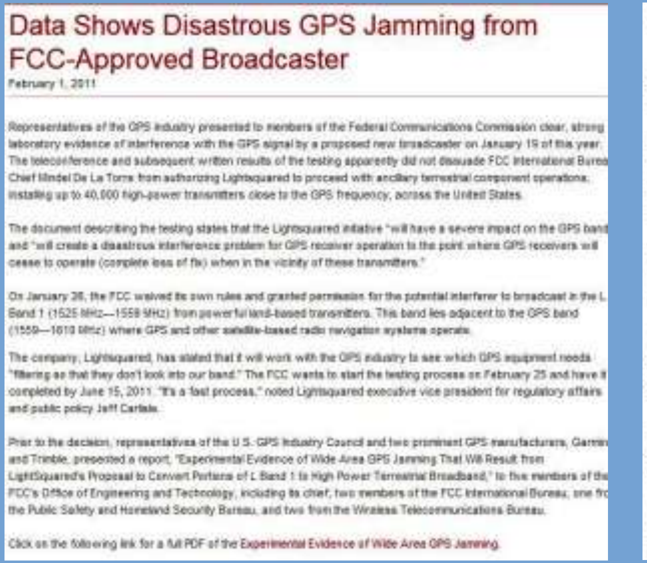
The Naval Postgraduate School (NPS), with a large program in science and engineering, is located at the south end of Monterey Bay. The Monterey Bay Aquarium Research Institute (MBARI) has its headquarters in Moss Landing and two major research vessels berthed there. This organization supports the Monterey Bay Aquarium and also has a large engineering program, especially in underwater remotely operated vehicles.

A view from the location of an unintentional GPS jammer across Moss Landing Harbor to the Monterey Bay Aquarium Research Institute. A GPS receiver with its antenna on the other side of the roof was continuously jammed for months.

MBARI has used GPS for precision location of their vessels since the early 1990's, before the U.S. Coast Guard set up their system of DGPS stations along the coast. MBARI, with assistance from NPS, set up a differential station at their location at Moss Landing, using a UHF data link to send the corrections to their vessels.

After the April jamming report, NPS set up a monitor of the MBARI DGPS corrections to log the number of satellites being tracked. This clearly

Locations of the RFI emitter and MBARI power plant upper right.



Data Shows Disastrous GPS Jamming from FCC-Approved Broadcaster

February 1, 2011

Representatives of the GPS industry presented to members of the Federal Communications Commission clear, strong laboratory evidence of interference with the GPS signal by a proposed new broadcaster on January 19 of this year. The teleconference and subsequent written results of the testing apparently did not dissuade FCC International Burea Chief Mindel De La Torre from authorizing Lightsquared to proceed with ancillary terrestrial component operations: installing up to 40,000 high-power transmitters close to the GPS frequency, across the United States.

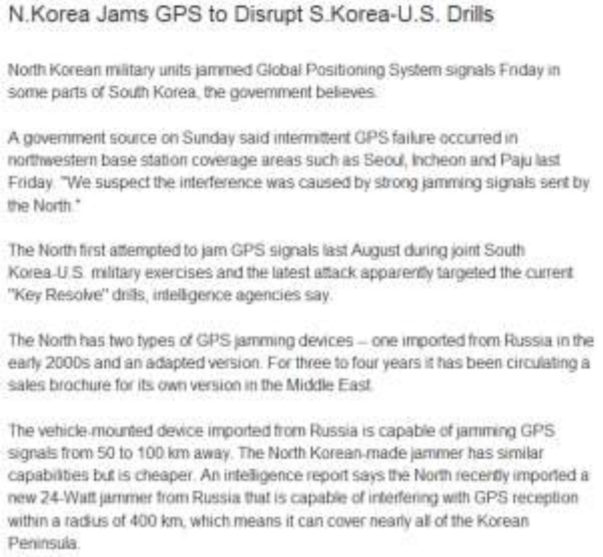
The document describing the testing states that the Lightsquared initiative "will have a severe impact on the GPS band and "will create a disastrous interference problem for GPS receiver operation to the point where GPS receivers will cease to operate (complete loss of fix) when in the vicinity of these transmitters."

On January 26, the FCC waived its own rules and granted permission for the potential interferer to broadcast in the L Band 1 (1525 MHz—1559 MHz) from powerful land-based transmitters. This band lies adjacent to the GPS band (1559—1610 MHz) where GPS and other satellite-based radio navigation systems operate.

The company, Lightsquared, has stated that it will work with the GPS industry to see which GPS equipment needs "filtering so that they don't look into our band." The FCC wants to start the testing process on February 25 and have it completed by June 15, 2011. "It's a fast process," noted Lightsquared executive vice president for regulatory affairs and public policy Jeff Carlisle.

Prior to the decision, representatives of the U.S. GPS Industry Council and two prominent GPS manufacturers, Garmi and Trimble, presented a report, "Experimental Evidence of Wide Area GPS Jamming That Will Result from LightSquared's Proposal to Convert Portions of L Band 1 to High Power Terrestrial Broadband," to five members of the FCC's Office of Engineering and Technology, including its chief, two members of the FCC International Bureau, one fro the Public Safety and Homeland Security Bureau, and two from the Wireless Telecommunications Bureau.

Click on the following link for a full PDF of the Experimental Evidence of Wide Area GPS Jamming.



N.Korea Jams GPS to Disrupt S.Korea-U.S. Drills

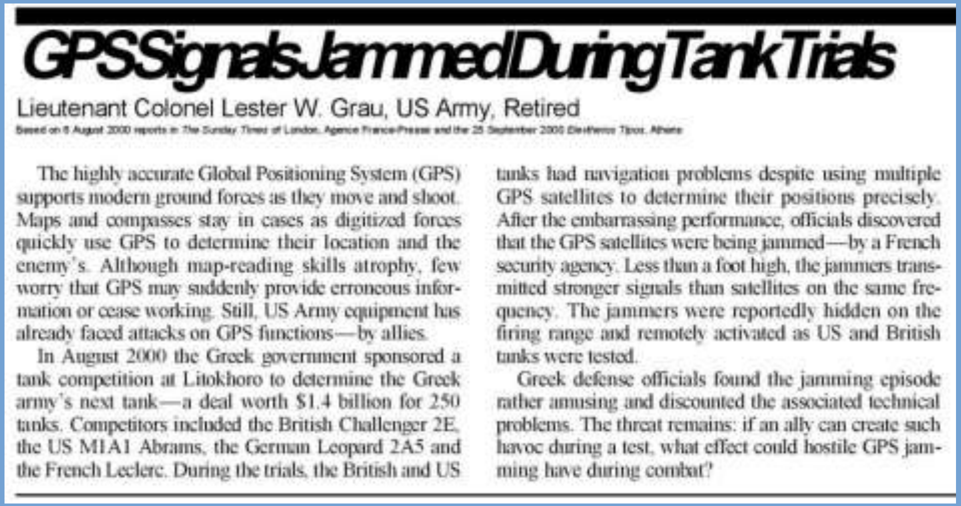
North Korean military units jammed Global Positioning System signals Friday in some parts of South Korea, the government believes.

A government source on Sunday said intermittent GPS failure occurred in northwestern base station coverage areas such as Seoul, Incheon and Paju last Friday. "We suspect the interference was caused by strong jamming signals sent by the North."

The North first attempted to jam GPS signals last August during joint South Korea-U.S. military exercises and the latest attack apparently targeted the current "Key Resolve" drills, intelligence agencies say.

The North has two types of GPS jamming devices – one imported from Russia in the early 2000s and an adapted version. For three to four years it has been circulating a sales brochure for its own version in the Middle East.

The vehicle-mounted device imported from Russia is capable of jamming GPS signals from 50 to 100 km away. The North Korean-made jammer has similar capabilities but is cheaper. An intelligence report says the North recently imported a new 24-Watt jammer from Russia that is capable of interfering with GPS reception within a radius of 400 km, which means it can cover nearly all of the Korean Peninsula.



GPS Signals Jammed During Tank Trials

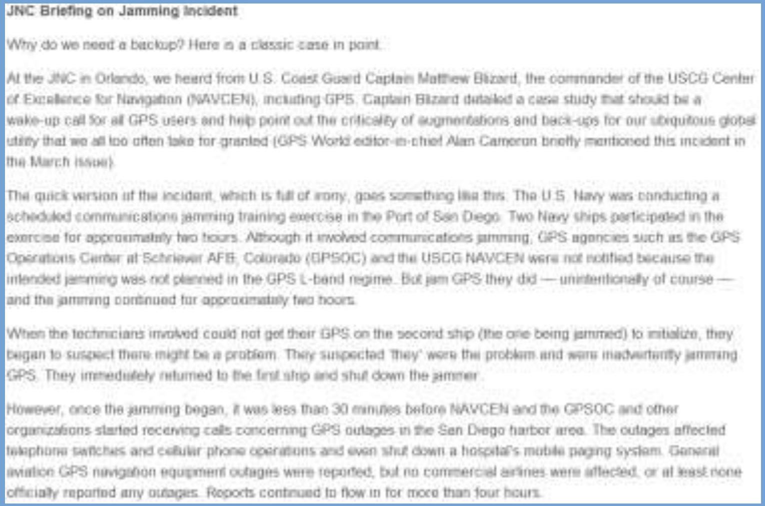
Lieutenant Colonel Lester W. Grau, US Army, Retired

Based on 6 August 2000 reports in *The Sunday Times* of London, Agence France-Presse and the 25 September 2000 *Eleftheros Tipos*, Athens

The highly accurate Global Positioning System (GPS) supports modern ground forces as they move and shoot. Maps and compasses stay in cases as digitized forces quickly use GPS to determine their location and the enemy's. Although map-reading skills atrophy, few worry that GPS may suddenly provide erroneous information or cease working. Still, US Army equipment has already faced attacks on GPS functions—by allies.

In August 2000 the Greek government sponsored a tank competition at Litokhoro to determine the Greek army's next tank—a deal worth $1.4 billion for 250 tanks. Competitors included the British Challenger 2E, the US M1A1 Abrams, the German Leopard 2A5 and the French Leclerc. During the trials, the British and US tanks had navigation problems despite using multiple GPS satellites to determine their positions precisely. After the embarrassing performance, officials discovered that the GPS satellites were being jammed—by a French security agency. Less than a foot high, the jammers transmitted stronger signals than satellites on the same frequency. The jammers were reportedly hidden on the firing range and remotely activated as US and British tanks were tested.

Greek defense officials found the jamming episode rather amusing and discounted the associated technical problems. The threat remains: if an ally can create such havoc during a test, what effect could hostile GPS jamming have during combat?



JNC Briefing on Jamming Incident

Why do we need a backup? Here is a classic case in point.

At the JNC in Orlando, we heard from U.S. Coast Guard Captain Matthew Bizard, the commander of the USCG Center of Excellence for Navigation (NAVCEN), including GPS. Captain Bizard detailed a case study that should be a wake-up call for all GPS users and help point out the criticality of augmentations and back-ups for our ubiquitous global utility that we all too often take for granted (GPS World editor-in-chief Alan Cameron briefly mentioned this incident in the March issue).

The quick version of the incident, which is full of irony, goes something like this. The U.S. Navy was conducting a scheduled communications jamming training exercise in the Port of San Diego. Two Navy ships participated in the exercise for approximately two hours. Although it involved communications jamming, GPS agencies such as the GPS Operations Center at Schriever AFB, Colorado (GPSOC) and the USCG NAVCEN were not notified because the intended jamming was not planned in the GPS L-band regime. But jam GPS they did — unintentionally of course — and the jamming continued for approximately two hours.

When the technicians involved could not get their GPS on the second ship (the one being jammed) to initialize, they began to suspect there might be a problem. They suspected 'they' were the problem and were inadvertently jamming GPS. They immediately returned to the first ship and shut down the jammer.

However, once the jamming began, it was less than 30 minutes before NAVCEN and the GPSOC and other organizations started receiving calls concerning GPS outages in the San Diego harbor area. The outages affected telephone switches and cellular phone operations and even shut down a hospital's mobile paging system. General aviation GPS navigation equipment outages were reported, but no commercial airlines were affected, or at least none officially reported any outages. Reports continued to flow in for more than four hours.

STRIDE

GPS Jamming

Field GPS jamming tests were conducted in November 2009 – June 2010 to study the effect of RFI on GPS signals

STRIDE

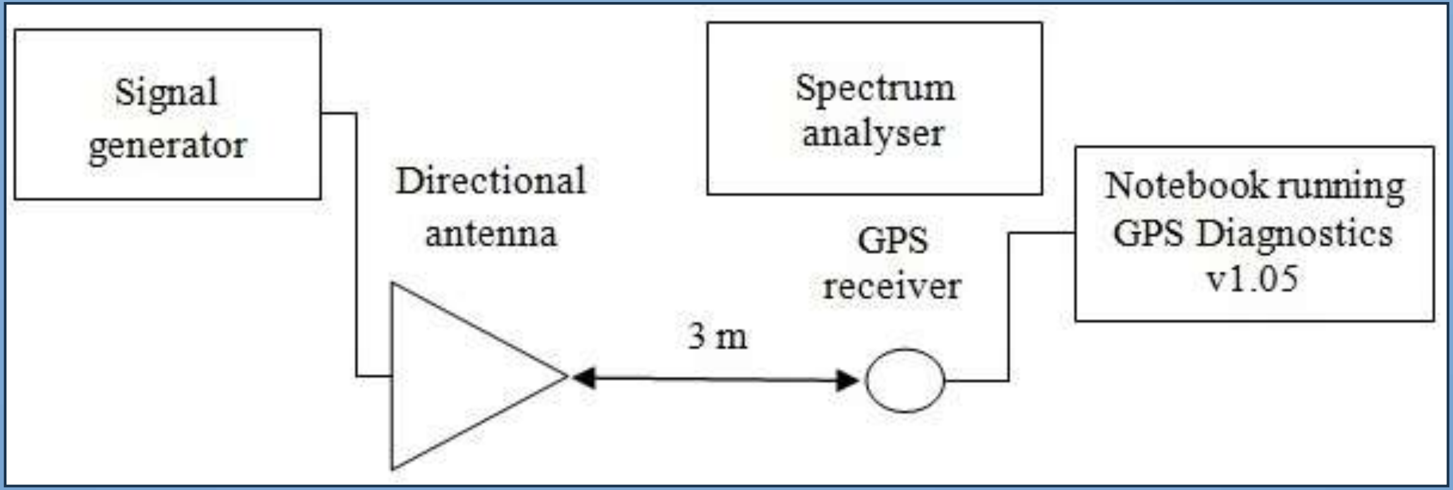
GPS Jamming

Test Site

STRIDE

GPS Jamming

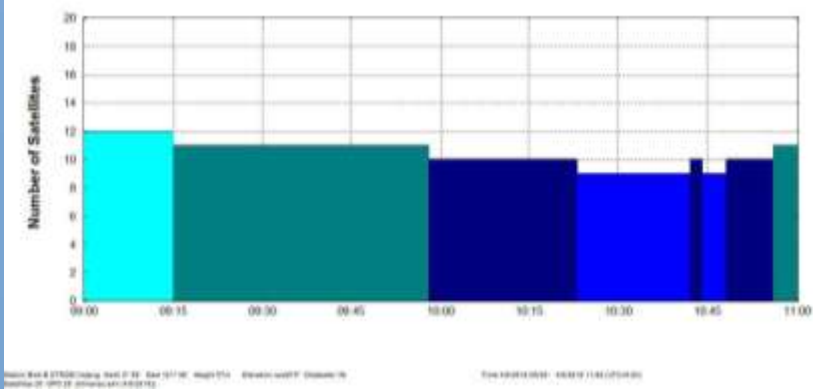
Test Setup

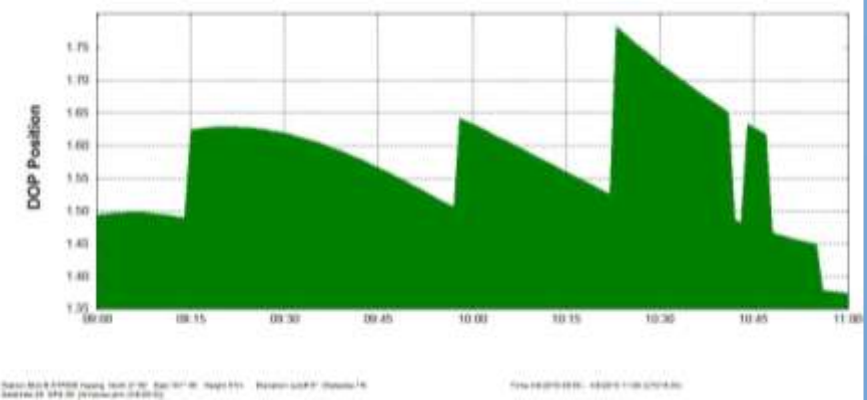


STRIDE

Field Evaluations

GPS Coverage Prediction
(Using Trimble Planning)





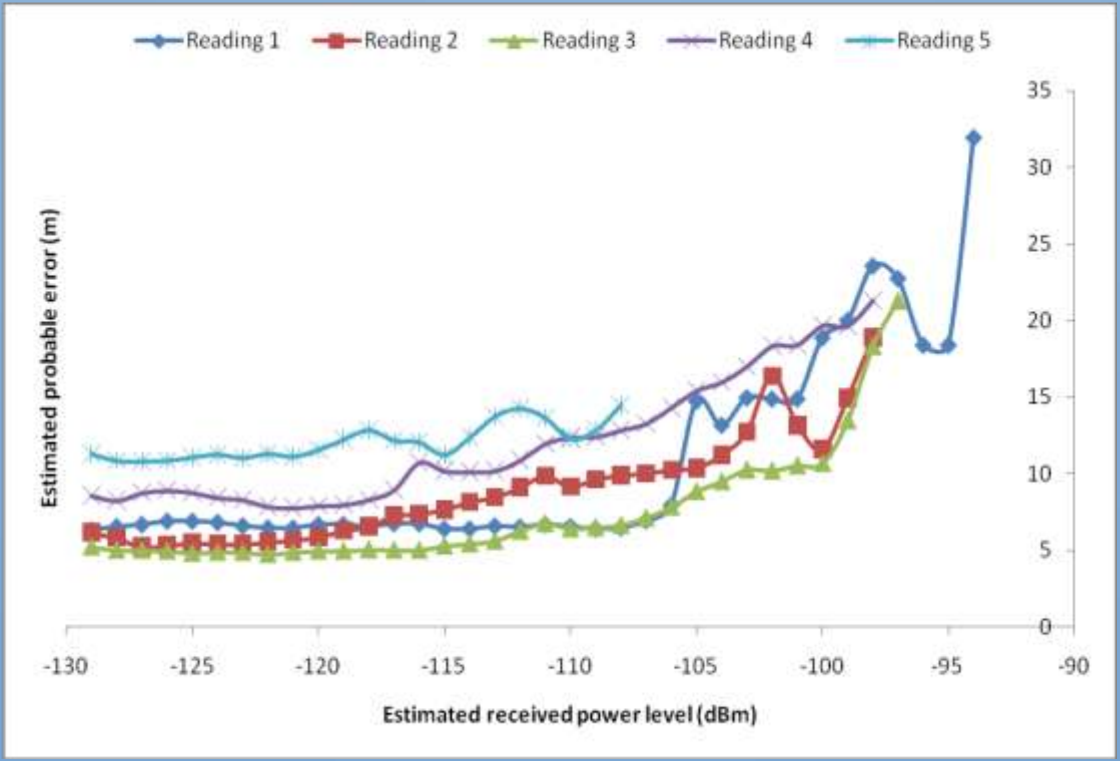
Satellite visibility

PDOP

STRIDE

GPS Jamming

Evaluation of the effect of RFI on GPS accuracy



Discussion

- The accuracy of results obtained was subject to various error parameters, such as:
  - Ionospheric and tropospheric delays,
  - Satellite clock, ephemeris and multipath errors
  - Unintentional signal interferences and obstructions
- All these errors are immeasurable and user-uncontrollable.
- The ideal testing methodology would be using a GNSS simulator which can be used to:
  - Generate multi-satellite GNSS configurations
  - Transmit GNSS signals which simulate real world scenarios
  - Adjust the various error parameters.
- This would allow for the evaluation of GNSS receiver performance under various repeatable conditions, as defined by the user.

STRIDE

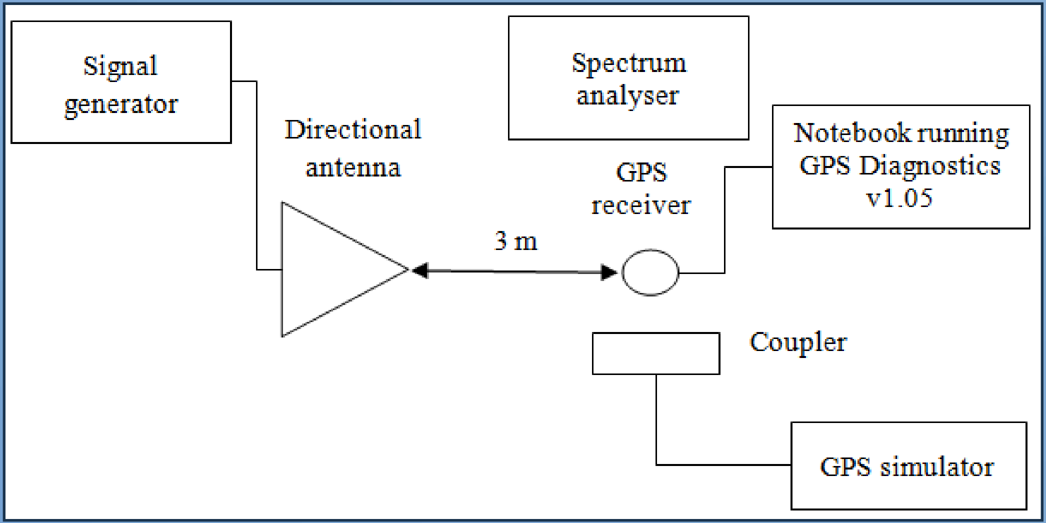
GPS Jamming

- The study was extended via the RMK10 project entitled *Evaluation of the Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Signals via GPS Simulation*.
- Simulated GPS signals generated using an Aeroflex GPSG-1000 GPS simulator.
- Tests conducted in STRIDE’s semi-anechoic chamber.

STRIDE

GPS Jamming

Test Setup



The following assumptions are made for the tests conducted:

- No ionospheric or troposheric delays
- Zero clock and ephemeris error
- No multipath fading, or unintended obstructions
- No unintended interference signals

STRIDE

GPS Jamming

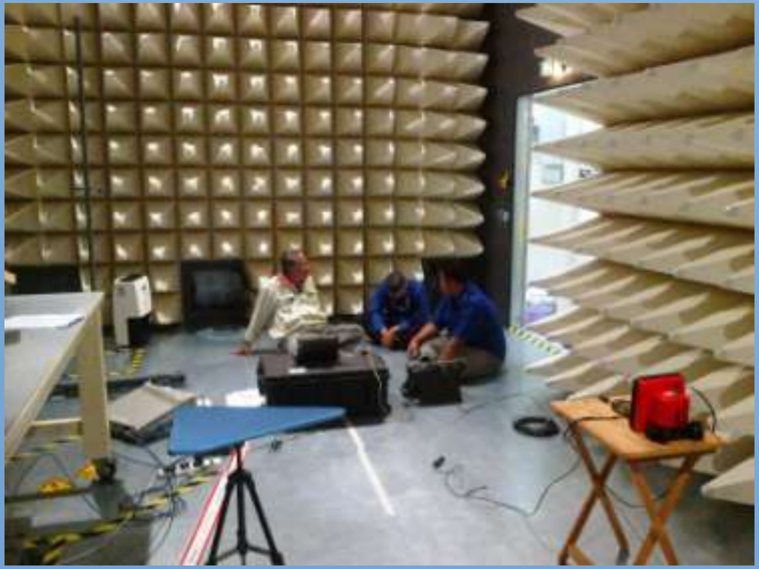
Test Scenarios

Test locations:

- N 2° 58’ E 101° 48’ (Kajang, Selangor, Malaysia)
- N 39° 45’ W 105° 00’ (Denver, Colorado, USA)
- S 16° 55’ E 145° 46’ (Cairns, Queensland, Australia)
- S 51° 37’ W 69° 12’ (Rio Gallegos, Argentina)

UTC times:

- 0000
- 0300
- 0600
- 0900

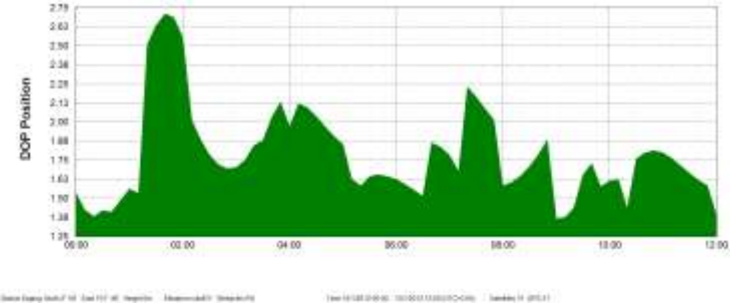


GPS signal power level:

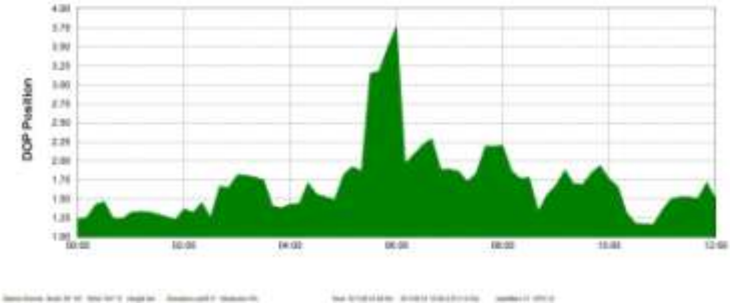
- -131 dBm
- -136 dBm
- -141 dBm
- -146 dBm
- -151 dBm
- -156 dBm

GPS Jamming

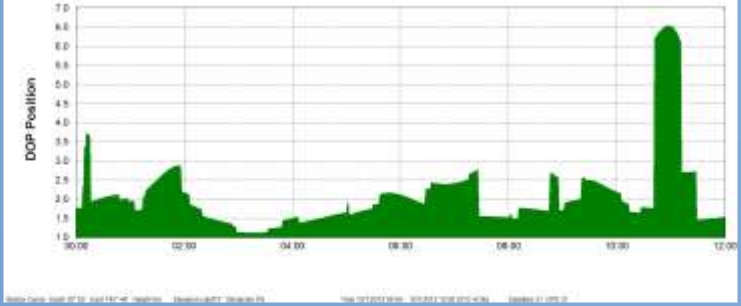
GPS coverage



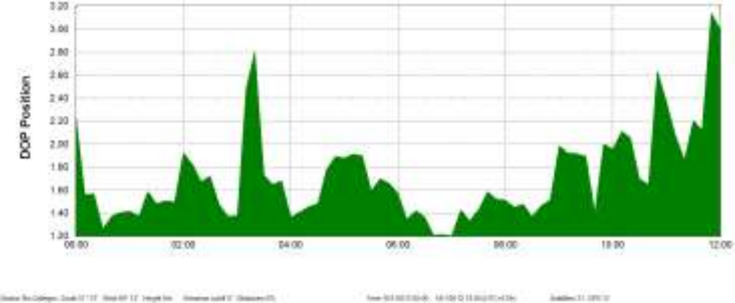
Kajang



Denver



Cairns



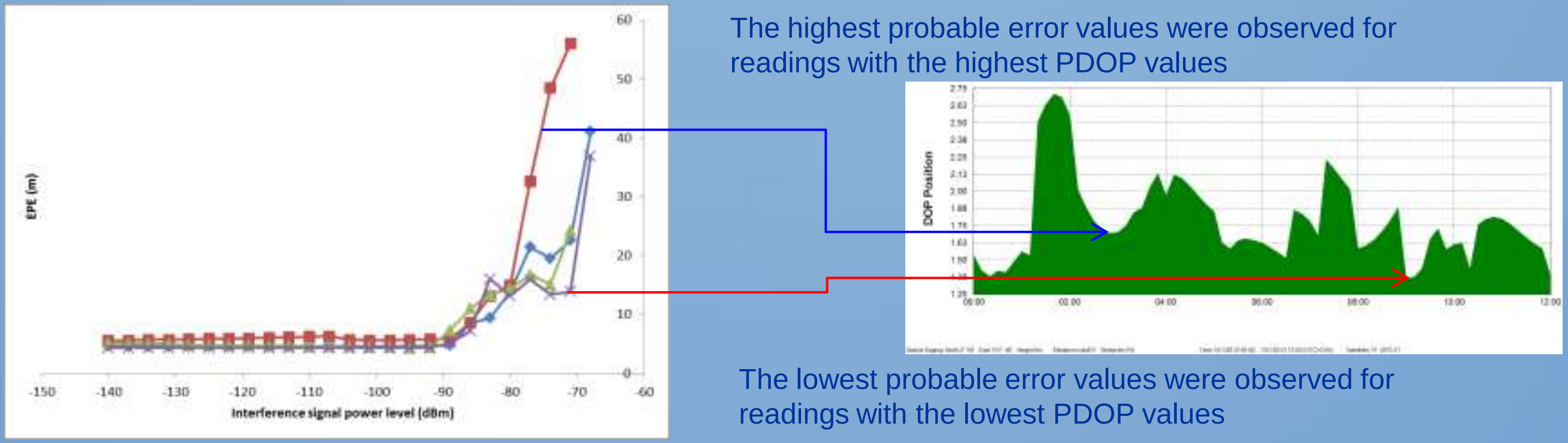
Rio Gallegos

STRIDE

GPS Jamming

Evaluation of the effect of RFI on GPS accuracy (EPE)

Kajang



The highest probable error values were observed for readings with the highest PDOP values

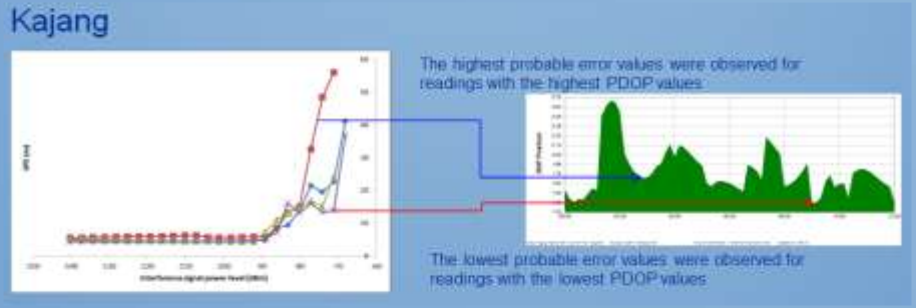
The lowest probable error values were observed for readings with the lowest PDOP values

—◆—0000 UTC —■—0300 UTC —▲—0600 UTC —✕—0900 UTC

STRIDE

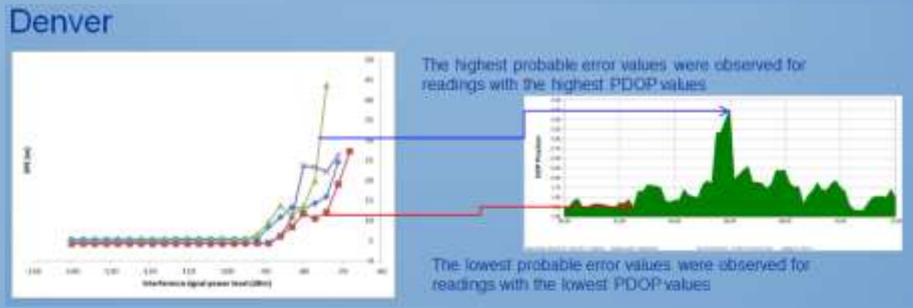
GPS Jamming

Evaluation of the effect of RFI on GPS accuracy (EPE)


Kajang

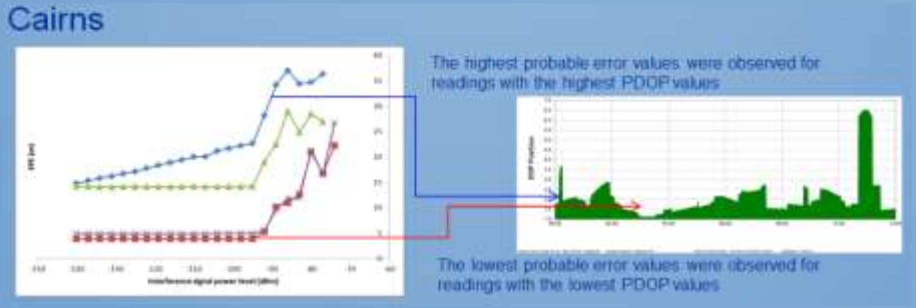
The highest probable error values were observed for readings with the highest PDOP values

The lowest probable error values were observed for readings with the lowest PDOP values


Denver

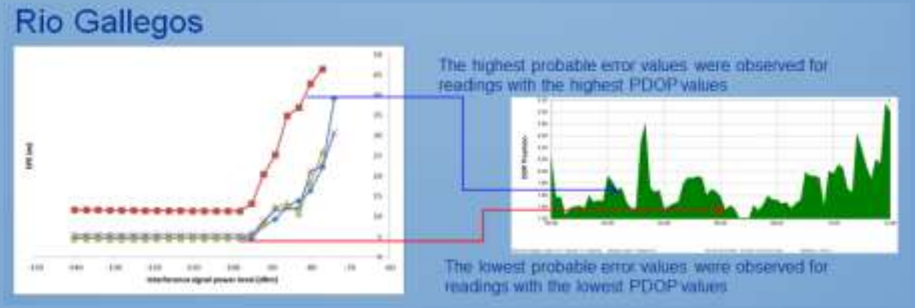
The highest probable error values were observed for readings with the highest PDOP values

The lowest probable error values were observed for readings with the lowest PDOP values


Cairns

The highest probable error values were observed for readings with the highest PDOP values

The lowest probable error values were observed for readings with the lowest PDOP values


Rio Gallegos

The highest probable error values were observed for readings with the highest PDOP values

The lowest probable error values were observed for readings with the lowest PDOP values

◆ 0000 UTC ■ 0300 UTC ▲ 0600 UTC ✕ 0900 UTC

STRIDE

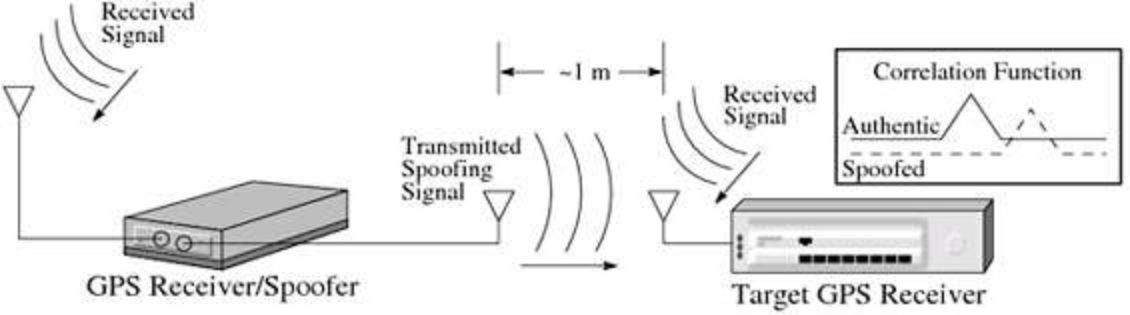
GPS Jamming

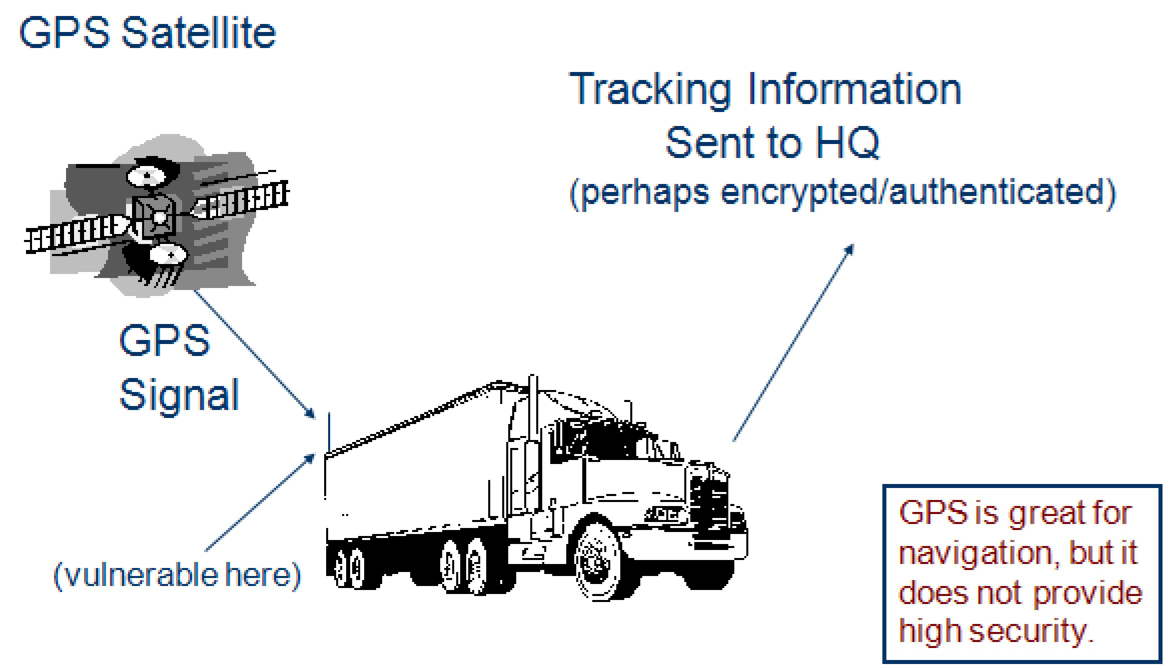
- The absence of other error parameters resulted in the required minimum jamming power levels to be significantly higher as compared to field evaluations.
- Varying probable error patterns are observed for the each of the readings:
  - This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over location and time, resulting in GPS accuracy being location / time dependent.
  - In general:
    - The highest probable error values were observed for readings with the highest PDOP values
    - The the lowest probable error values were observed for readings with the lowest PDOP values.

STRIDE

GNSS Spoofing

- Forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers
- Even if a spoofer is not fully successful, he / she can still create significant errors and jam GNSS signals over large areas




GPS Satellite

Tracking Information Sent to HQ (perhaps encrypted/authenticated)

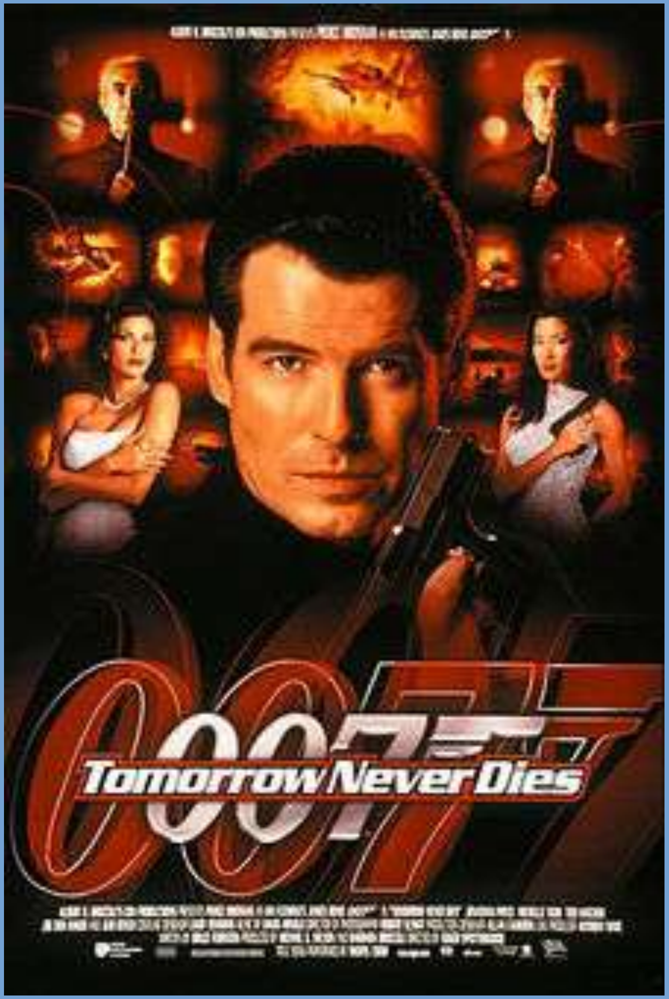
GPS Signal

(vulnerable here)

GPS is great for navigation, but it does not provide high security.

STRIDE

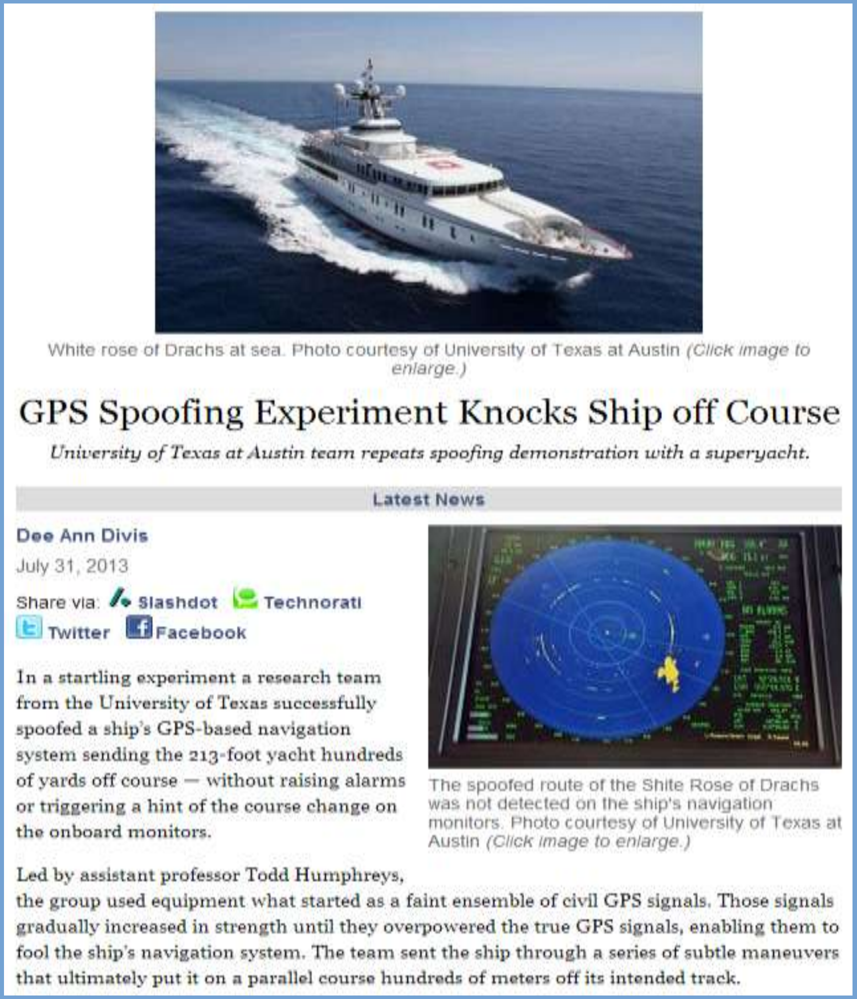
GNSS Spoofing



GPS spoofing used to trick a British vessel into Chinese waters

STRIDE

GNSS Spoofing



White rose of Drachs at sea. Photo courtesy of University of Texas at Austin *(Click image to enlarge.)*

GPS Spoofing Experiment Knocks Ship off Course

University of Texas at Austin team repeats spoofing demonstration with a superyacht.

Latest News

Dee Ann Divis

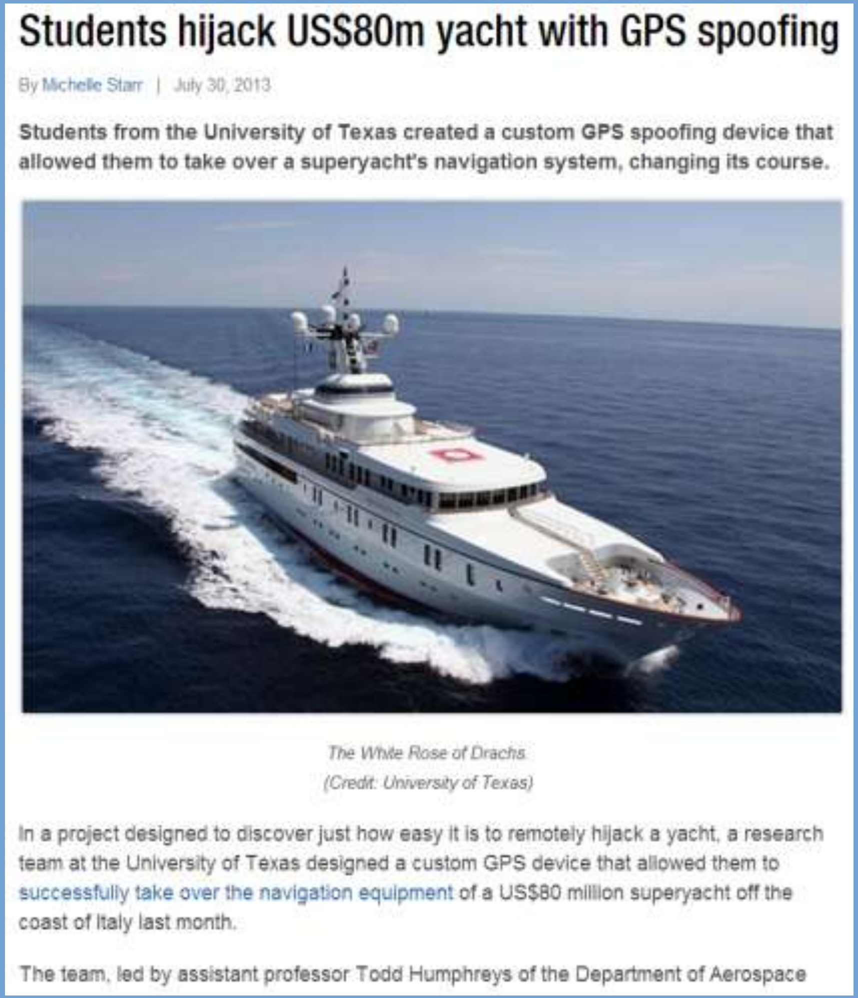
July 31, 2013

Share via: Slashdot Technorati Twitter Facebook

In a startling experiment a research team from the University of Texas successfully spoofed a ship's GPS-based navigation system sending the 213-foot yacht hundreds of yards off course — without raising alarms or triggering a hint of the course change on the onboard monitors.

The spoofed route of the Shite Rose of Drachs was not detected on the ship's navigation monitors. Photo courtesy of University of Texas at Austin *(Click image to enlarge.)*

Led by assistant professor Todd Humphreys, the group used equipment what started as a faint ensemble of civil GPS signals. Those signals gradually increased in strength until they overpowered the true GPS signals, enabling them to fool the ship's navigation system. The team sent the ship through a series of subtle maneuvers that ultimately put it on a parallel course hundreds of meters off its intended track.



Students hijack US$80m yacht with GPS spoofing

By Michelle Starr | July 30, 2013

Students from the University of Texas created a custom GPS spoofing device that allowed them to take over a superyacht's navigation system, changing its course.

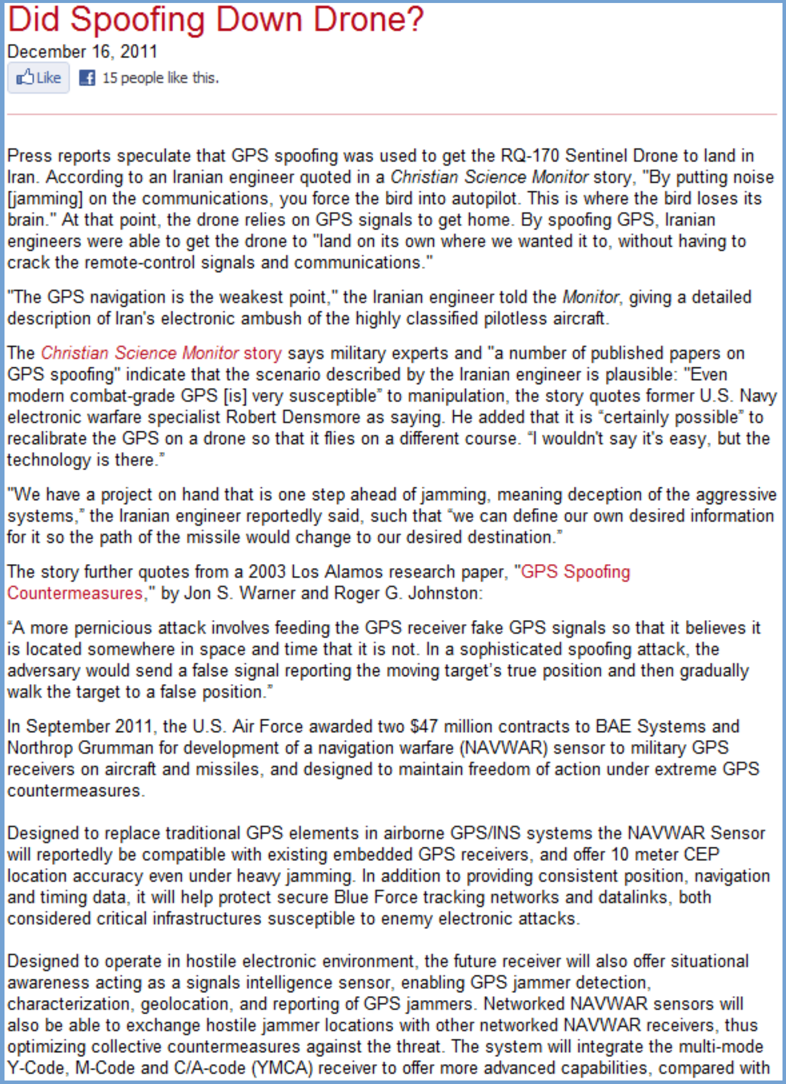
The White Rose of Drachs
(Credit: University of Texas)

In a project designed to discover just how easy it is to remotely hijack a yacht, a research team at the University of Texas designed a custom GPS device that allowed them to successfully take over the navigation equipment of a US$80 million superyacht off the coast of Italy last month.

The team, led by assistant professor Todd Humphreys of the Department of Aerospace

STRIDE

GNSS Spoofing



Did Spoofing Down Drone?

December 16, 2011

Like 15 people like this.

Press reports speculate that GPS spoofing was used to get the RQ-170 Sentinel Drone to land in Iran. According to an Iranian engineer quoted in a *Christian Science Monitor* story, "By putting noise [jamming] on the communications, you force the bird into autopilot. This is where the bird loses its brain." At that point, the drone relies on GPS signals to get home. By spoofing GPS, Iranian engineers were able to get the drone to "land on its own where we wanted it to, without having to crack the remote-control signals and communications."

"The GPS navigation is the weakest point," the Iranian engineer told the *Monitor*, giving a detailed description of Iran's electronic ambush of the highly classified pilotless aircraft.

The *Christian Science Monitor* story says military experts and "a number of published papers on GPS spoofing" indicate that the scenario described by the Iranian engineer is plausible: "Even modern combat-grade GPS [is] very susceptible" to manipulation, the story quotes former U.S. Navy electronic warfare specialist Robert Densmore as saying. He added that it is "certainly possible" to recalibrate the GPS on a drone so that it flies on a different course. "I wouldn't say it's easy, but the technology is there."

"We have a project on hand that is one step ahead of jamming, meaning deception of the aggressive systems," the Iranian engineer reportedly said, such that "we can define our own desired information for it so the path of the missile would change to our desired destination."

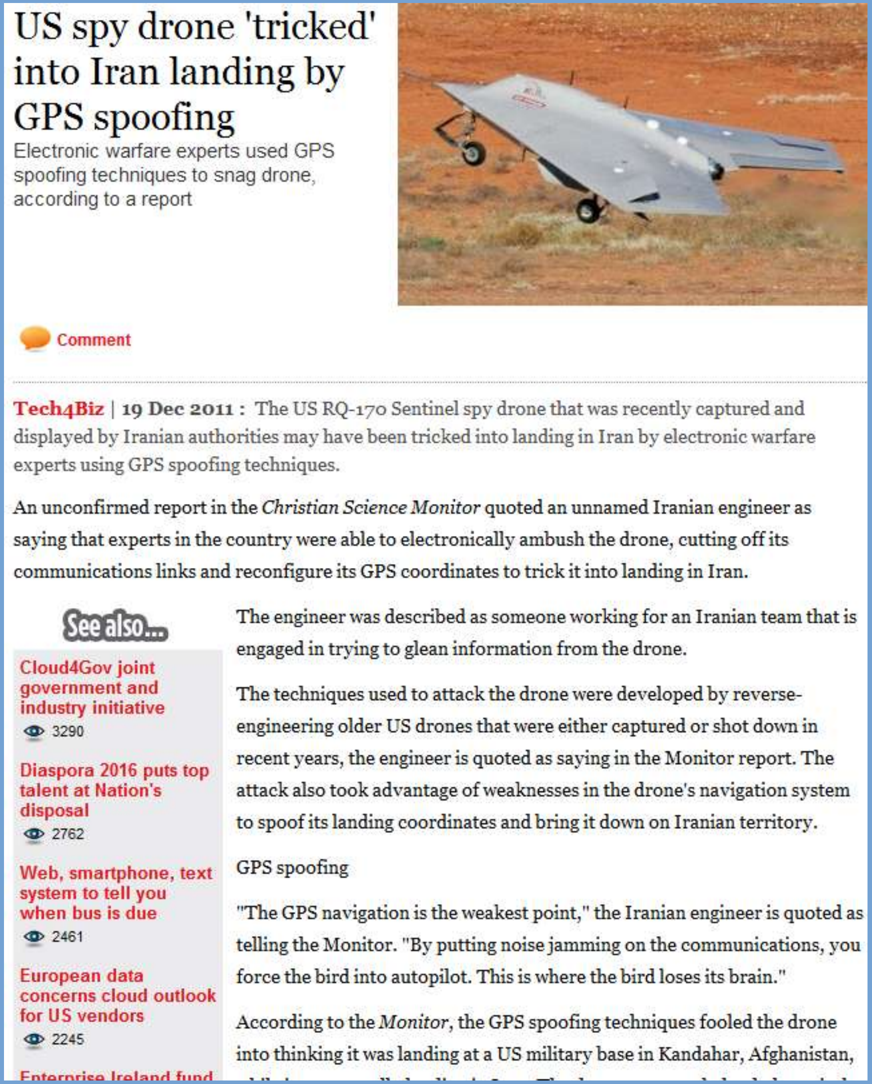
The story further quotes from a 2003 Los Alamos research paper, "GPS Spoofing Countermeasures," by Jon S. Warner and Roger G. Johnston:

"A more pernicious attack involves feeding the GPS receiver fake GPS signals so that it believes it is located somewhere in space and time that it is not. In a sophisticated spoofing attack, the adversary would send a false signal reporting the moving target's true position and then gradually walk the target to a false position."

In September 2011, the U.S. Air Force awarded two $47 million contracts to BAE Systems and Northrop Grumman for development of a navigation warfare (NAVWAR) sensor to military GPS receivers on aircraft and missiles, and designed to maintain freedom of action under extreme GPS countermeasures.

Designed to replace traditional GPS elements in airborne GPS/INS systems the NAVWAR Sensor will reportedly be compatible with existing embedded GPS receivers, and offer 10 meter CEP location accuracy even under heavy jamming. In addition to providing consistent position, navigation and timing data, it will help protect secure Blue Force tracking networks and datalinks, both considered critical infrastructures susceptible to enemy electronic attacks.

Designed to operate in hostile electronic environment, the future receiver will also offer situational awareness acting as a signals intelligence sensor, enabling GPS jammer detection, characterization, geolocation, and reporting of GPS jammers. Networked NAVWAR sensors will also be able to exchange hostile jammer locations with other networked NAVWAR receivers, thus optimizing collective countermeasures against the threat. The system will integrate the multi-mode Y-Code, M-Code and C/A-code (YMCA) receiver to offer more advanced capabilities, compared with



US spy drone 'tricked' into Iran landing by GPS spoofing

Electronic warfare experts used GPS spoofing techniques to snag drone, according to a report

Comment

Tech4Biz | **19 Dec 2011 :** The US RQ-170 Sentinel spy drone that was recently captured and displayed by Iranian authorities may have been tricked into landing in Iran by electronic warfare experts using GPS spoofing techniques.

An unconfirmed report in the *Christian Science Monitor* quoted an unnamed Iranian engineer as saying that experts in the country were able to electronically ambush the drone, cutting off its communications links and reconfigure its GPS coordinates to trick it into landing in Iran.

See also...

Cloud4Gov joint government and industry initiative
3290

Diaspora 2016 puts top talent at Nation's disposal
2762

Web, smartphone, text system to tell you when bus is due
2461

European data concerns cloud outlook for US vendors
2245

Enterprise Ireland fund

The engineer was described as someone working for an Iranian team that is engaged in trying to glean information from the drone.

The techniques used to attack the drone were developed by reverse-engineering older US drones that were either captured or shot down in recent years, the engineer is quoted as saying in the Monitor report. The attack also took advantage of weaknesses in the drone's navigation system to spoof its landing coordinates and bring it down on Iranian territory.

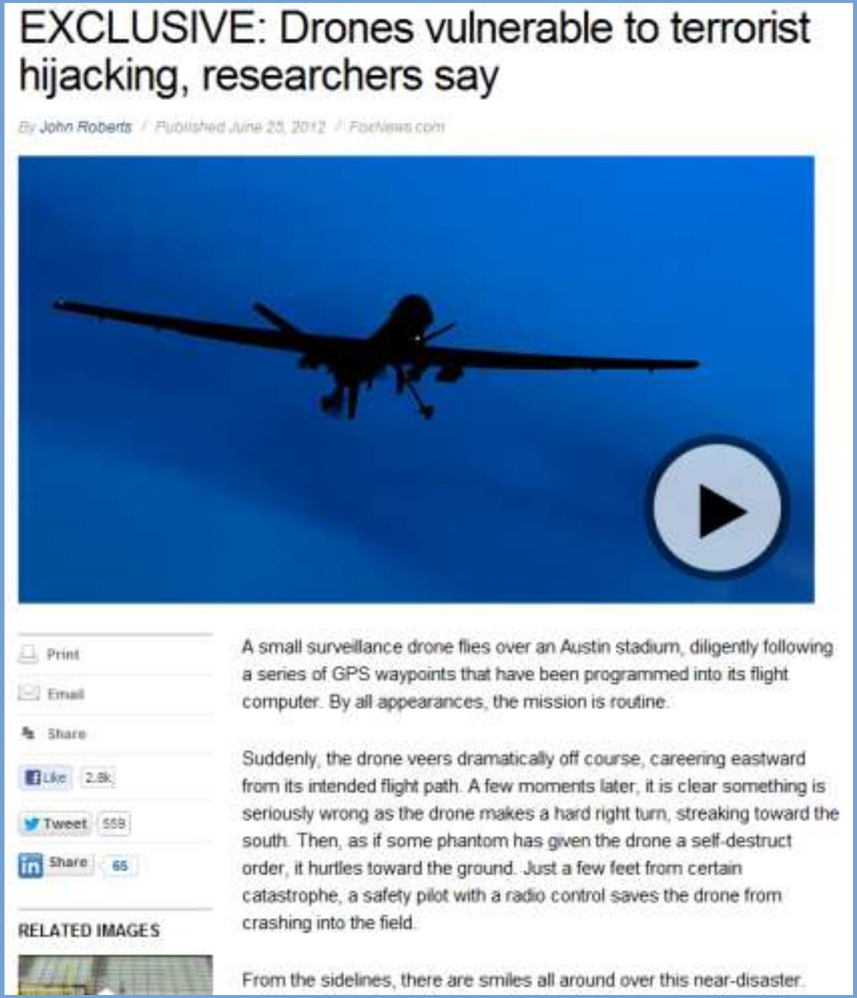
GPS spoofing

"The GPS navigation is the weakest point," the Iranian engineer is quoted as telling the Monitor. "By putting noise jamming on the communications, you force the bird into autopilot. This is where the bird loses its brain."

According to the *Monitor*, the GPS spoofing techniques fooled the drone into thinking it was landing at a US military base in Kandahar, Afghanistan,

STRIDE

GNSS Spoofing



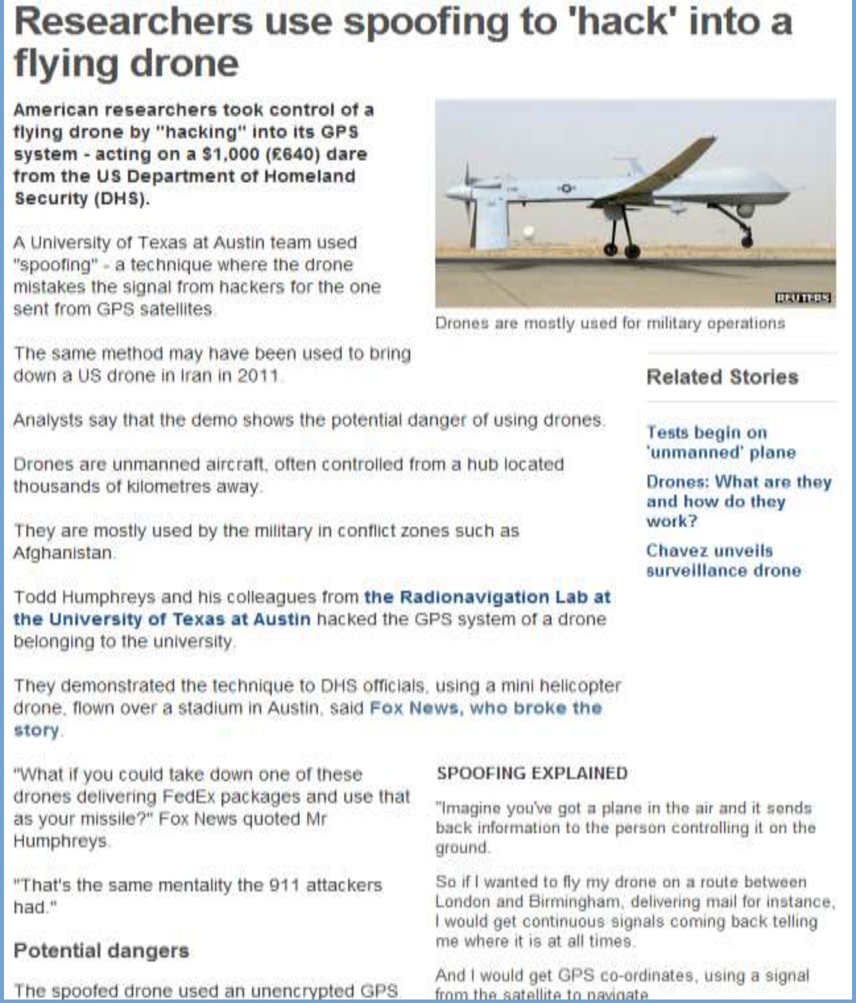
EXCLUSIVE: Drones vulnerable to terrorist hijacking, researchers say

By John Roberts / Published June 25, 2012 / FoxNews.com

A small surveillance drone flies over an Austin stadium, diligently following a series of GPS waypoints that have been programmed into its flight computer. By all appearances, the mission is routine.

Suddenly, the drone veers dramatically off course, careering eastward from its intended flight path. A few moments later, it is clear something is seriously wrong as the drone makes a hard right turn, streaking toward the south. Then, as if some phantom has given the drone a self-destruct order, it hurtles toward the ground. Just a few feet from certain catastrophe, a safety pilot with a radio control saves the drone from crashing into the field.

From the sidelines, there are smiles all around over this near-disaster.



Researchers use spoofing to 'hack' into a flying drone

American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).

A University of Texas at Austin team used "spoofing" - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

The same method may have been used to bring down a US drone in Iran in 2011.

Analysts say that the demo shows the potential danger of using drones.

Drones are unmanned aircraft, often controlled from a hub located thousands of kilometres away.

They are mostly used by the military in conflict zones such as Afghanistan.

Todd Humphreys and his colleagues from **the Radionavigation Lab at the University of Texas at Austin** hacked the GPS system of a drone belonging to the university.

They demonstrated the technique to DHS officials, using a mini helicopter drone, flown over a stadium in Austin, said **Fox News, who broke the story**.

"What if you could take down one of these drones delivering FedEx packages and use that as your missile?" Fox News quoted Mr Humphreys.

"That's the same mentality the 911 attackers had."

Potential dangers

The spoofed drone used an unencrypted GPS

Drones are mostly used for military operations

Related Stories

Tests begin on 'unmanned' plane

Drones: What are they and how do they work?

Chavez unveils surveillance drone

SPOOFING EXPLAINED

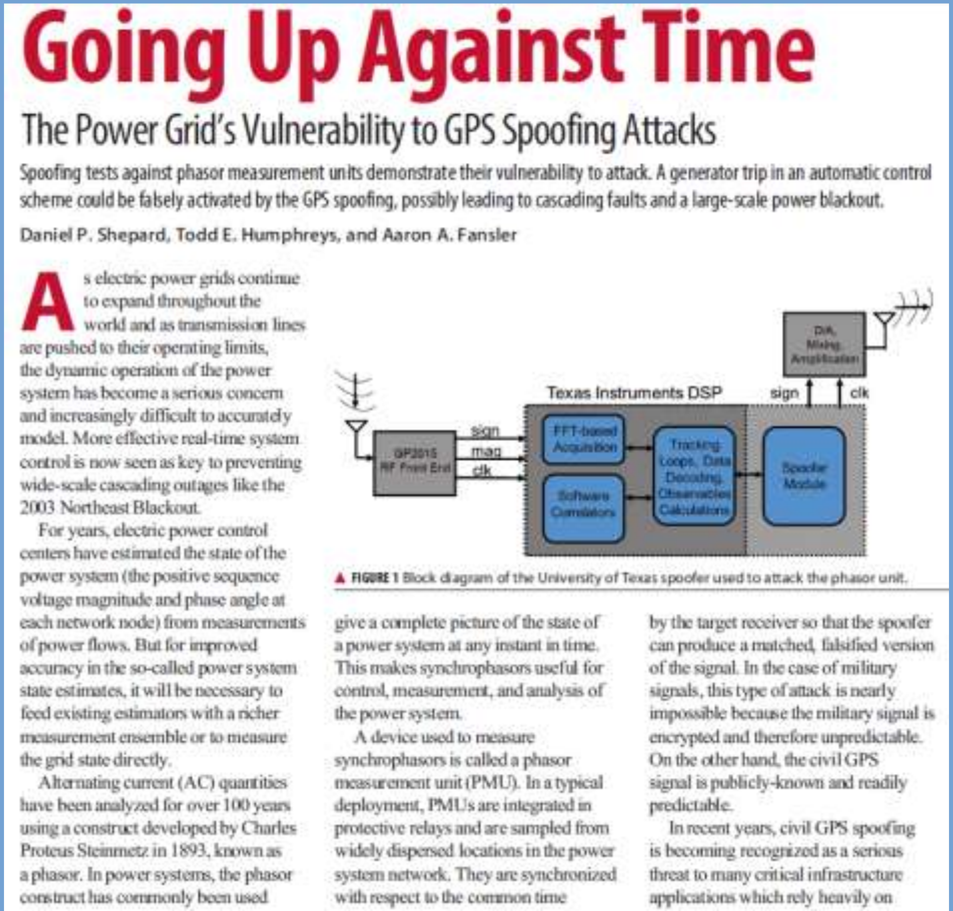
"Imagine you've got a plane in the air and it sends back information to the person controlling it on the ground.

So if I wanted to fly my drone on a route between London and Birmingham, delivering mail for instance, I would get continuous signals coming back telling me where it is at all times.

And I would get GPS co-ordinates, using a signal from the satellite to navigate

STRIDE

GNSS Spoofing



Going Up Against Time

The Power Grid's Vulnerability to GPS Spoofing Attacks

Spoofing tests against phasor measurement units demonstrate their vulnerability to attack. A generator trip in an automatic control scheme could be falsely activated by the GPS spoofing, possibly leading to cascading faults and a large-scale power blackout.

Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler

As electric power grids continue to expand throughout the world and as transmission lines are pushed to their operating limits, the dynamic operation of the power system has become a serious concern and increasingly difficult to accurately model. More effective real-time system control is now seen as key to preventing wide-scale cascading outages like the 2003 Northeast Blackout.

For years, electric power control centers have estimated the state of the power system (the positive sequence voltage magnitude and phase angle at each network node) from measurements of power flows. But for improved accuracy in the so-called power system state estimates, it will be necessary to feed existing estimators with a richer measurement ensemble or to measure the grid state directly.

Alternating current (AC) quantities have been analyzed for over 100 years using a construct developed by Charles Proteus Steinmetz in 1893, known as a phasor. In power systems, the phasor construct has commonly been used

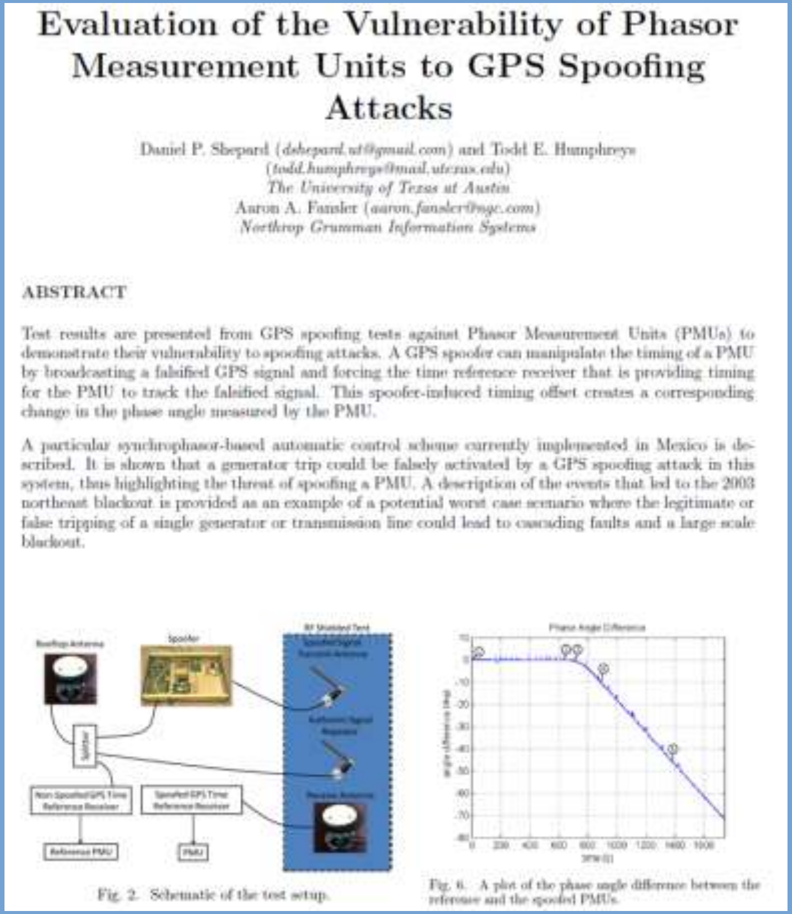
▲ FIGURE 1 Block diagram of the University of Texas spoofer used to attack the phasor unit.

give a complete picture of the state of a power system at any instant in time. This makes synchrophasors useful for control, measurement, and analysis of the power system.

A device used to measure synchrophasors is called a phasor measurement unit (PMU). In a typical deployment, PMUs are integrated in protective relays and are sampled from widely dispersed locations in the power system network. They are synchronized with respect to the common time

by the target receiver so that the spoofer can produce a matched, falsified version of the signal. In the case of military signals, this type of attack is nearly impossible because the military signal is encrypted and therefore unpredictable. On the other hand, the civil GPS signal is publicly-known and readily predictable.

In recent years, civil GPS spoofing is becoming recognized as a serious threat to many critical infrastructure applications which rely heavily on



Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks

Daniel P. Shepard (*dshepard.ut@gmail.com*) and Todd E. Humphreys
(*todd.humphreys@mail.utexas.edu*)
The University of Texas at Austin
Aaron A. Fansler (*aaron.fansler@ngc.com*)
Northrop Grumman Information Systems

ABSTRACT

Test results are presented from GPS spoofing tests against Phasor Measurement Units (PMUs) to demonstrate their vulnerability to spoofing attacks. A GPS spoofer can manipulate the timing of a PMU by broadcasting a falsified GPS signal and forcing the time reference receiver that is providing timing for the PMU to track the falsified signal. This spoofer-induced timing offset creates a corresponding change in the phase angle measured by the PMU.

A particular synchrophasor-based automatic control scheme currently implemented in Mexico is described. It is shown that a generator trip could be falsely activated by a GPS spoofing attack in this system, thus highlighting the threat of spoofing a PMU. A description of the events that led to the 2003 northeast blackout is provided as an example of a potential worst case scenario where the legitimate or false tripping of a single generator or transmission line could lead to cascading faults and a large scale blackout.

Rooftop Antenna
Spoofer
RF Shielded Tent
Spoofed Signal Transmit Antenna
Authentic Signal Repeater
Receive Antenna
Splitter
Non Spoofed GPS Time Reference Receiver
Spoofed GPS Time Reference Receiver
Reference PMU
PMU

Fig. 2. Schematic of the test setup.

Fig. 6. A plot of the phase angle difference between the reference and the spoofed PMUs.

STRIDE

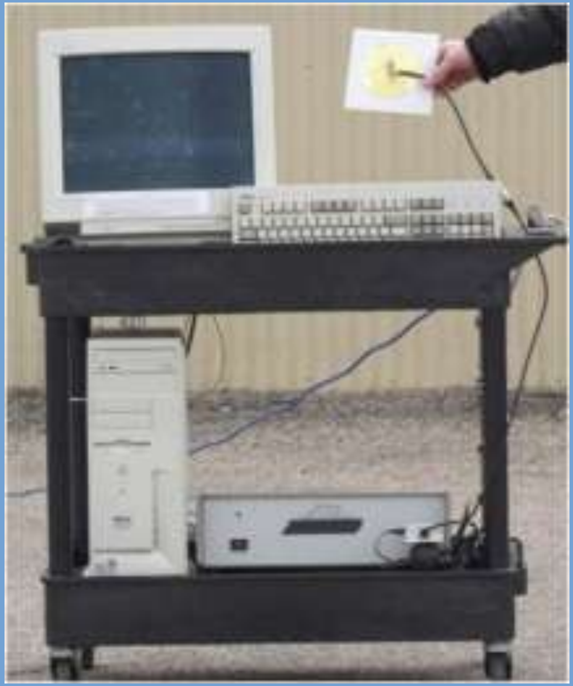
GNSS Spoofing

- A number of GNSS simulators have been designed for legal purposes
- In the wrong hands, can be used for spoofing

STRIDE

GNSS Spoofing

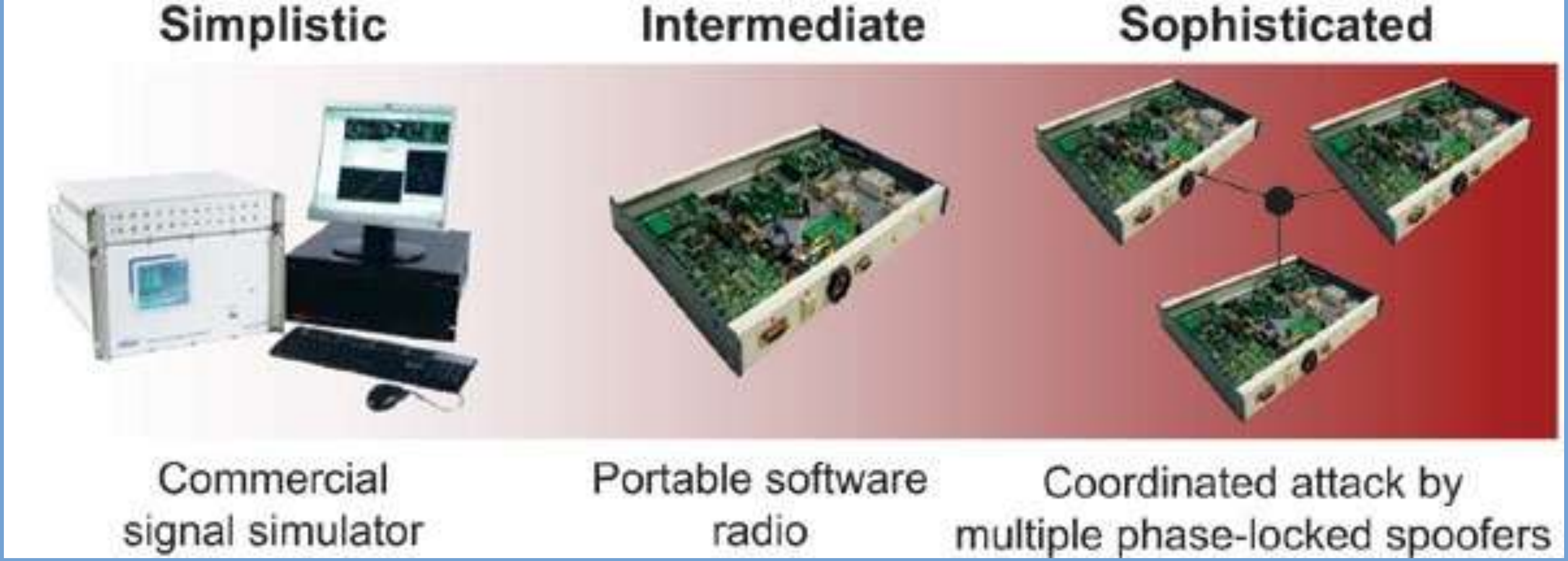
GNSS simulators can be built with relatively low cost equipment



STRIDE

GNSS Spoofing

The spoofing threat continuum


Simplistic
Intermediate
Sophisticated
Commercial signal simulator
Portable software radio
Coordinated attack by multiple phase-locked spoofers

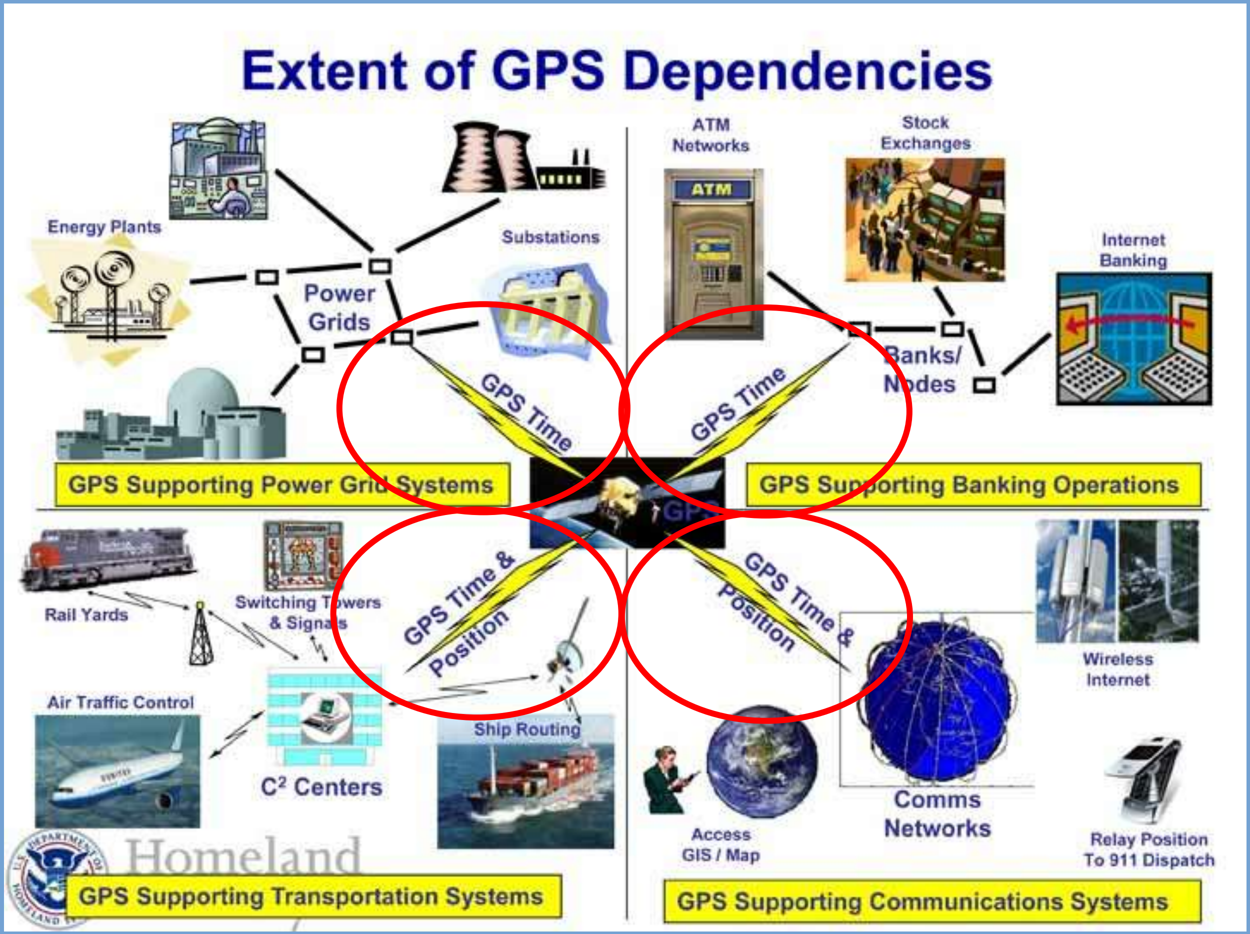
GNSS Spoofing

Meaconing

- GNSS record and playback systems record real GNSS signals and retransmit the signals to evaluated GNSS receivers.
- While spoofing using this method cannot be used to impose user-defined scenarios on a receiver, it can still cause the receiver to compute false location fixes using the transmitted real GNSS signals.
- Furthermore, this form of attack can be used for spoofing military GNSS signals

STRIDE

GNSS Spoofing

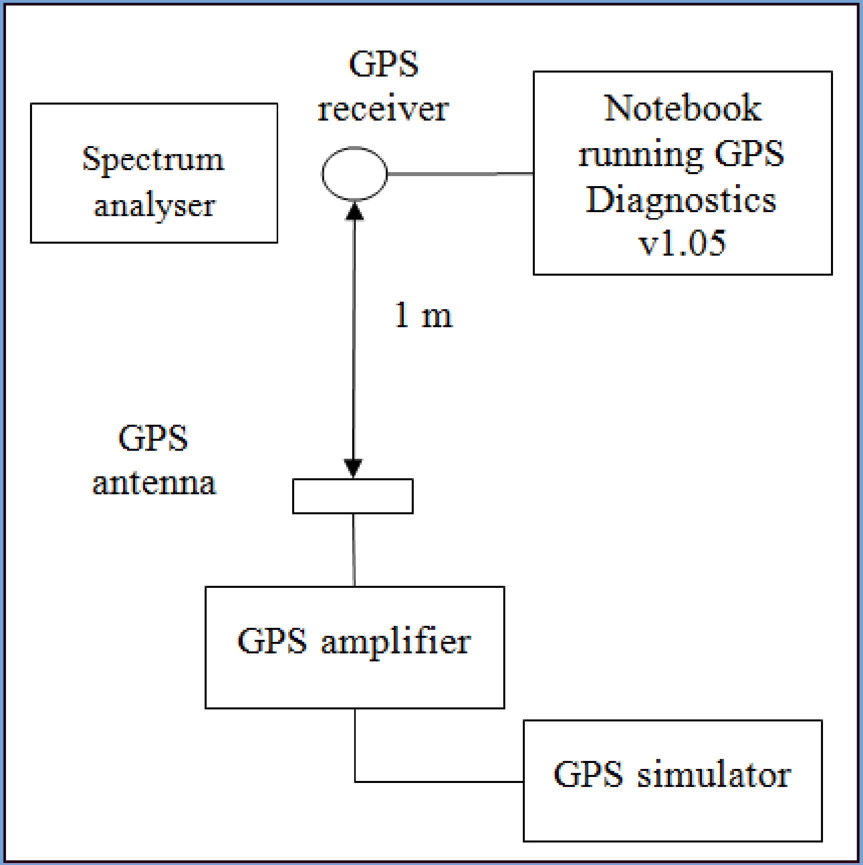


STRIDE

GPS Spoofing

Test Setup

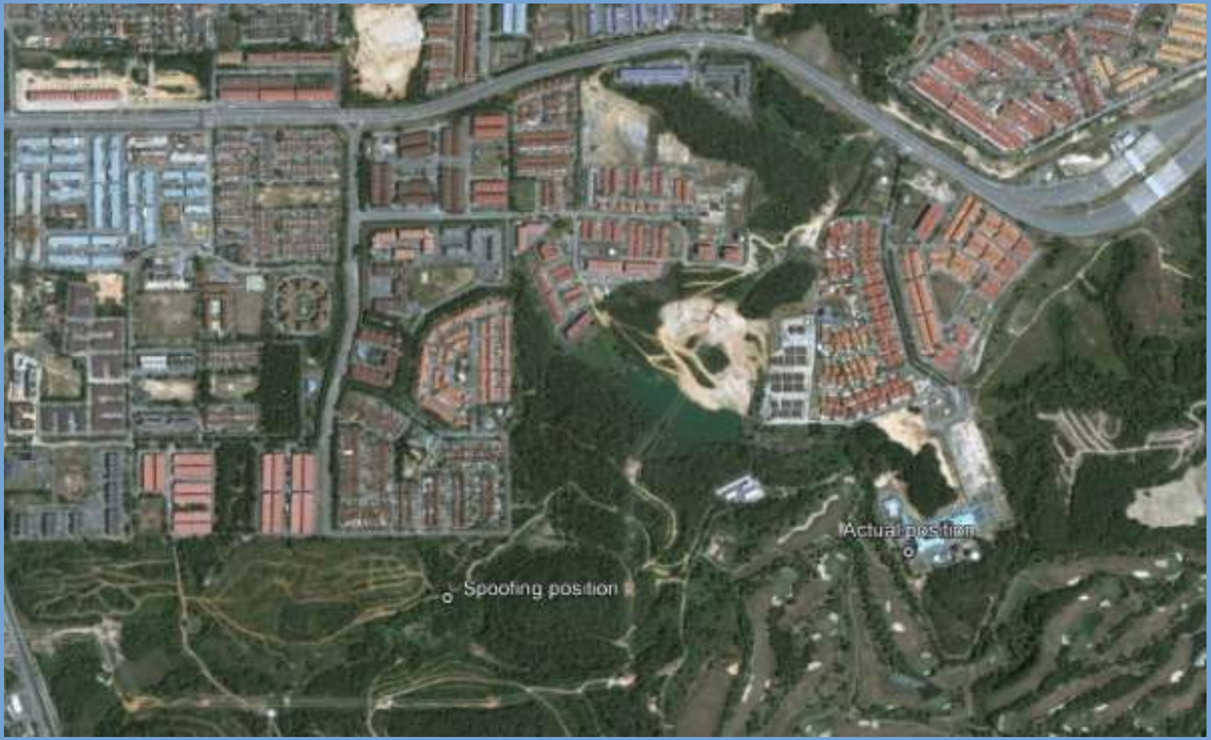
- This study is aimed at evaluating GPS performance during simplistic GPS spoofing attacks.
- Spoofing is conducted using a standalone GPS simulator, which at present poses the greatest near-term threat.
- In this type of spoofing attack, the spoofing signal is not synchronised (in terms of power level, phase, Doppler shift and data content) with the genuine signals received by the target GPS receiver.
- This could cause the target GPS receiver to temporarily lose position fix lock first, before being taken over by the spoofing signal.



GPS Spoofing

Test Scenario

- Test area located at N 2º 58.056’ E 101º 48.586’ 70m
- The spoofing signal is set for position of N 2º 58’ E 101º 48’ 80m, while the time is set at the simulator’s GPS receiver time.

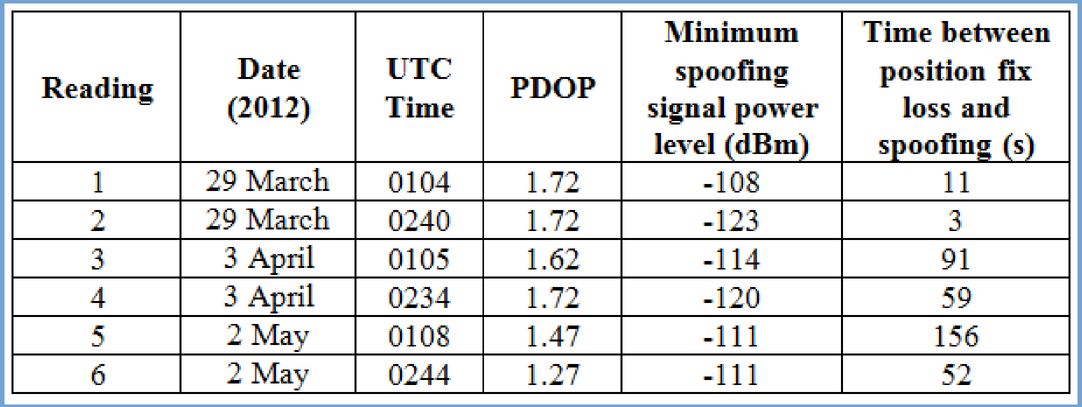


STRIDE

GPS Spoofing

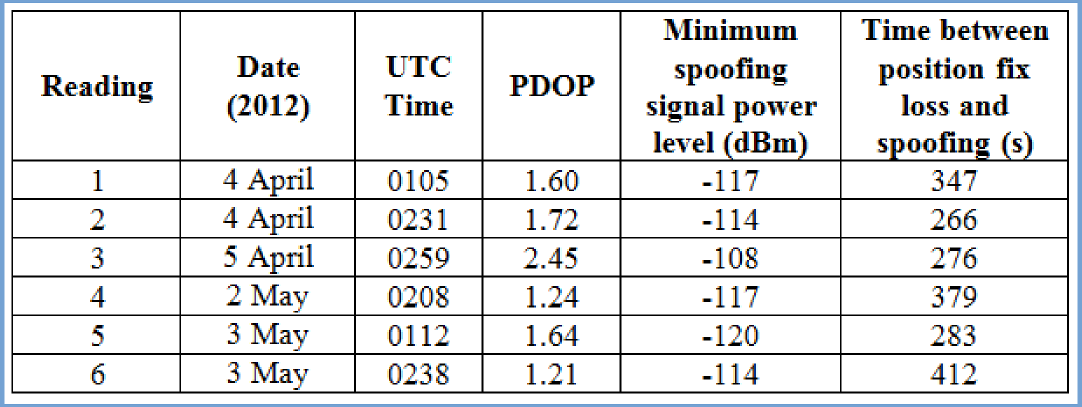
The effect of GPS spoofing attacks

Evaluated GPS receiver



Reading	Date (2012)	UTC Time	PDOP	Minimum spoofing signal power level (dBm)	Time between position fix loss and spoofing (s)
1	29 March	0104	1.72	-108	11
2	29 March	0240	1.72	-123	3
3	3 April	0105	1.62	-114	91
4	3 April	0234	1.72	-120	59
5	2 May	0108	1.47	-111	156
6	2 May	0244	1.27	-111	52

Reference GPS receiver



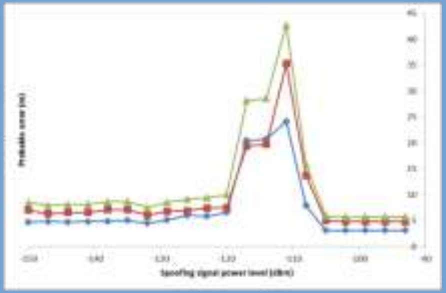
Reading	Date (2012)	UTC Time	PDOP	Minimum spoofing signal power level (dBm)	Time between position fix loss and spoofing (s)
1	4 April	0105	1.60	-117	347
2	4 April	0231	1.72	-114	266
3	5 April	0259	2.45	-108	276
4	2 May	0208	1.24	-117	379
5	3 May	0112	1.64	-120	283
6	3 May	0238	1.21	-114	412

STRIDE

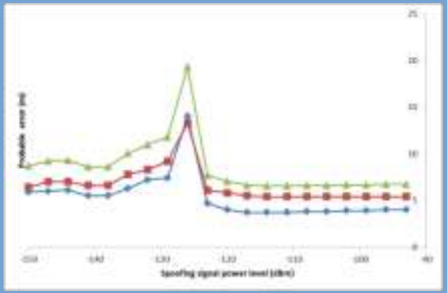
GPS Spoofing Tests

The effect of spoofing on GPS accuracy

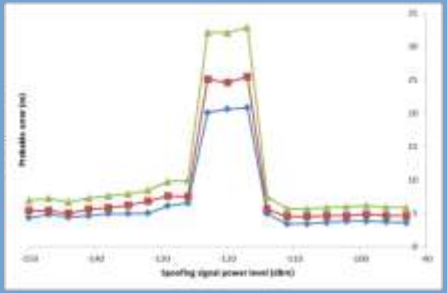
Evaluated GPS receiver



Reading 1

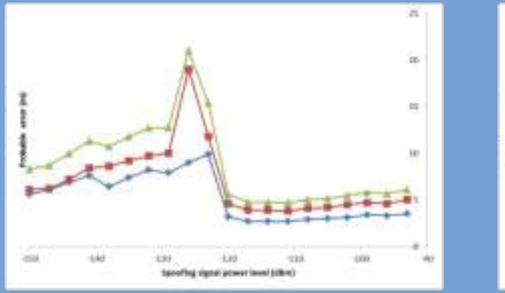


Reading 2

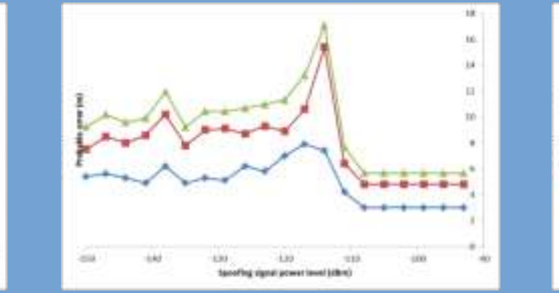


Reading 3

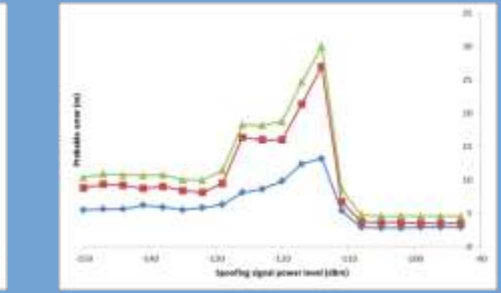
◆ HPE ■ VPE ▲ EPE



Reading 4



Reading 5



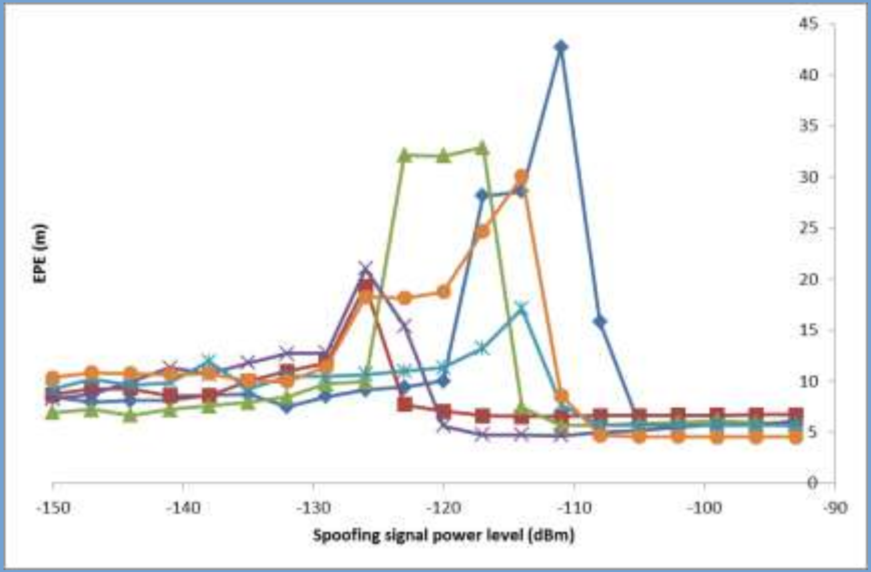
Reading 6

STRIDE

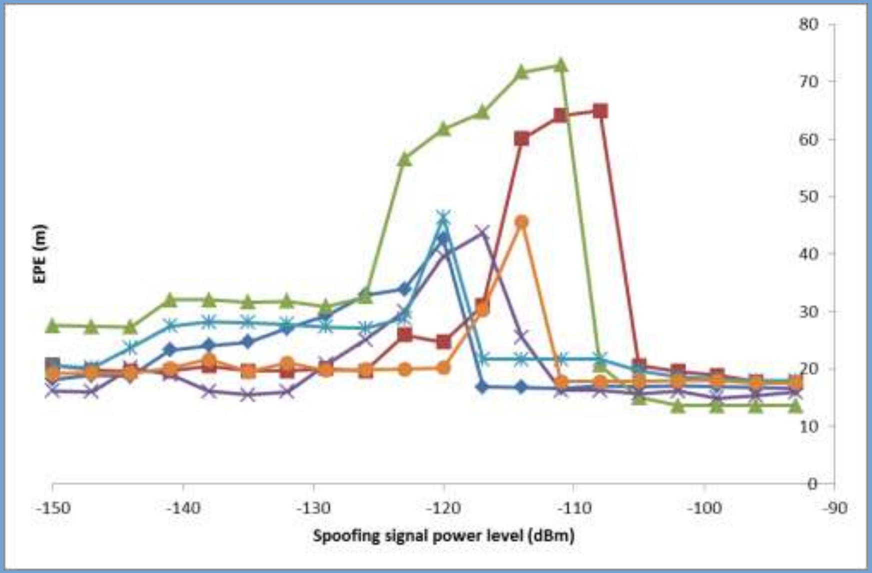
GPS Spoofing

The effect of spoofing on GPS accuracy

Evaluated GPS receiver



Reference GPS receiver



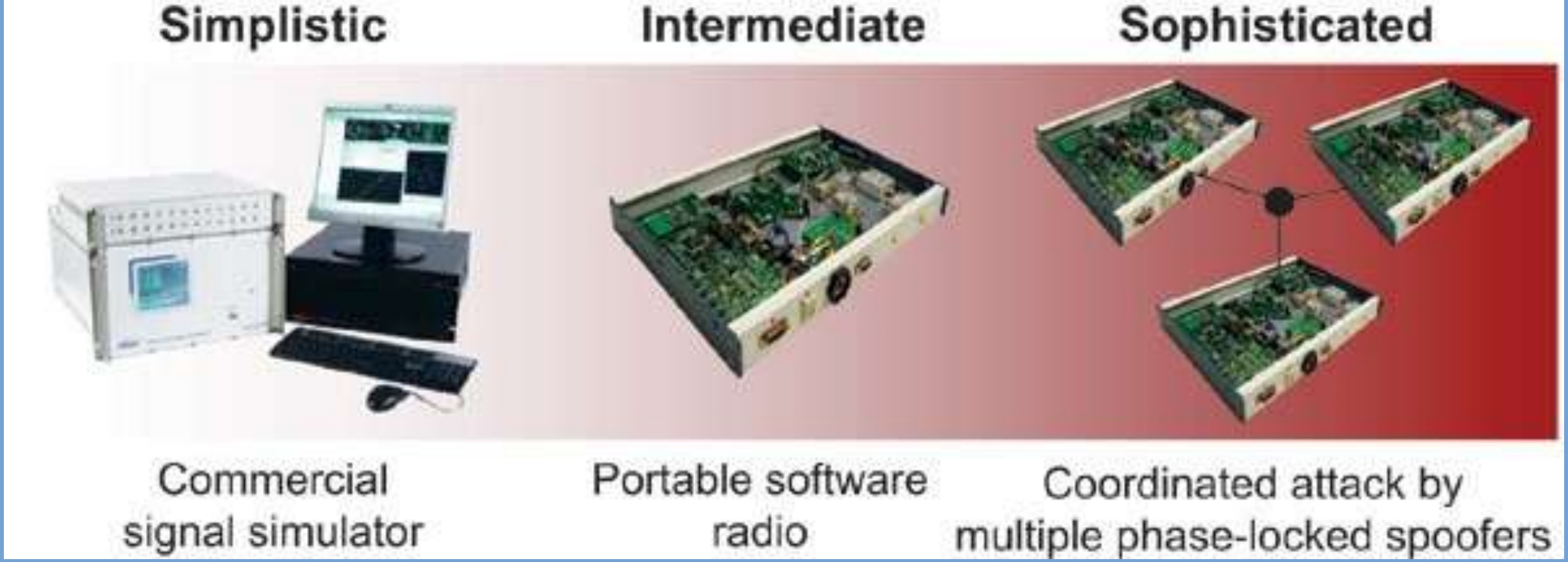
GPS Spoofing

- Characteristics of simplistic GPS spoofing:
  - Spoofing signal comes from a single direction
  - GPS receiver temporarily loses position fix lock before being taken over by the spoofing signal
  - Increased carrier-to-noise density (C/N_0) levels, resulting in improved accuracy.
- Rudimentary counter-spoofing measures:
  - Angle-of-arrival discrimination
  - Loss of lock notification
  - Notification of increase in C/N_0 levels and accuracy
- Many of present GNSS receivers are not equipped with such measures, and hence, are vulnerable to simplistic spoofing attacks.

STRIDE

GPS Spoofing

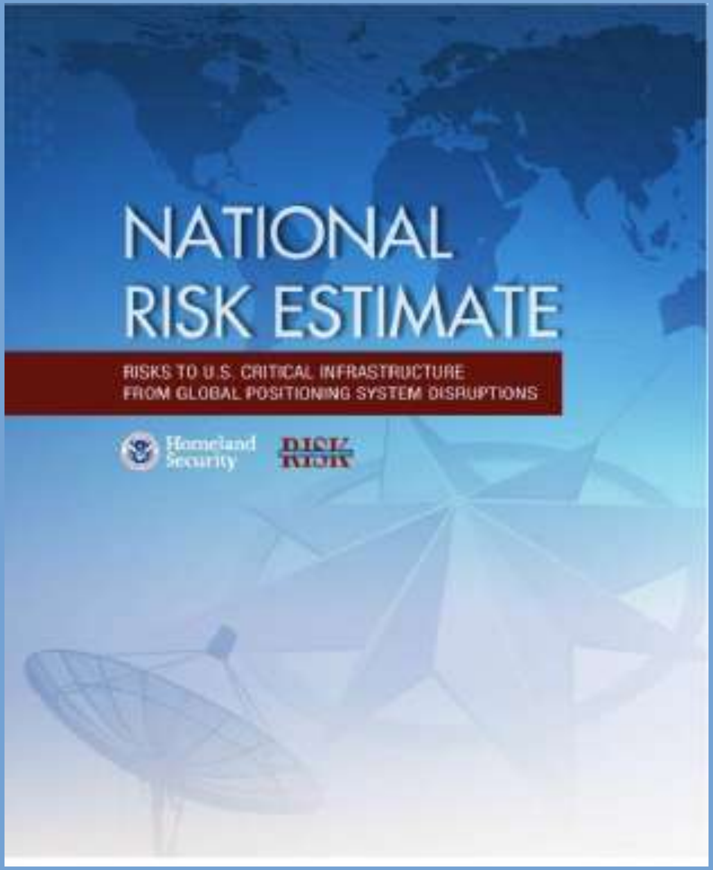
The spoofing threat continuum


Simplistic
Intermediate
Sophisticated
Commercial signal simulator
Portable software radio
Coordinated attack by multiple phase-locked spoofers

- Simplistic spoofing attacks are easily detectable due to poor synchronisation between genuine and spoofing GNSS signals
- Intermediate and sophisticated spoofing are much harder to detect as spoofing signals are synchronised with genuine signals

STRIDE

GNSS Jamming & Spoofing



NATIONAL RISK ESTIMATE

RISKS TO U.S. CRITICAL INFRASTRUCTURE FROM GLOBAL POSITIONING SYSTEM DISRUPTIONS

Homeland Security

RISK

Jamming disruptions are more likely than spoofing incidents - but the latter are of " higher consequence“.

Conclusion

- While any GNSS receiver evaluation should encompass field tests, such tests have limitations in terms on anticipating and controlling the various error parameters as well as inability to repeat the test scenarios.
- In contrast, GNSS simulation provides advantages of repeatability, allowing for specific test scenarios to be applied repeatedly with varying user-controlled parameters.
- In addition, these evaluations are conducted in tightly controlled environments to eliminate factors that could influence the repeatability of the tests.
- Hence, a complete evaluation of GNSS receivers should encompass both field tests and GNSS simulation.

STRIDE

Presentation Outline

- Review of activities conducted on vulnerabilities of GPS to:
  - Radio frequency interference (RFI)
  - Simplistic spoofing
  - Static multipath
  - GPS satellite clock error
  - Power consumption
  - Speed measurement
- Future research direction (RMK11):
  - Intermediate spoofing
  - Dynamic multipath
  - Ionospheric and troposheric delays
  - Extension to other GNSS systems; GLONASS, BeiDou and Galileo

Output: 2009-2015

Publications	
Journals	15
Conferences	10
Presentations	7
Periodicals	2
Workshops	2

GPS Test & Evaluation Facilities
Accuracy assessment (static and dynamic)
Radio frequency interference (RFI)
Simplistic spoofing
Static multipath
GPS satellite clock error

Human Capital Development	
Master	2
Industrial trainees	10

STRIDE

GPS Functional Tests

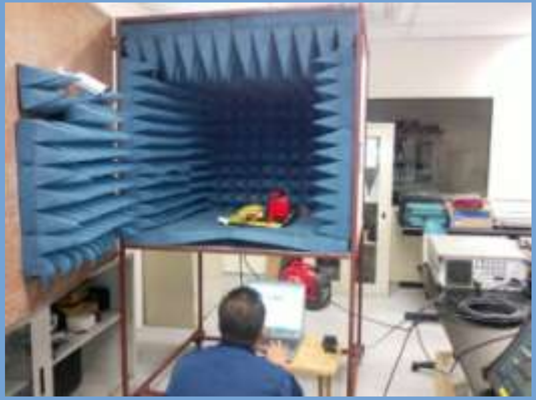
Pendulum Instruments GPS-12R

Magellan Z-Max

Trimble Geoexplorer 6000 GeoXH, Nomad 900G and Juno SB

Topcon Hiper GA

Trimble R8



ProMark 200

STRIDE

Research Collaborations

- Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Static Observations (2012)
  - Collaboration with the Faculty of Architecture, Planning and Surveying (FSPU), Universiti Teknologi MARA (UiTM)
  - Project Co-Leaders:
    - Assoc. Prof. Sr. Dr. Azman Mohd Suldi
    - Mr. Ahmad Norhisyam Idris

- Power Efficient Global Positioning System (GPS) Receiver Design (2014)
  - Collaboration with the Department of Computer and Communication Systems Engineering, Universiti Putra Malaysia (UPM)
  - Project Co-Leaders:
    - Dr. Fakhrul Zaman Rokhani
    - Mr. Fawaz Mohamed Jumaah

THANK YOU