SCIENCE & TECHNOLOGY RESEARCH INSTITUTE
FOR DEFENCE
MINISTRY OF DEFENCE
STRIDE

Evaluating Global Positioning System (GPS) Adjacent-Band Compatibility via 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

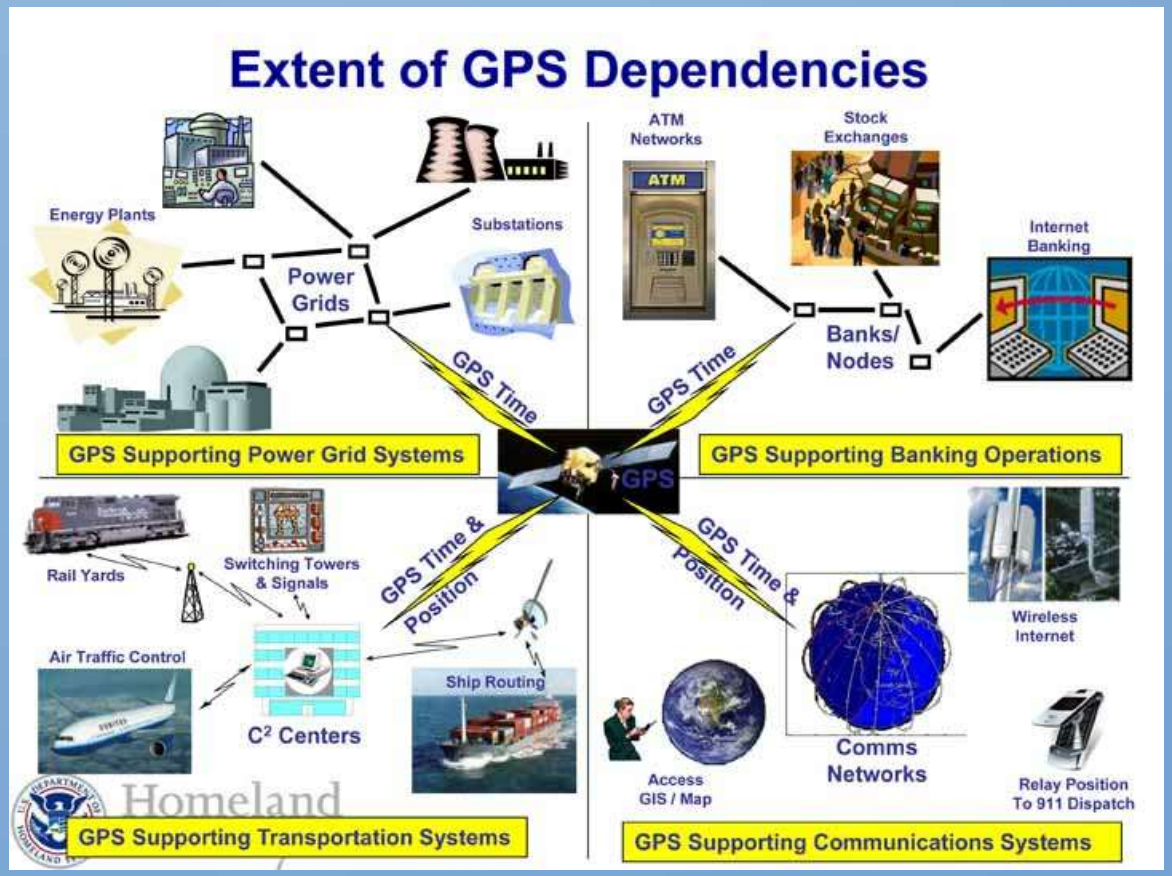
FOC: Full operational capability

STRIDE

Introduction

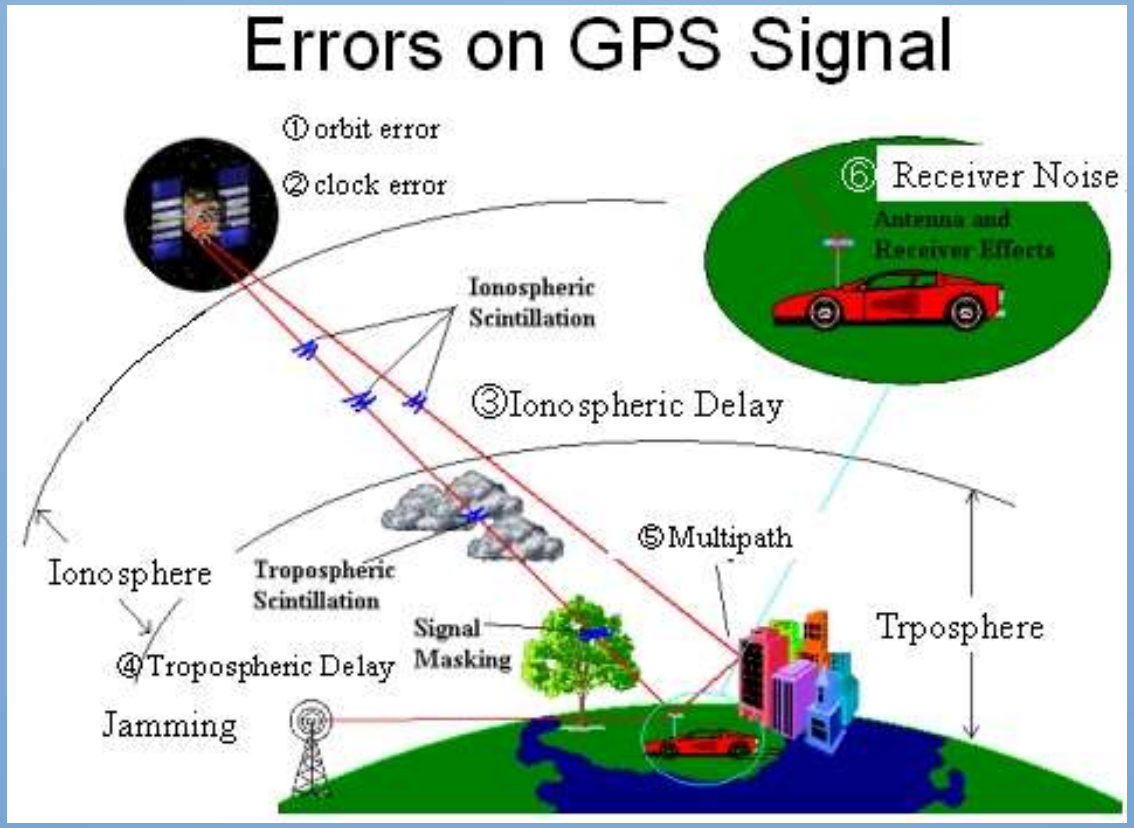
Increasing use for PNT applications:

- ♦Positioning
- ♦Navigation
- ♦Timing



STRIDE

GNSS Vulnerabilities



Source: IranMap.com

STRIDE

GNSS Jamming

Report estimates cost of disruption to GPS in UK would be £1bn per day

Err, maybe it's time for backup?

By Kat Hall 19 Jun 2017 at 08:37 SHARE

The UK stands to lose £1bn per day in the event of a major disruption to the Global Positioning System (GPS), according to a government report

Emergency services would also be severely affected and struggle to cope with demand. Longer emergency calls, less efficient dispatch, navigation, and congested roads would mean a total estimated loss of £1.5bn, the report said.

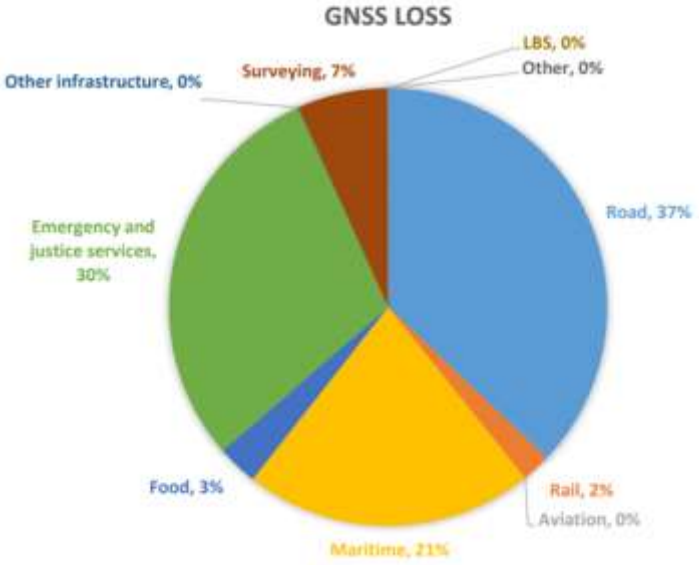
Besides navigation, many industries are reliant on GPS software for swathes of critical applications such as financial trading and precision docking of oil tankers.

Economic impact to the UK of a disruption to GNSS

Showcase Report

April 2017

LE London Economics



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.

STRIDE

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	Evaluation of the Effect of Global Positioning System (GPS) Antenna Orientation on GPS Performance	Internal	October 2015 – August 2016
8	Evaluation of Global Positioning System (GPS) Adjacent Band Compatibility via GPS Simulation	Internal	October 2016 - Current
9	Simulation and Modelling of Global Navigation Satellite System (GNSS) Vulnerabilities	Proposed for RMK11	January 2016 – December 2019

STRIDE

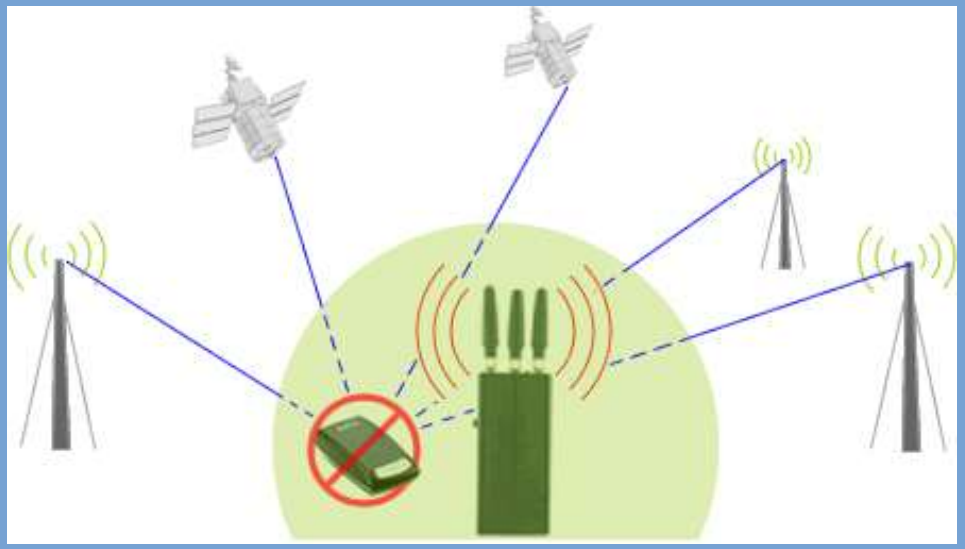
Presentation Outline

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

STRIDE

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 bought online

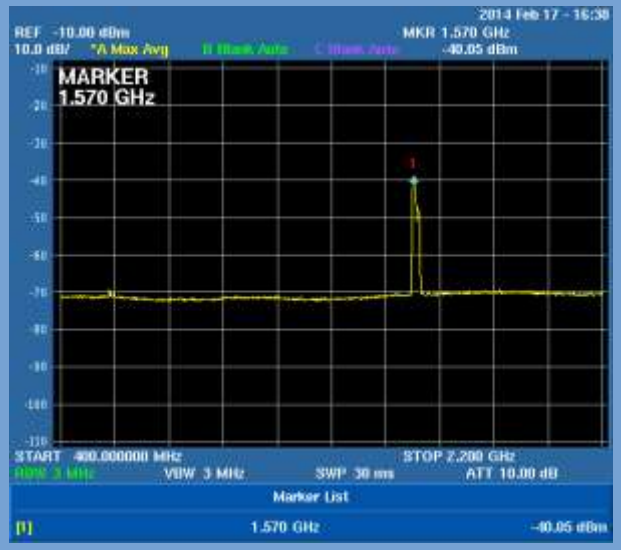
Given jamming radius: 5 - 10 m

Peak received signal at 3 m: -40.05 dBm

Transmitted power: -14.14 dBm (0.04 W)

Jamming radius (-80 dBm): 29.82 m

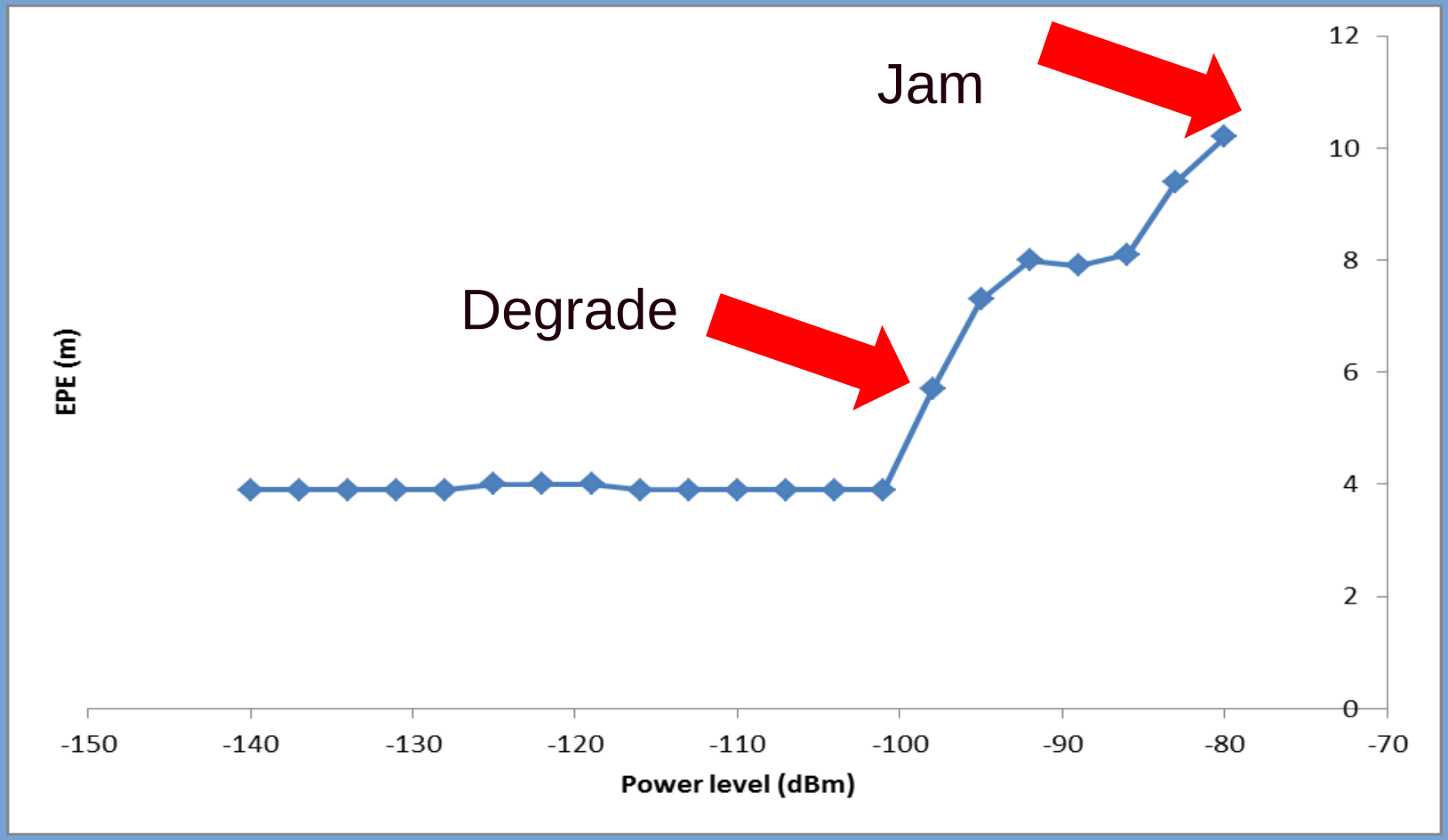
Degradation of accuracy (-105 dBm): 530.42 m



STRIDE

Results & Discussion

Kajang, UTC 0000, 2 MHz, -130 dBm, 1575.42 dBm



STRIDE

GNSS Jamming

GPS jammer bought online

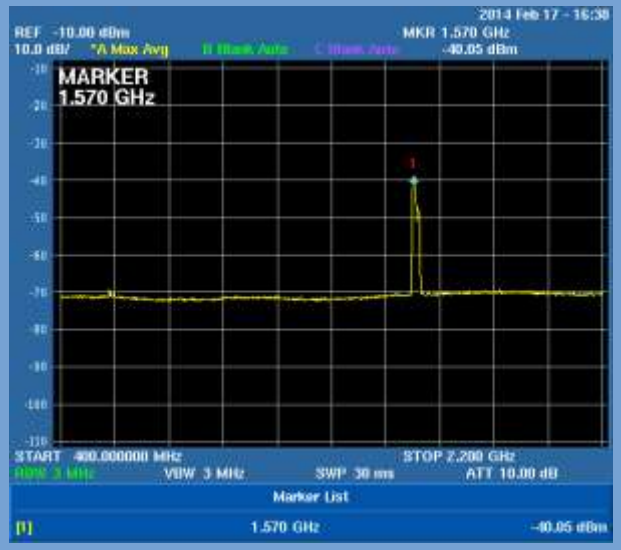
Given jamming radius: 5 - 10 m

Peak received signal at 3 m: -40.05 dBm

Transmitted power: -14.14 dBm (0.04 W)

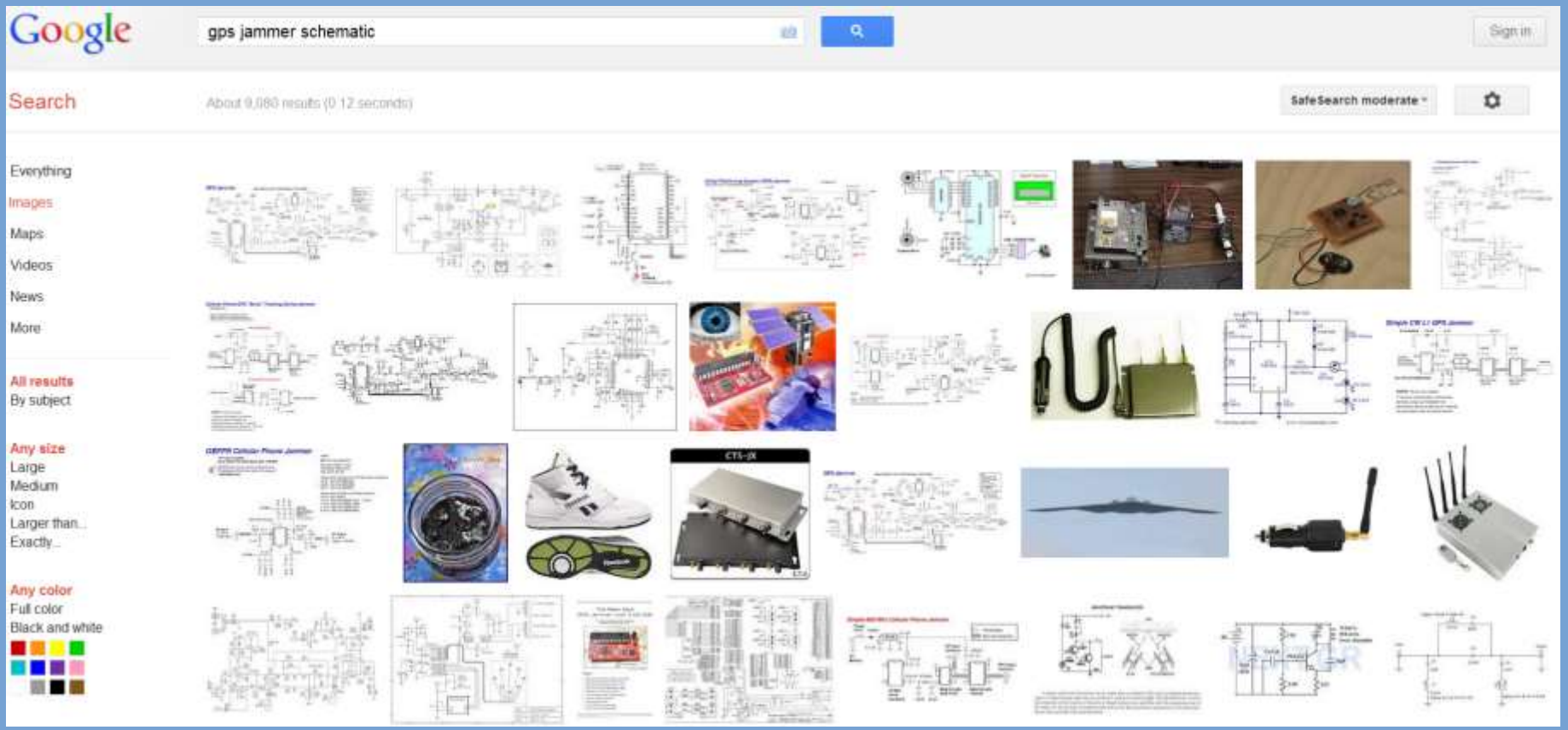
Jamming radius (-80 dBm): 29.82 m

Degradation of accuracy (-105 dBm): 530.42 m



STRIDE

GNSS Jamming



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 Communications Commission (FCC). When the problem persisted for another month, we launched an effort at the local level to determine the cause of the jamming.

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.

Moss Landing is a moderate-sized harbor about 180 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.

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.

Locations of the RFI emitter and MBARI power plant upper right

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

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 Bureau Chief Ilindel 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 as 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, Garmin 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 the 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 Typos, 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 Blizard, the commander of the USCG Center of Excellence for Navigation (NAVCEN), including GPS. Captain Blizard 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

GNSS Jamming

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 *Elevtheros 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.

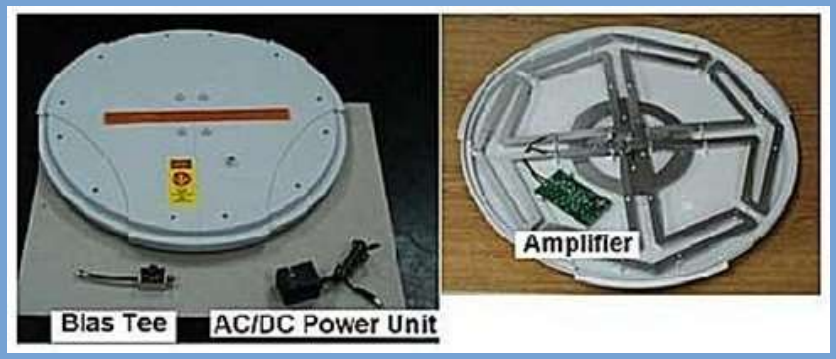
In August 2000 the Greek government sponsored a tank competition at Litokhoro to determine the Greek army's next tank—a deal worth $1.4 billion for 250 tanks. Competitors included the British Challenger 2E, the US M1A1 Abrams, the German Leopard 2A5 and the French Leclerc. During the trials, the British 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?

STRIDE

GNSS Jamming

April – May 2001: GPS coverage in Moss Landing, California, was severely disrupted by poorly designed television amplifiers



STRIDE

GNSS Jamming

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 Blizard, the commander of the USCG Center of Excellence for Navigation (NAVCEN), including GPS. Captain Blizard 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

GNSS Jamming

Demonstrating the effects of GPS jamming on marine navigation

Professor David Last
Dr Alan Grant
Dr Nick Ward

3rd GNSS Vulnerabilities and Solutions Conference
Baska, Croatia 5-8 September 2010

Abstract

The paper presents the results of trials that explore the sensitivity of a ship's GPS receiving systems to GPS jamming, especially at very low jamming power levels. The results include the production of Hazardously Misleading Information, multiple alarms and the simultaneous failure of many on-board systems. The vulnerable elements include the ship's radar, gyro-compass and Automatic Identification System, the very systems on which navigation may depend under conditions of low visibility.

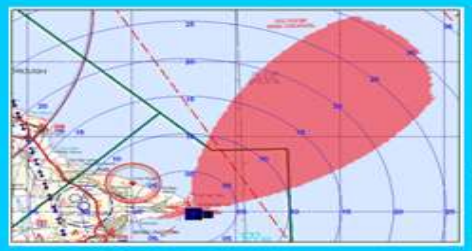
Introduction

GPS position information is now at the heart of our distribution industries, just-in-time manufacturing, emergency service operations, even mining, road-building and farming. GPS also provides the high-precision timing that keeps telephone networks, the Internet, banking transactions and even some electric power systems on line. Quietly, positioning, navigation and timing have become essential elements of the critical infrastructure of our nations. Lose them, and we are potentially in a dark, silent and dangerous world!

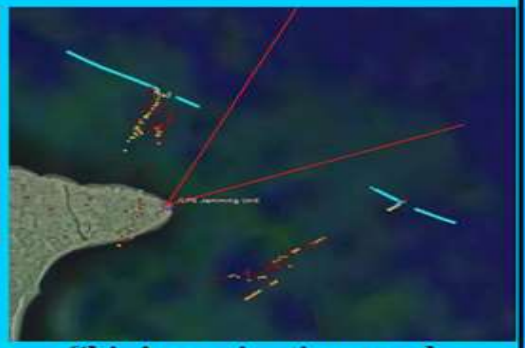
Let us focus on the use of satellite navigation at sea. GPS is at the heart of the integrated bridges and electronic chart displays on vessels that give one man finger-tip control of a 100,000 tonne ship, at 25 knots. Yet often such vessels depend for their navigation essentially on GPS alone. Many professionals in the world of transport act as if GPS were infallible and simply cannot see what is unsafe about navigating a ship

General Lighthouse Authorities of the UK & Ireland (GLAs)

Flamborough GPS Jamming Trials

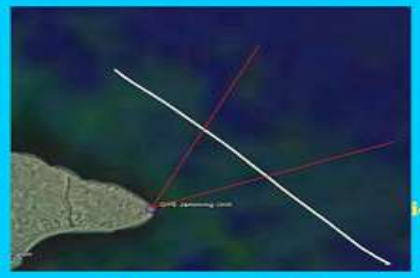


Jamming zone



Ship's navigation track

Pictures: www.gla-rcuav.org/pdfs/GPS_Jamming_and_the_impact_on_maritime_navigation.pdf



Flamborough trial:
White track: eLoran through jamming

Galatea Trial
Green marker: eLoran
Blue marker: erroneous GPS

Pictures: www.gla-rcuav.org/pdfs/GPS_Jamming_and_the_impact_on_maritime_navigation.pdf

STRIDE

GNSS Jamming

GPS disruption a full-fledged aviation problem

March 6, 2017 - By Guy Buesnel and Paul Crampton

Facebook Twitter Google LinkedIn 1 Comments

Several jamming incidents in 2016 highlight the increasing reliance on GNSS by commercial aviation and vulnerabilities of PNT-dependent devices and systems to real-world GNSS threats.

Notices to Airmen (NOTAMs) and other warnings to pilots and crews reported GPS signal jamming near major international airports. Aircraft approaching or flying over these airports were advised to avoid using RNAV technology to plan their approach or landing, due to the presence of GPS signal jamming.

The NASA Aviation Safety Reporting System (ASRS) database contains records of pilot-reported incidents, which rose from 11 in 2013 to 28 in 2015, and they continued to grow in 2016.

Simulator scenarios should include likely effects of interference on GNSS systems and devices, particularly for aviation.

STRIDE

GNSS Jamming

- In short:
  - GNSS jamming is easy to conduct
  - The source of jamming is difficult to detect
  - The effect of GNSS jamming can be severe

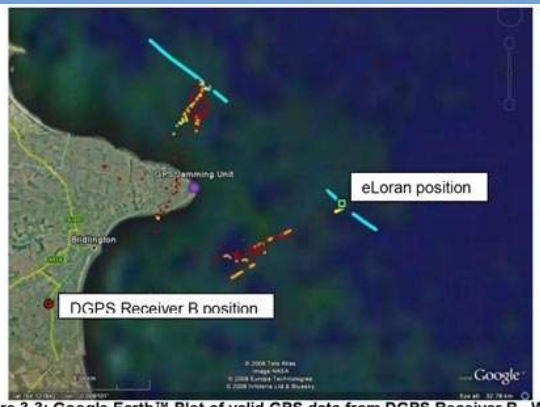
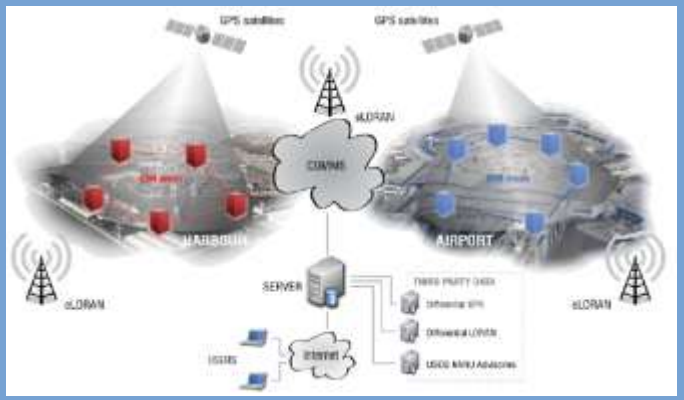


Figure 3-3: Google Earth™ Plot of valid GPS data from DGPS Receiver B. When comparing the reported position (red circle) against the eLoran position (green square) for the same time, one can see an error of 22Km with the reported DGPS Receiver B position being on land. (Colours indicate reported speed: blue <15knts, yellow< 50knts, orange <100knots and red >100knts)



STRIDE

GNSS Jamming

GPS anti-jam increasingly big business

August 29, 2016 - By Alan Cameron

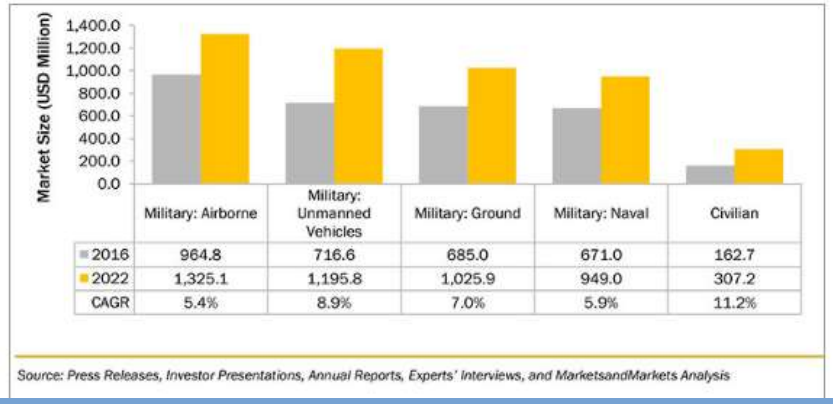
Facebook Twitter Google LinkedIn 0 Comments

It's getting bigger all the time, GPS/GNSS business. And coming along in its wake, starting to grow like a sproutly little brother, is GPS anti-jamming, to safeguard the signal in various scenarios.

The anti-jamming market for GPS is expected to reach US$4.8 billion in value and 309.2 thousand units in volume by 2022, according to a newly released report by Research and Markets, a Dublin, Ireland-based market research "store."

Anti-jam technology sales revenue will increase at a compound annual growth rate (CAGR) of 7.0 percent between 2016 and 2022, while volume goes up 10.1 percent. Major drivers at the moment lie in the military sector, but that could well change in the next decade. The proliferation of low-cost GPS jammers is seeing to that.

Meanwhile, any armed force that puts its faith in guided missiles now feels the acute need for a secured weapons system, something not easy to accomplish. Flight-control applications are especially vulnerable.



	Military: Airborne	Military: Unmanned Vehicles	Military: Ground	Military: Naval	Civilian
2016	964.8	716.6	685.0	671.0	162.7
2022	1,325.1	1,195.8	1,025.9	949.0	307.2
CAGR	5.4%	8.9%	7.0%	5.9%	11.2%

Source: Press Releases, Investor Presentations, Annual Reports, Experts' Interviews, and MarketsandMarkets Analysis

STRIDE

GPS Jamming

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

STRIDE

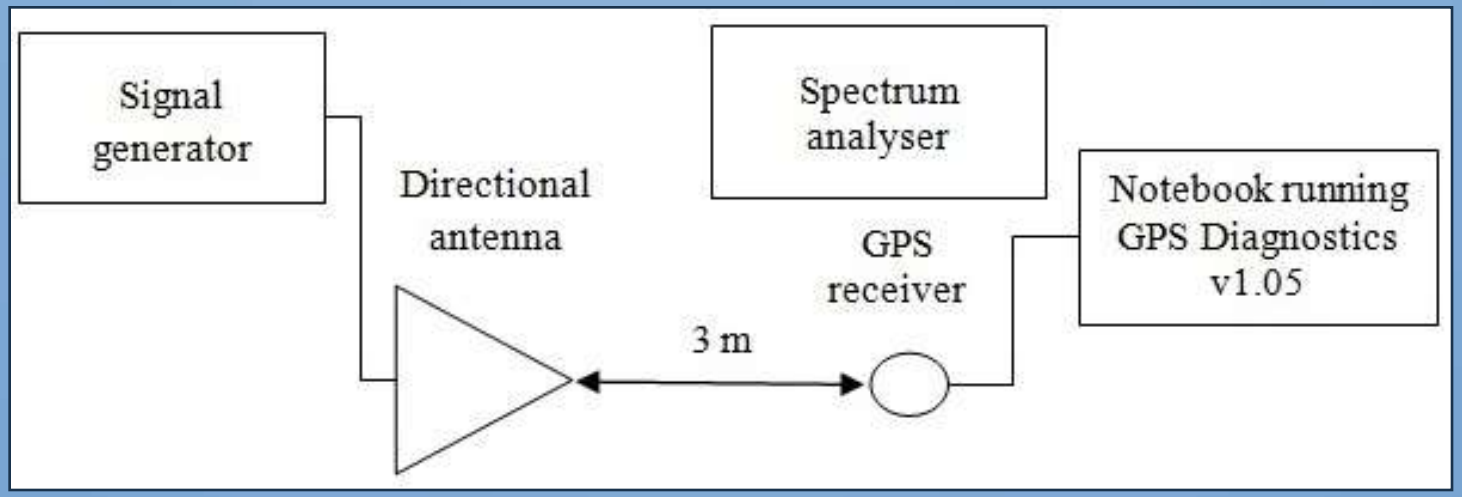
GPS Jamming

Test Site

STRIDE

GPS Jamming

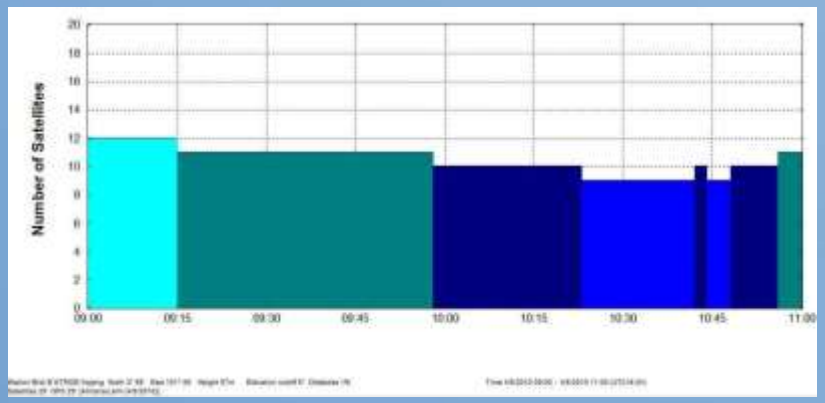
Test Setup



STRIDE

Field Evaluations

GPS Coverage Prediction
(Using Trimble Planning)



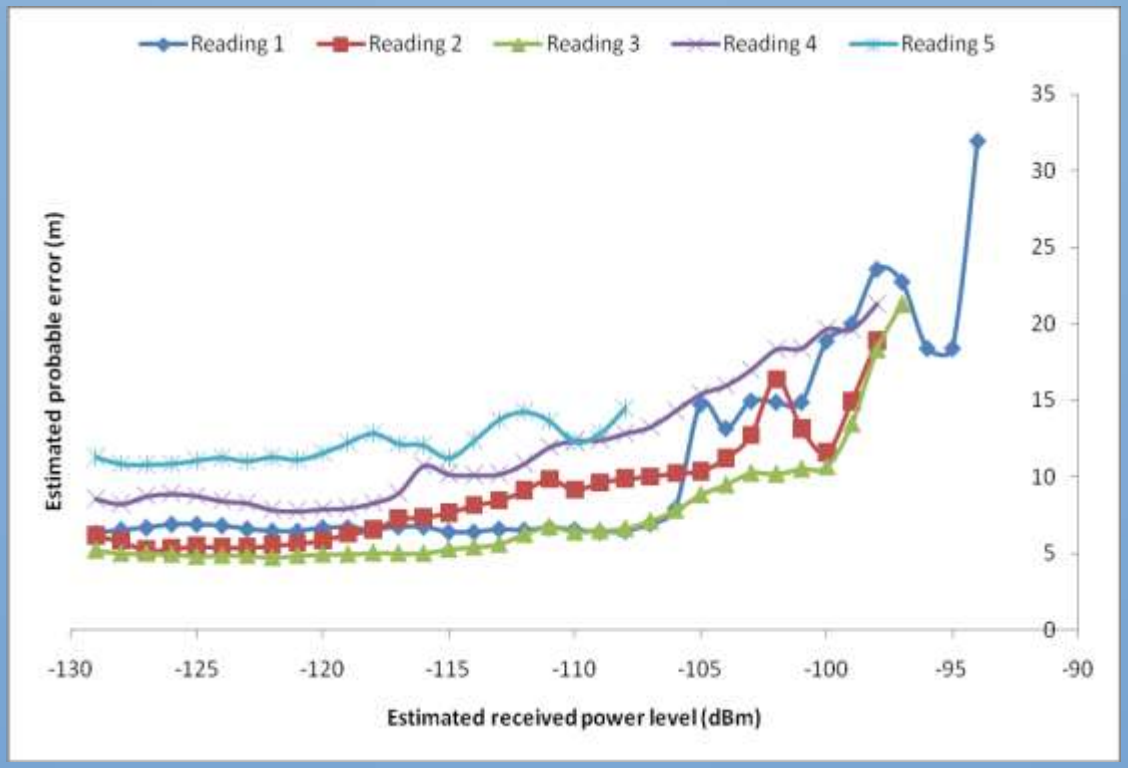
Satellite visibility

PDOP

STRIDE

GPS Jamming

Evaluation of the effect of RFI on GPS accuracy



STRIDE

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

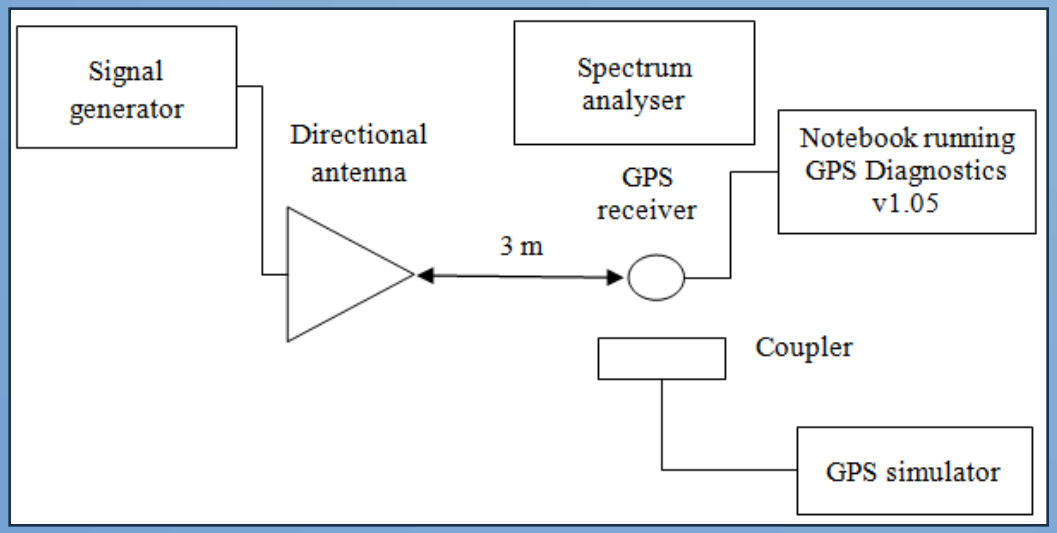
GPS Jamming

- 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

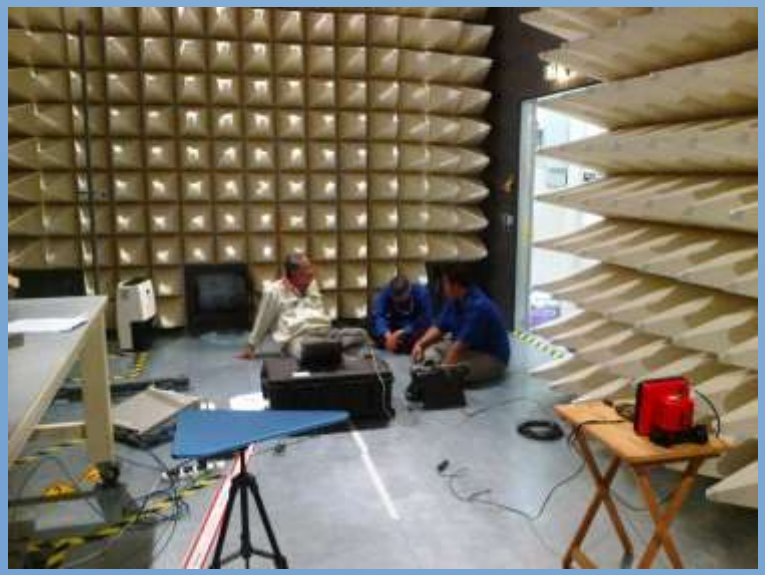
Test Scenarios

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

STRIDE

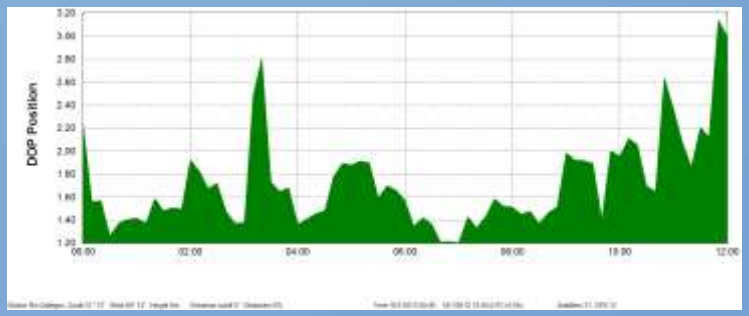
GPS Jamming

GPS coverage

Kajang

Denver

Cairns



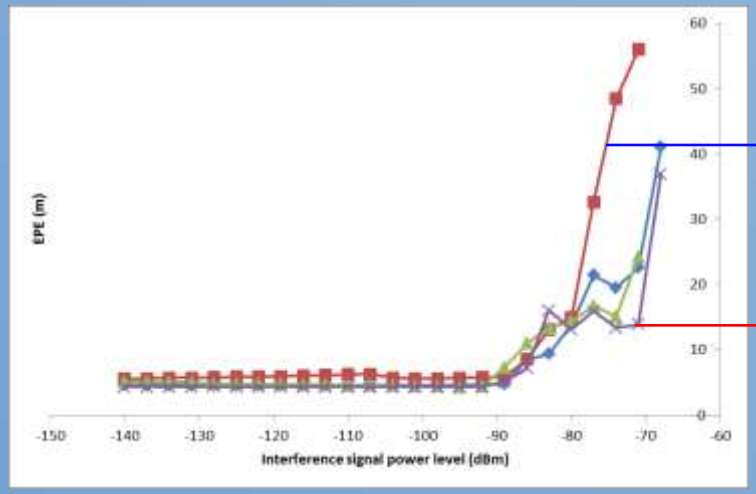
Rio Gallegos

STRIDE

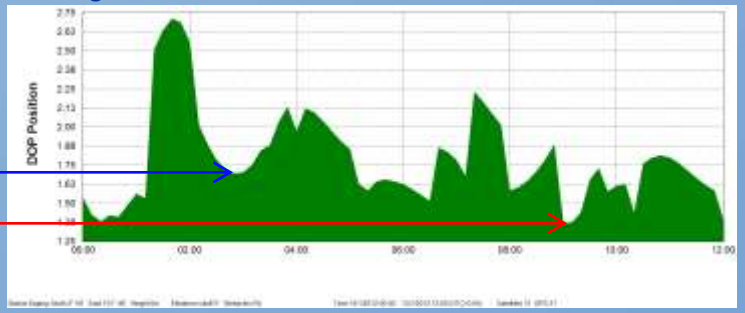
GPS Jamming

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

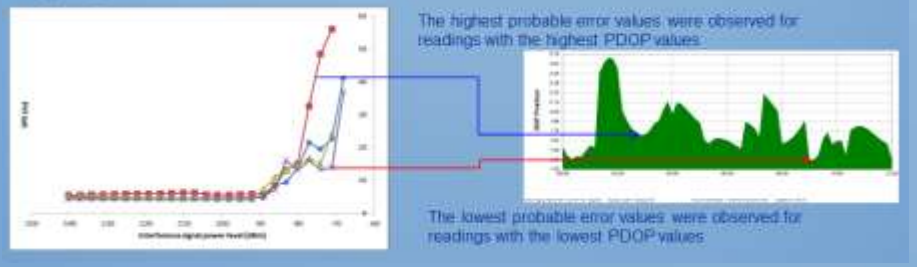
0000 UTC 0300 UTC 0600 UTC 0900 UTC

STRIDE

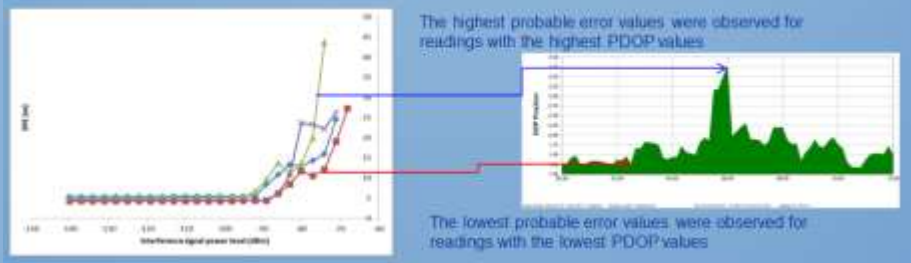
GPS Jamming

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

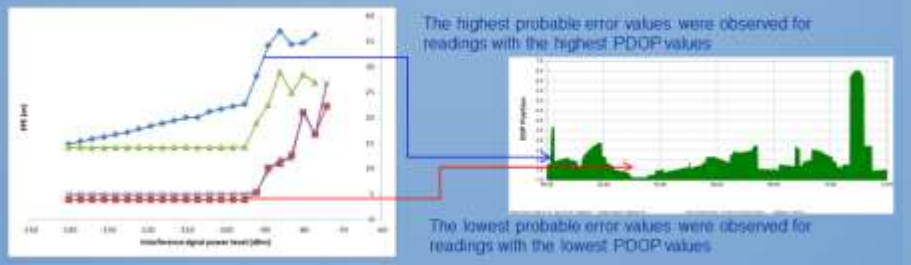
Kajang



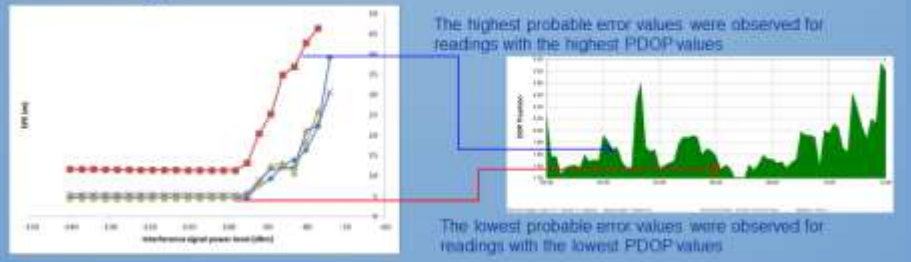
Denver



Cairns



Rio Gallegos



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

Adjacent-Band Compatibility

Intentional

(Deliberate)

The studies conducted thus far have been focused on in-band interference

Unintentional

(Accidental)

Adjacent-band interference signals at frequencies close to the GPS signal bandwidth can also disrupt the performance of GPS receivers

STRIDE

Adjacent-Band Compatibility

- Every radio signal, even though it operates in a specific portion of the spectrum, introduces interference into adjacent portions of the spectrum.
- The amount of interference that is permissible to seep over into adjacent spectrums is controlled in many countries by their respective communications commissions, but it is not possible to eliminate it completely.
- The higher the transmission power used, the higher the interferences will be in adjacent portions of the spectrum.
- Increasing usage of wireless devices has resulted in increased occurrences of adjacent-band interference for GPS receivers.

STRIDE

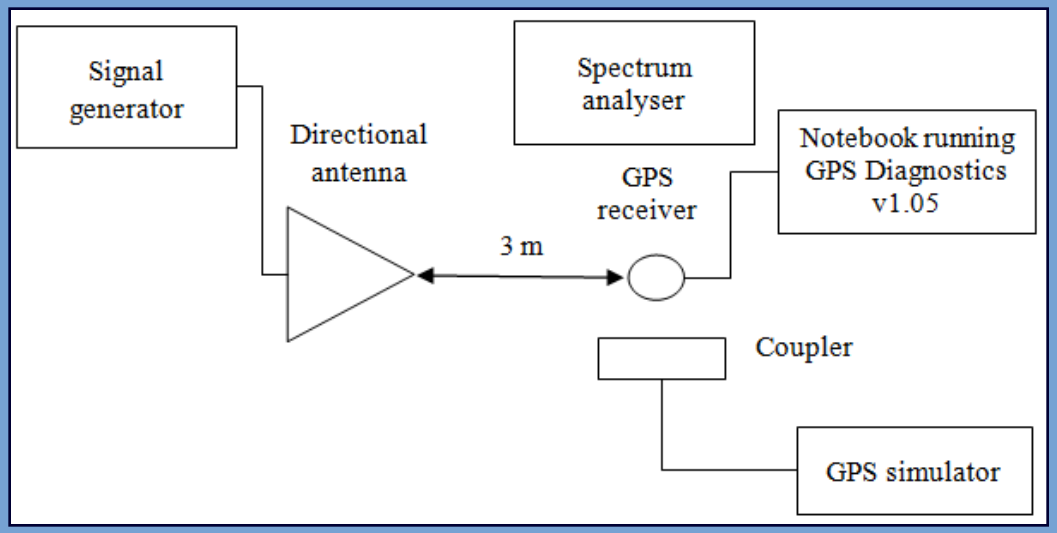
Objectives

- Evaluating the adjacent radio frequency band power levels that can be tolerated by the GPS L1 coarse acquisition (C/A) signal
- Advance understanding of the extent to which such power levels impact GPS performance

STRIDE

Methodology

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

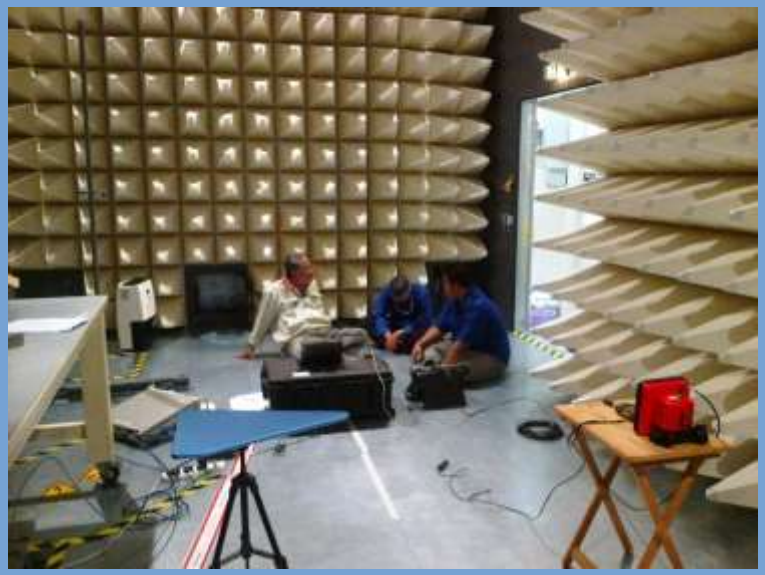
Test Scenarios

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:

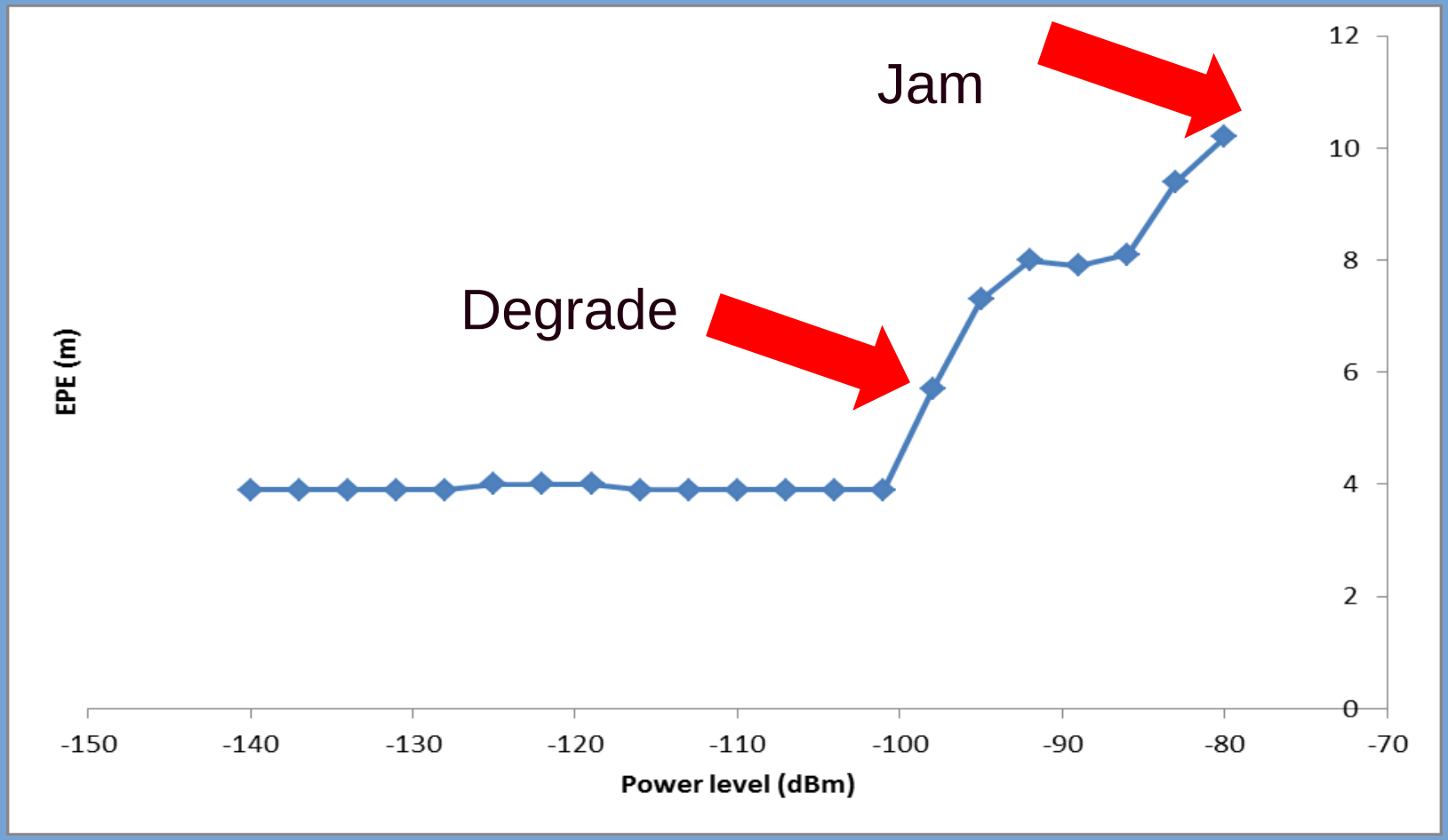
- -130 dBm
- -135 dBm
- -140 dBm
- -145 dBm

Interference signal frequencies of 1,475 to 1,675 MHz and bandwidhts of 2, 5, 10 and 20 MHz

STRIDE

Results & Discussion

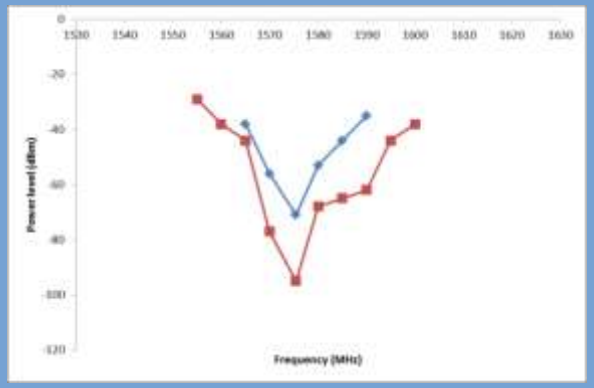
Kajang, UTC 0000, 2 MHz, -130 dBm, 1575.42 dBm



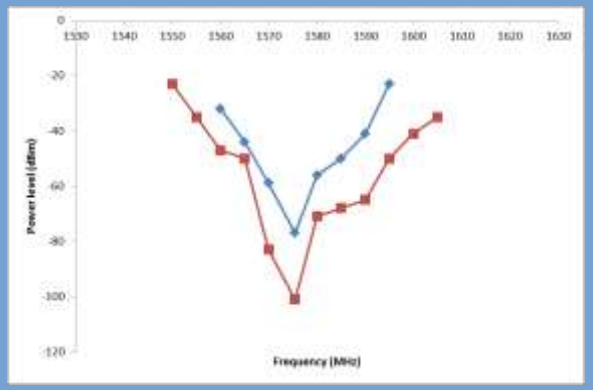
STRIDE

Results & Discussion

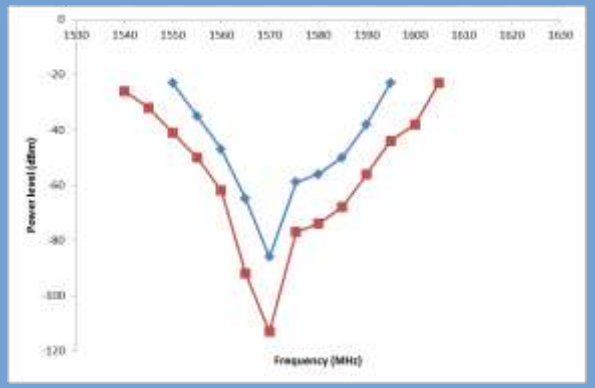
Kajang, UTC 0000, 2 MHz



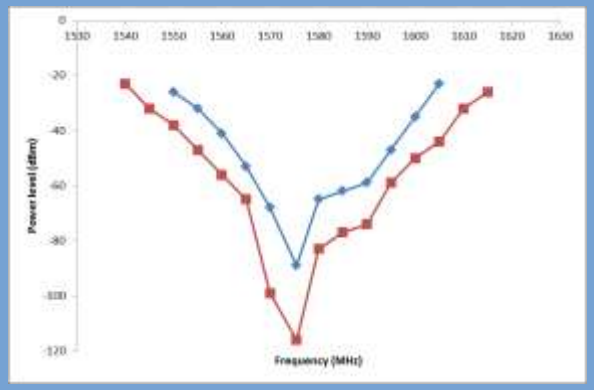
-130 dBm



-135 dBm



-140 dBm

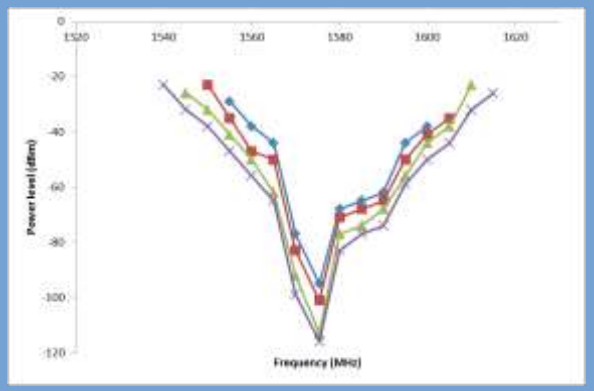


-145 dBm

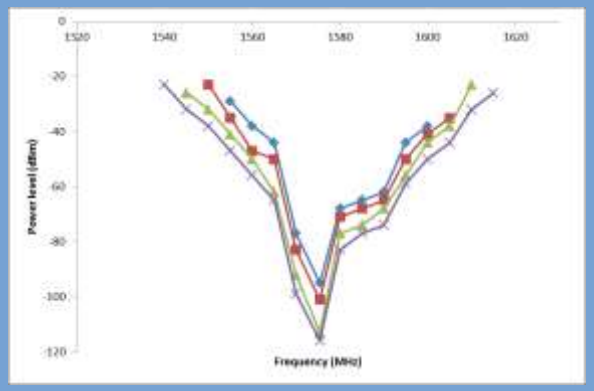
STRIDE

Results & Discussion

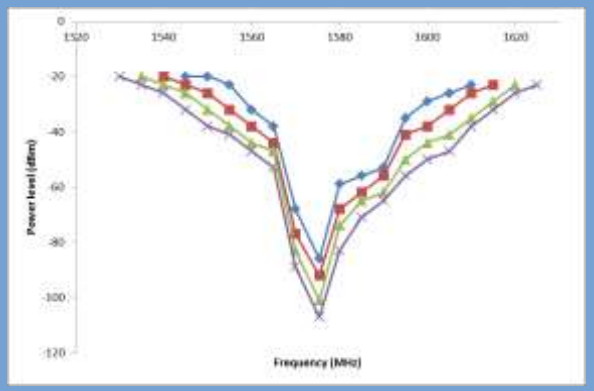
Kajang, UTC 0000



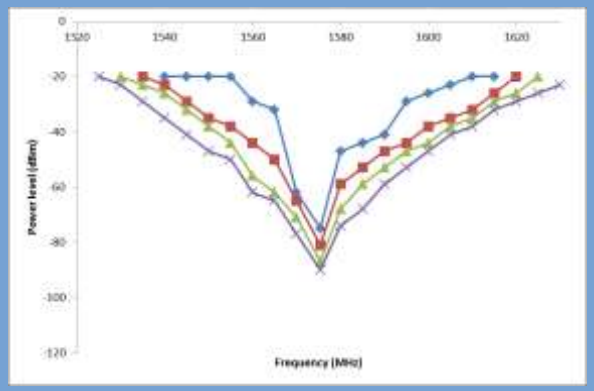
2 MHz



5 MHz



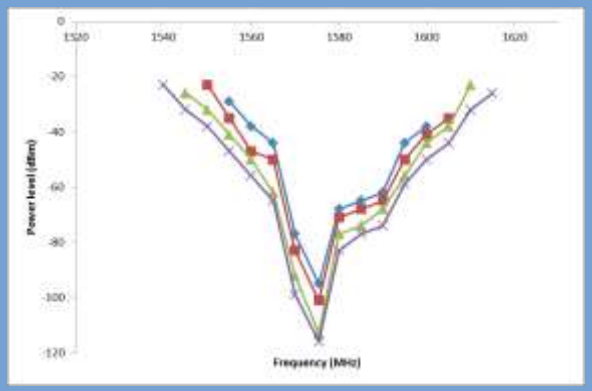
10 MHz



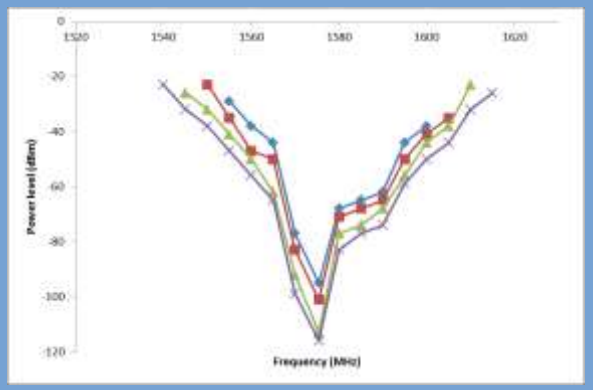
20 MHz

Results & Discussion

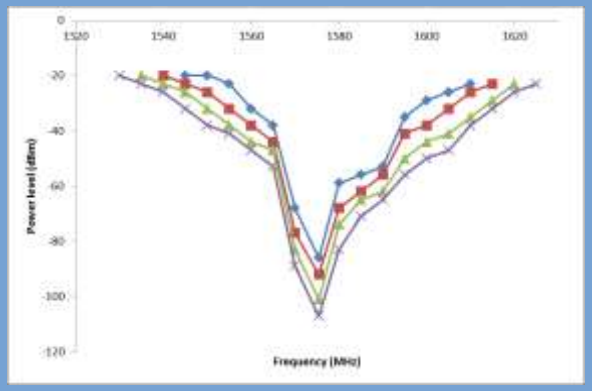
Kajang, UTC 0000



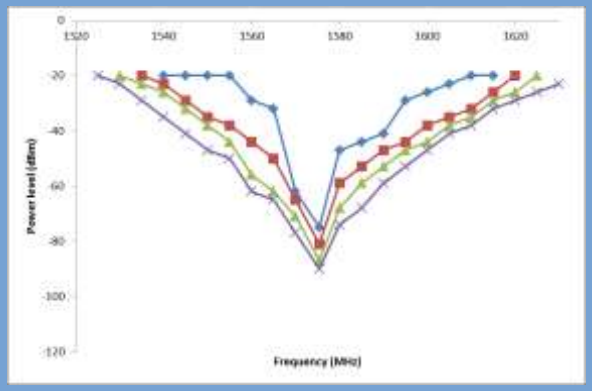
2 MHz



5 MHz



10 MHz



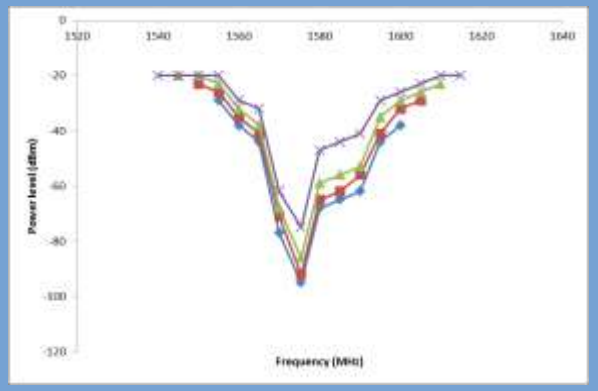
20 MHz

- Decreasing power levels of the GPS signal decrease the power levels and increase the range of frequencies of interference signals that affect the GPS signal.
- As the carrier frequency of the interference signals moves away from the frequency of the GPS (1575.42 MHz), the power levels required to affect the GPS signal increase.

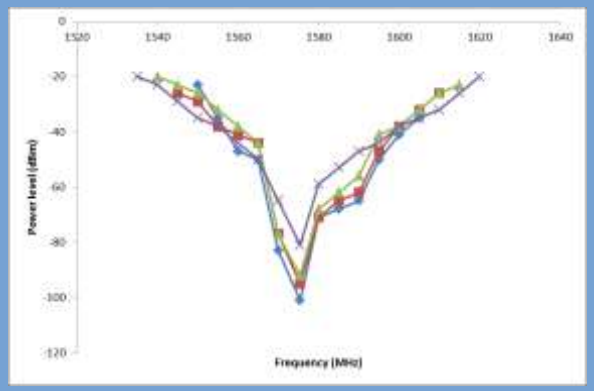
STRIDE

Results & Discussion

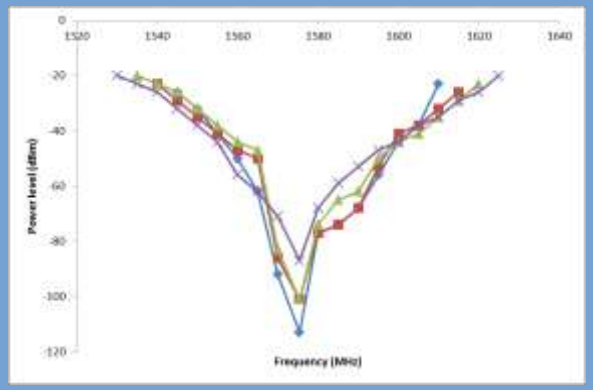
Kajang, UTC 0000



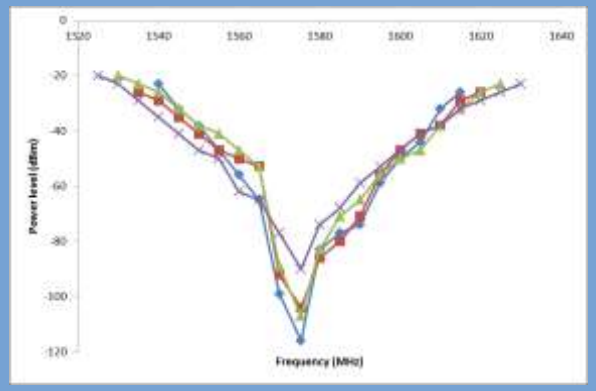
-130 dBm



-135 dBm



-140 dBm



-145 dBm

- Increasing bandwidth of interference signals:
  - Increases the range of frequencies that can affect GPS signal.
  - The power levels that affect GPS signal increase, as the interference signal's strength is dispersed over a wider bandwidth.

STRIDE

Conclusion

- The GPS L1 C/A signal is susceptible to adjacent band interference.
- Factors that affect the level of disruption include GPS signal power level, and carrier frequency and bandwidth of interference signals.
- Decreasing power levels of the GPS signal decreases the power levels and increases the range of frequencies of interference signals that affect the GPS signal.
- As the carrier frequency of the interference signals moves away from the frequency of the GPS signal (1575.42 MHz), the power levels required to affect the GPS signal increase.
- Furthermore, increasing bandwidths of interference signals increase the power level but increase the range of frequencies that can affect GPS signal.
- Further studies are required using a wider range of GPS signals, in particular L2C and L5, as well as other GNSS systems (GLONASS, BeiDou and Galileo), in order to develop appropriate GNSS spectrum interference standards.

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

STRIDE

GPS Functional Tests

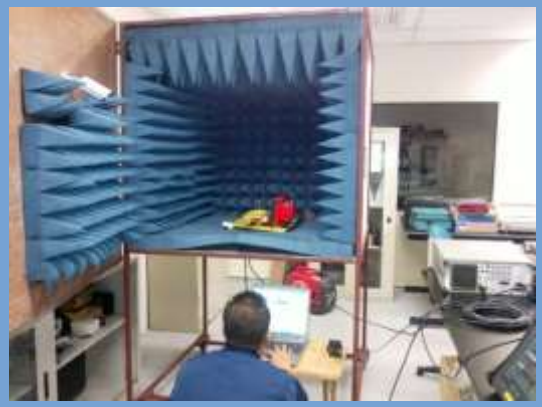
Pendulum Instruments GPS-12R

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