Airborne Networking for Augmented Positioning, Navigation and Timing

AIRBORNE NETWORKING SYMPOSIUM
31 January 2012

Alison Brown

NAVSYS Corporation

14960 Woodcarver Road

Colorado Springs, CO 80921

Phone: 719-481-4877

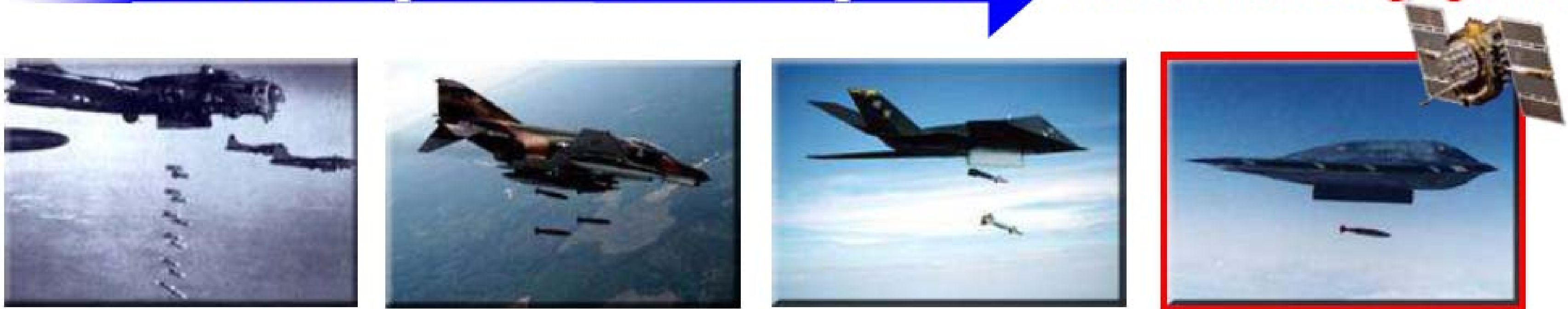
A Space Enabled Reconnaissance-Strike Complex: The New American Way of War

KTO, 1991	Unguided	245,000	92%
(Desert Storm): 37 Days	Laser/EO-guided	20,450	8%
1 Mbps/5K Forces			
Serbia, 1999	Unguided	16,000	66%
(Allied Force)	Laser/EO-guided	7,000	31%
78 Days; 24.5 Mbps/5K	GPS-guided	700	3%
Afghanistan, 2001-02	Unguided	9,000	41%
(Enduring Freedom)	Laser/EO-guided	6,000	27%
90 Days; 68.2 Mbps/5K	GPS-guided	7,000	32%
Iraq, 2003	Unguided	9,251	32%
(Iraqi Freedom)	Guided	19,948	68%
29 Days; 51.1 Mbps/5K			

GPS and Precision Strike

Fewer Sorties for a Greater Effect

Position, Navigation and Timing - GPS → **Precision Engagement**



1500 B-17 sorties	30 F-4 sorties	1 F-117 sortie	1 B-2 sortie
9000 bombs (250#)	176 bombs (500#)	2 bombs (2000#)	16 bombs (2000#)
One 60’ x 100’ target	One Target	Two Targets/Sortie	16 Targets/Pass
W.W.II	Vietnam	Desert Storm	All Weather

What is the threat to PNT?

- GPS Degradation
  - RF emitters can create areas where GPS signals are not available
- GPS Denial
  - Cyber attack could disable GPS control or spoof UE reception
- GPS Destruction
  - Anti-satellite (ASAT) attack

Commercial GPS Threat

- Designed to Block GPS and GSM signals
- Available for purchase over the Internet

- U.S. Communications Act prohibits blocking or interfering with radio communications
- FCC can fine up to $11K per device sold

GPS Spoofing Threat

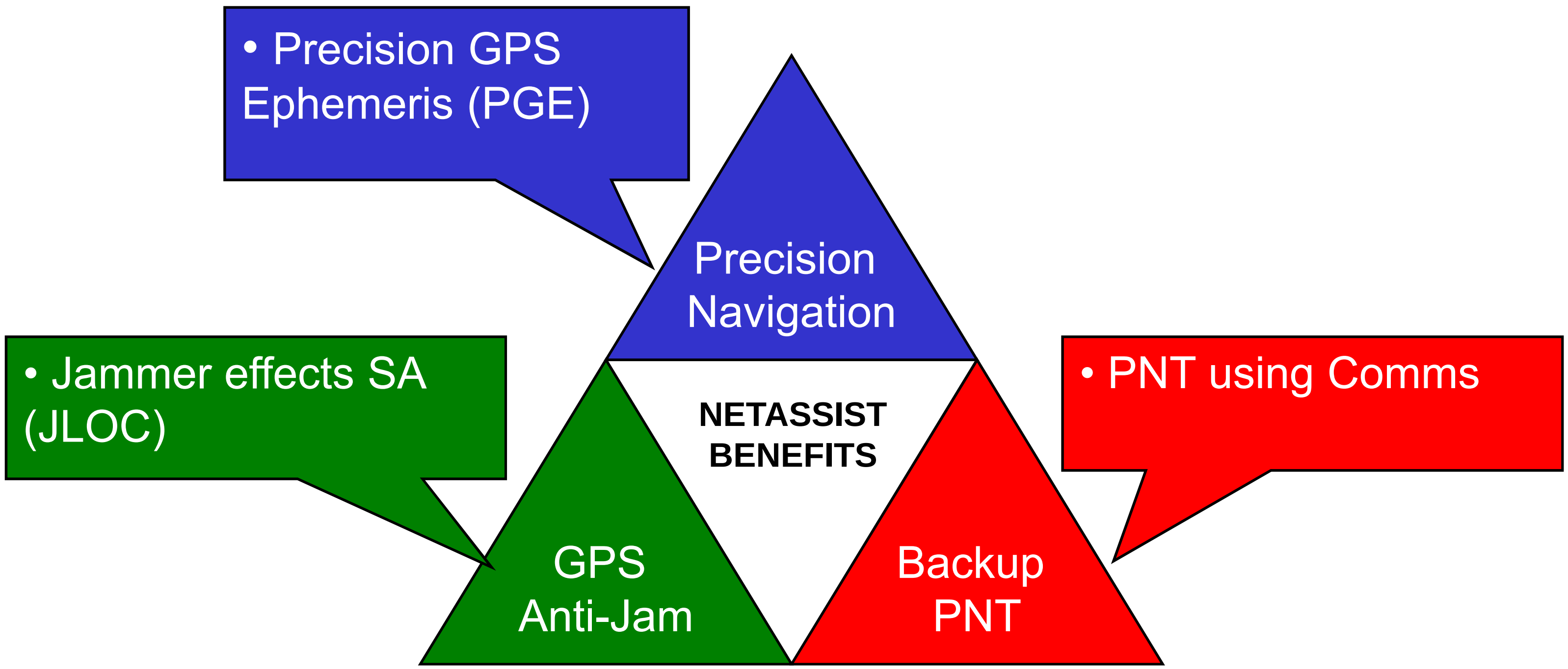
- Iranian engineer claimed US. drone “tricked” into landing in Iran by electronically hacking into its navigational weak spot and 'spoofing' its GPS system

RQ-170 seen on display in Iran

Takeaways from Schriever Wargames on GPS destruction

- "A day without space" will be years without space until we can constitute our air/space capability
- We must develop concepts of operation that assure continuity of mission operations in a variety of threat conditions
- We must train for contingencies and be able to fight through the threat to continue to provide capabilities (e.g. navigation without GPS)

Benefits of Network Assisted GPS for Military Users



5 deg Mask Angle

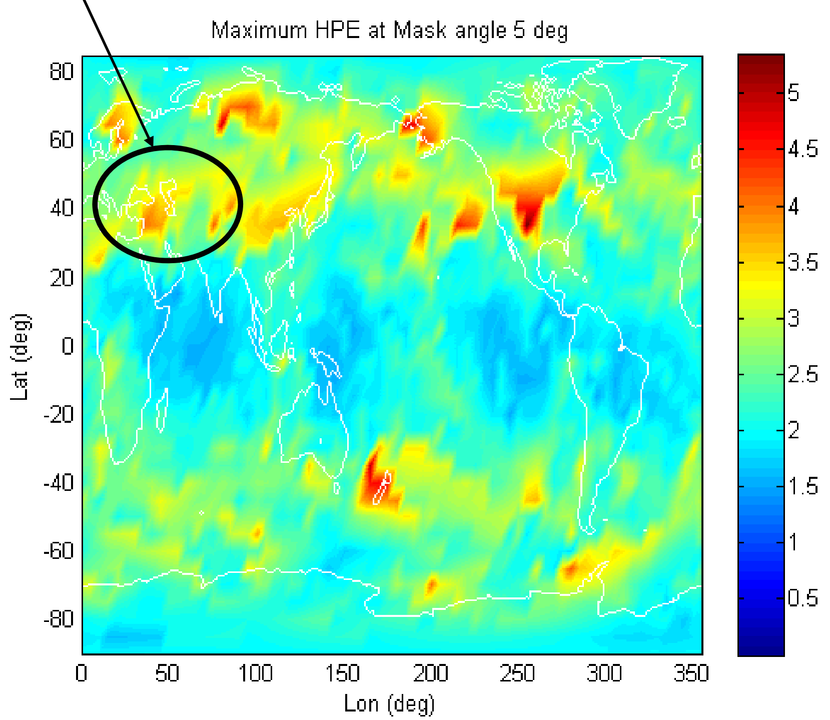
With PGE corrections < 1 m HPE, 1 m VPE
Without PGE corrections > 5 m HPE, 10 m VPE

Iraq / Afghan Theater

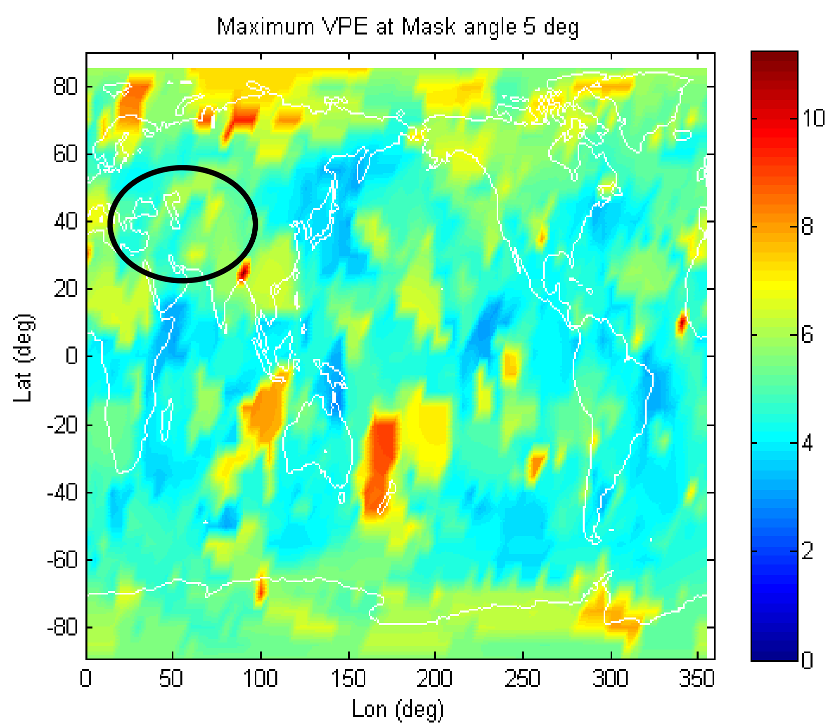
Horizontal

March 2010

Vertical



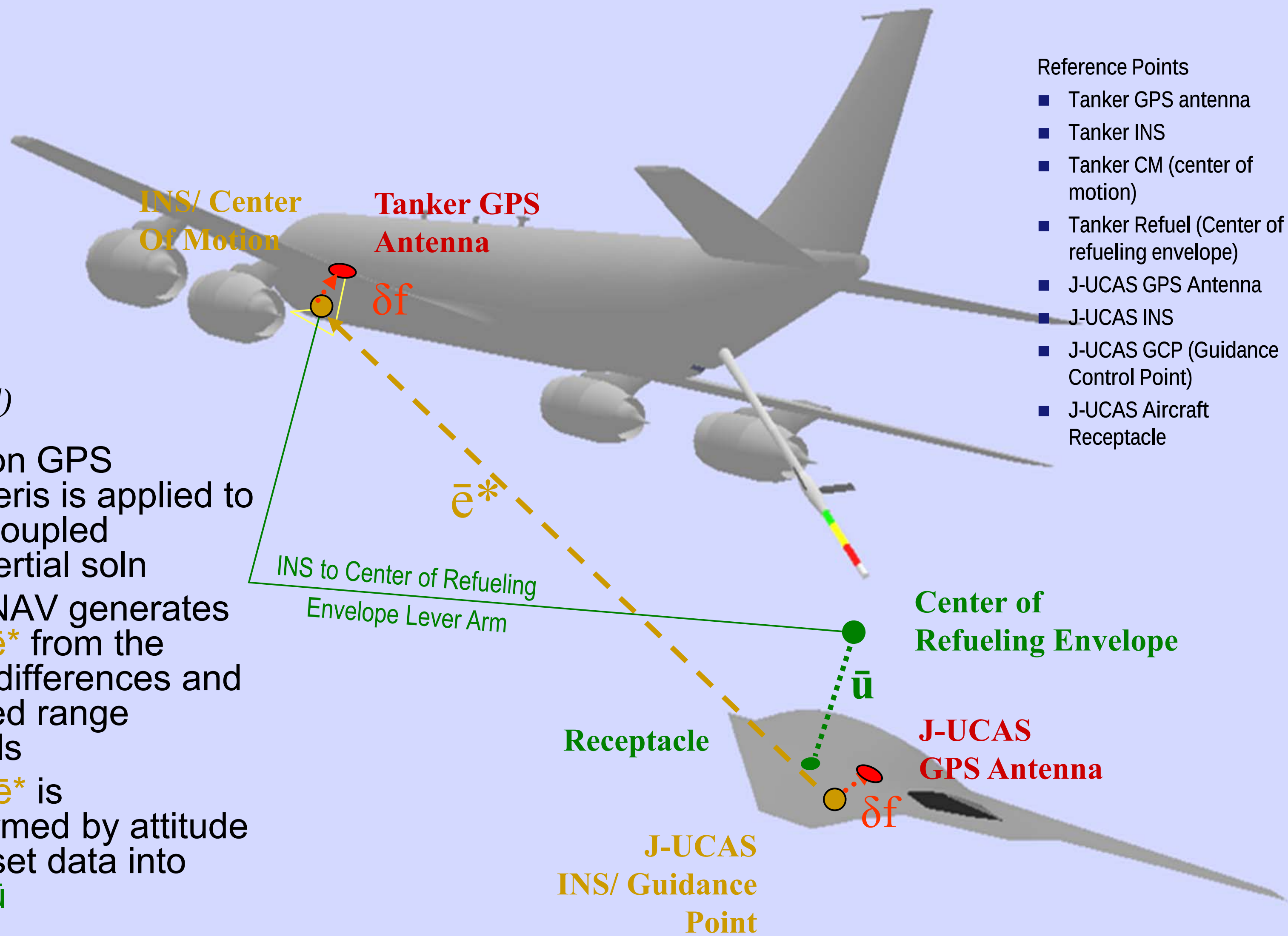
Scale from 0 to 5.5 meters



Scale from 0 to 11 meters

Any poor geometry conditions are excluded (PDOP > 6)

How Precision RELNAV Works

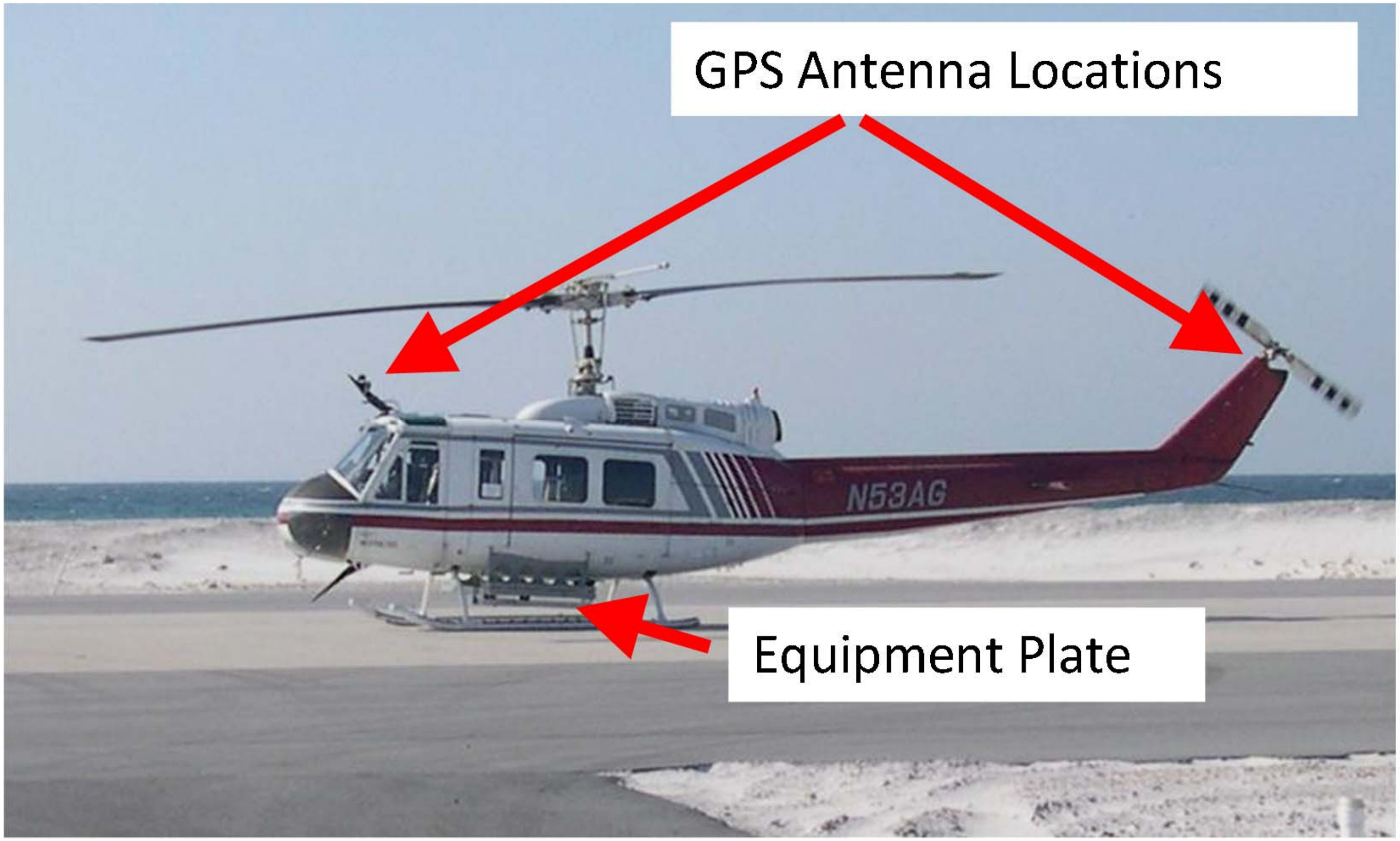


Reference Points
- Tanker GPS antenna
- Tanker INS
- Tanker CM (center of motion)
- Tanker Refuel (Center of refueling envelope)
- J-UCAS GPS Antenna
- J-UCAS INS
- J-UCAS GCP (Guidance Control Point)
- J-UCAS Aircraft Receptacle

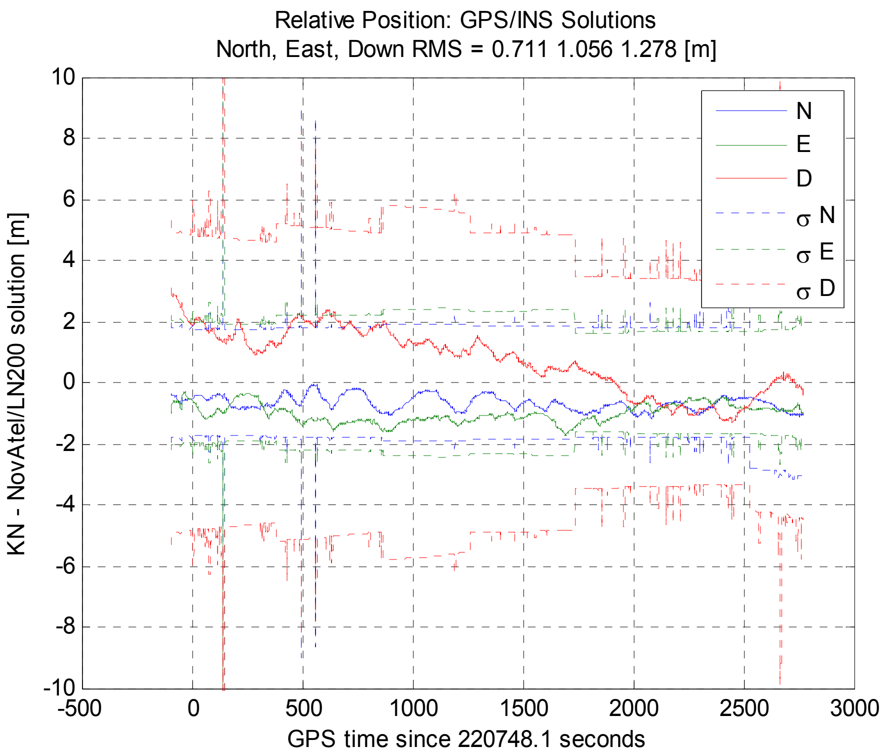
(Simplified)

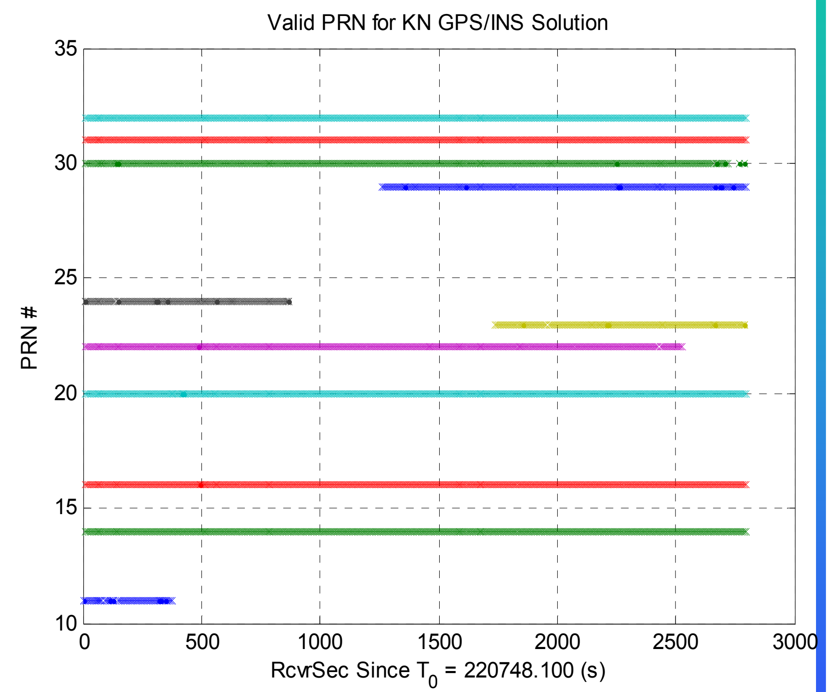
- Precision GPS Ephemeris is applied to tightly coupled GPS/inertial soln
- P-RELNAV generates vector $\bar{e}^*$ from the inertial differences and observed range residuals
- Vector $\bar{e}^*$ is transformed by attitude and offset data into vector $\bar{u}$

UH-1 Flight Test at Eglin AFB 9-12 August 2010
Carried dual GPS/inertial systems + truth reference



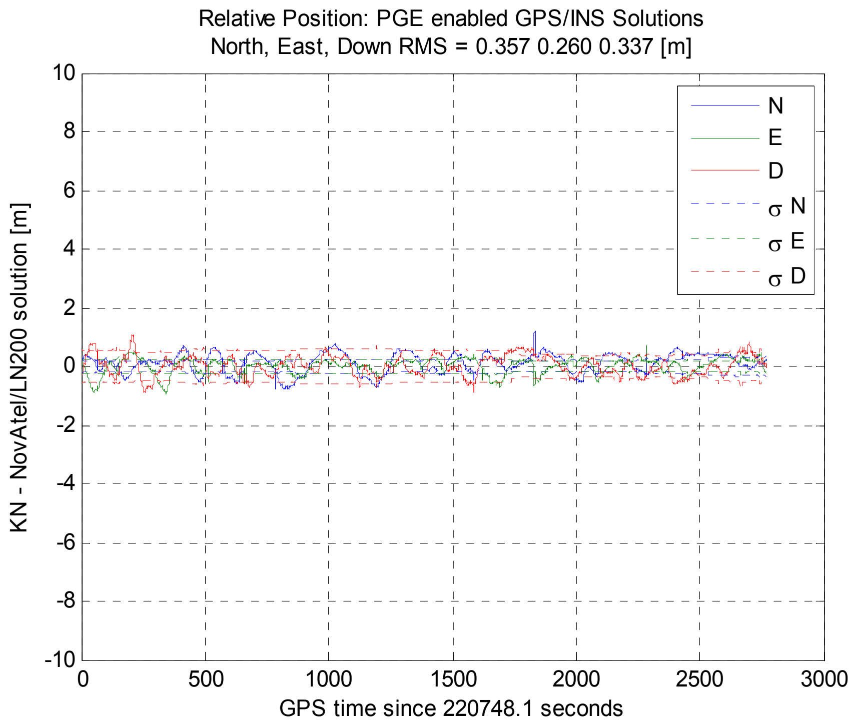
Relative Position – Difference between GPS/INS Solutions (no PGE)





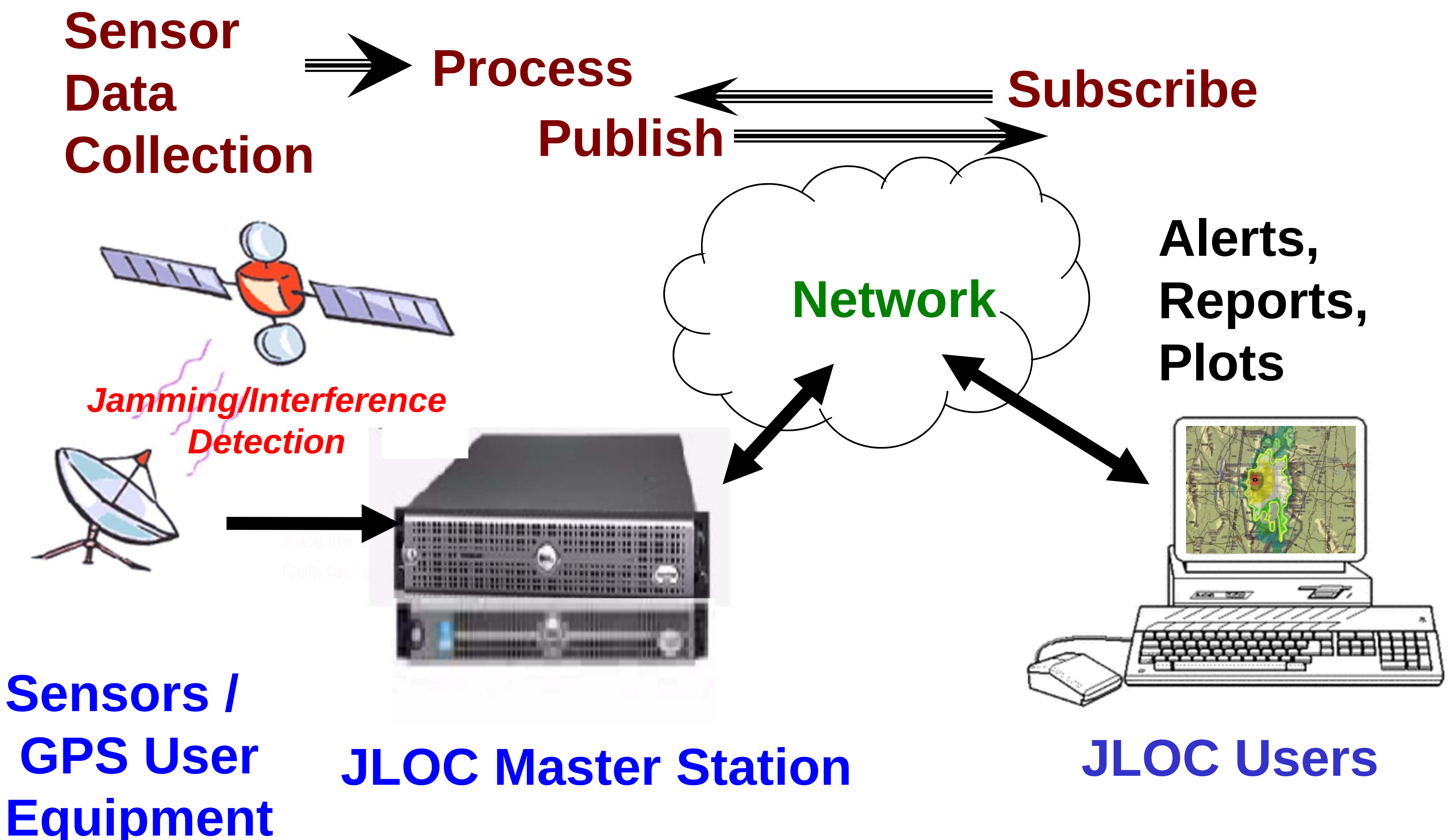
- GPS/INS solution "trends" between biased position offset when GPS satellites change, even when two GPS units track the same satellites

Relative Position – Difference between GPS/INS Solutions (with PGE)



- PGE corrections remove GPS system biases
- Relative position solution < 0.35 m 1-sigma (per axis)
- Peak axis excursions reduced to < 1 m
- Further improvements possible using KF residual updates

JLOC – GPS Jammer SA



Current JLOC Operations

SENSORS	PORTAL	CLIENT

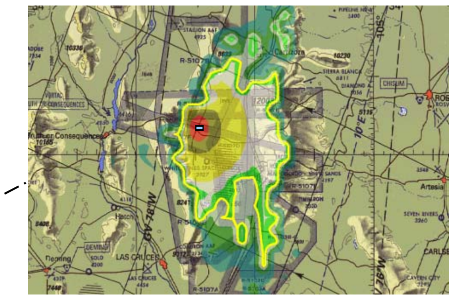
GPS UE C/N0 Sensors

GPS Threat Locations

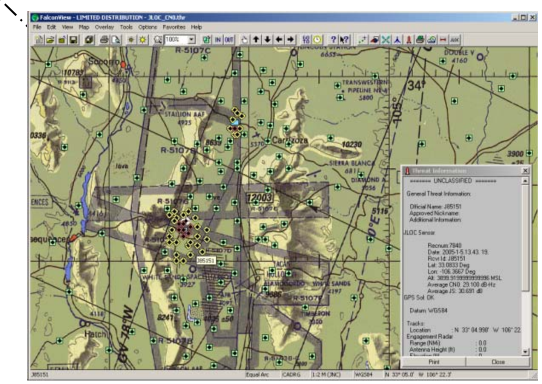
SIPRNET

NGA JLOC Master Station

JLOC Portal



JLOC Client

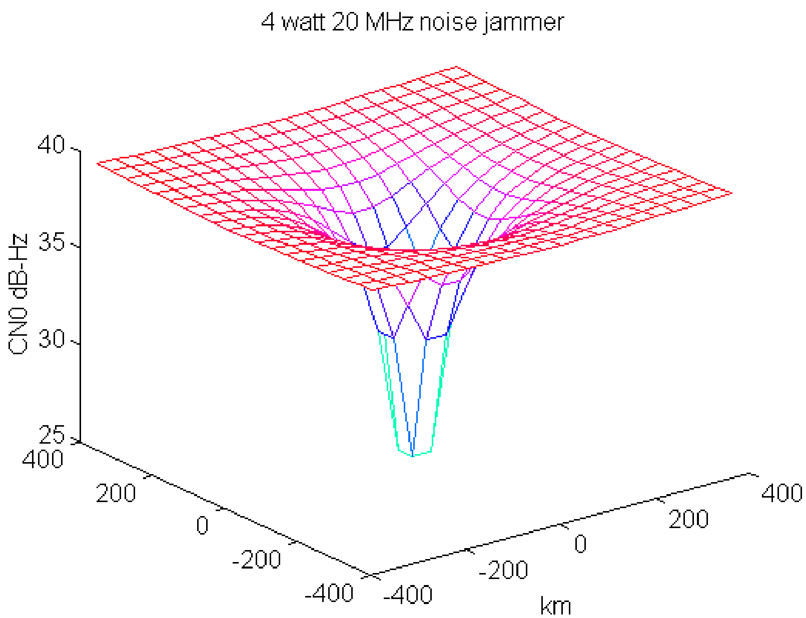


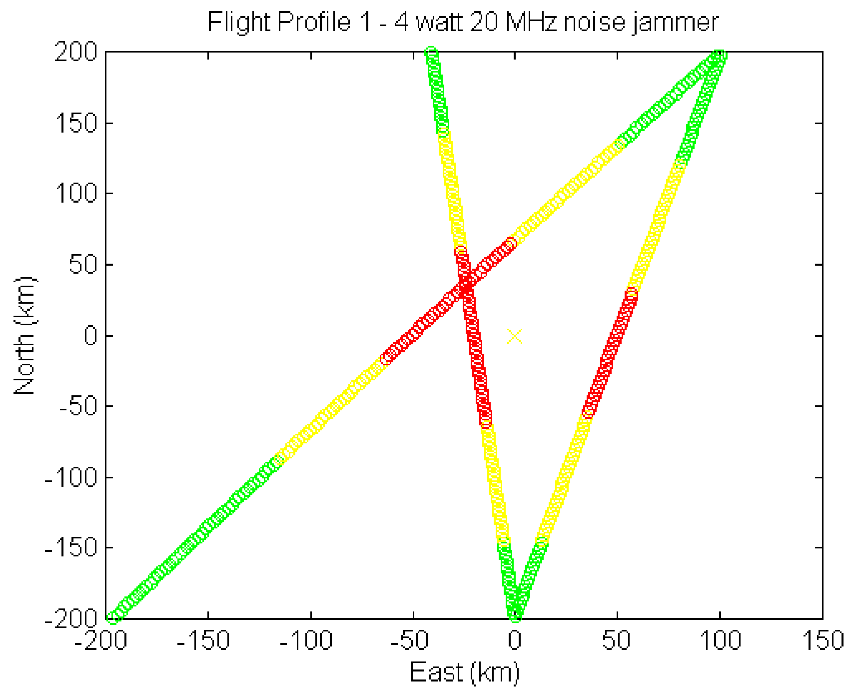
JLOC Client

JLOC Sensor Types

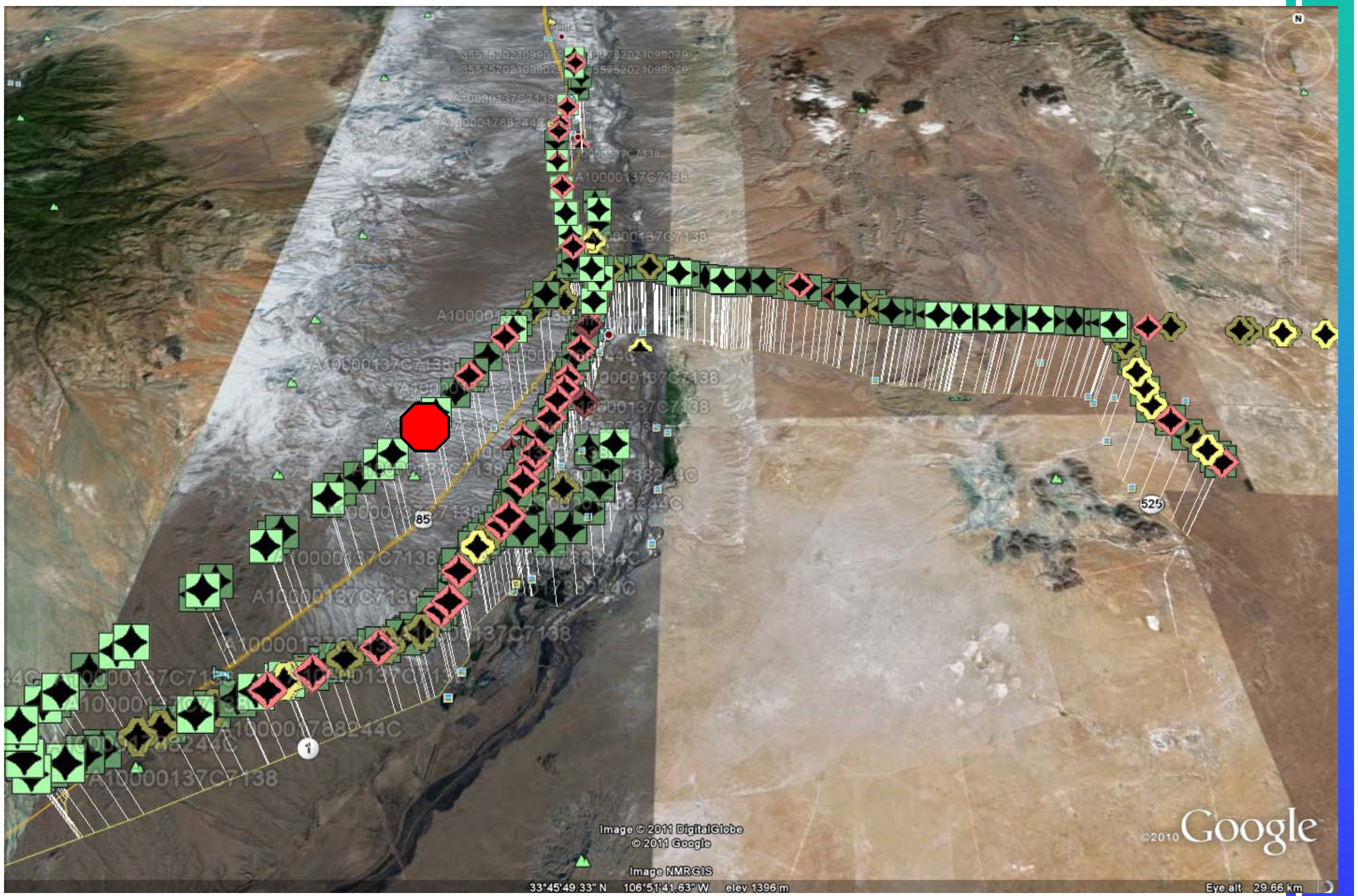
- C/N0 Sensors
  - JLOC reports generated when signal degradation or I/S increase observed
- Threat Sensors
  - Provide estimated geolocation of threats
- AOA Sensors
  - Provide angle of arrival (direction) of threat
- TDOA Sensors
  - Provide raw data for estimating threat location

Multiple GPS UE C/N0 sensor reports indicate region of GPS jamming



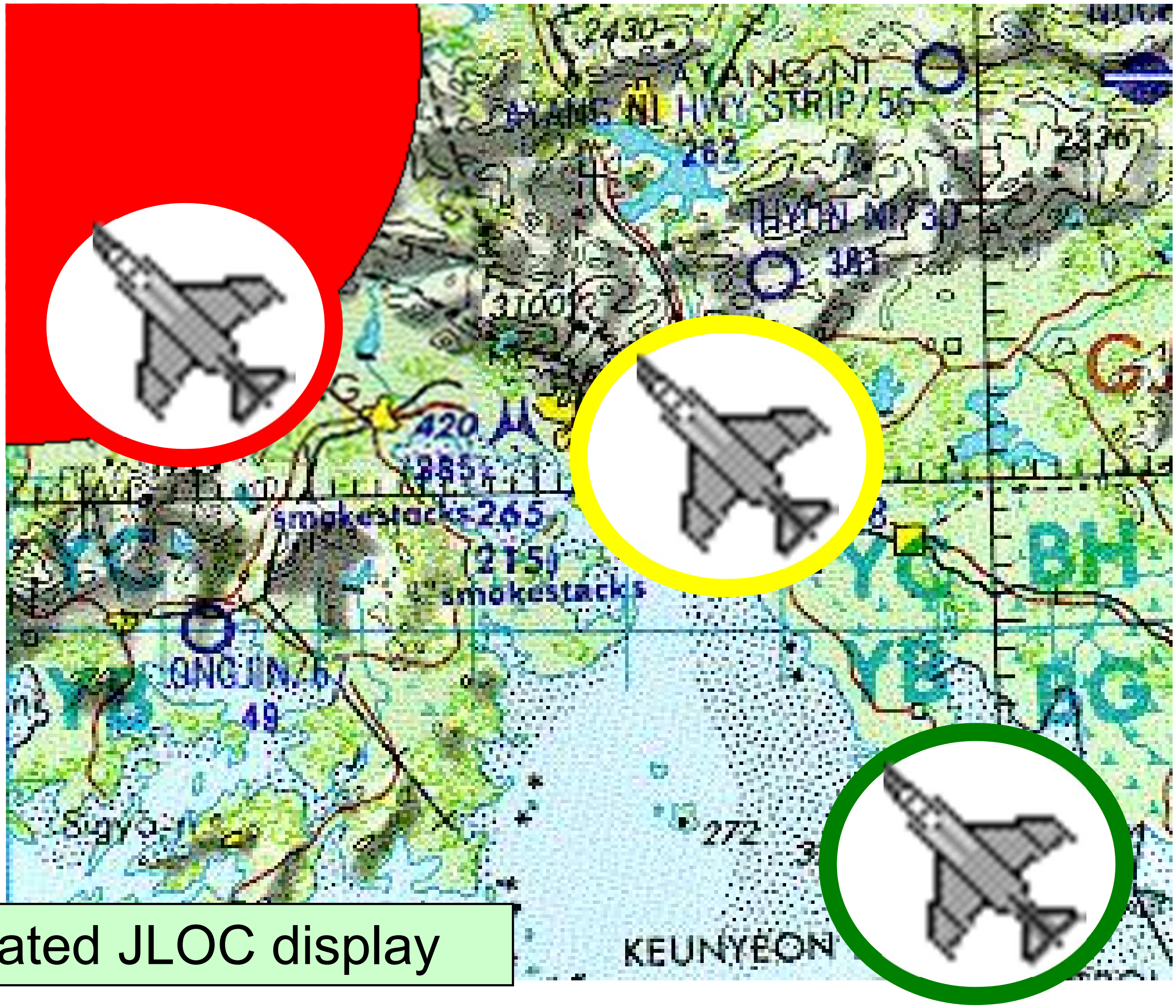


Android C/N0 Data Collect at White Sands



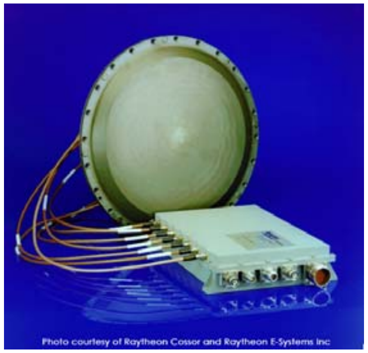
Example Airborne Networking JLOC Reports

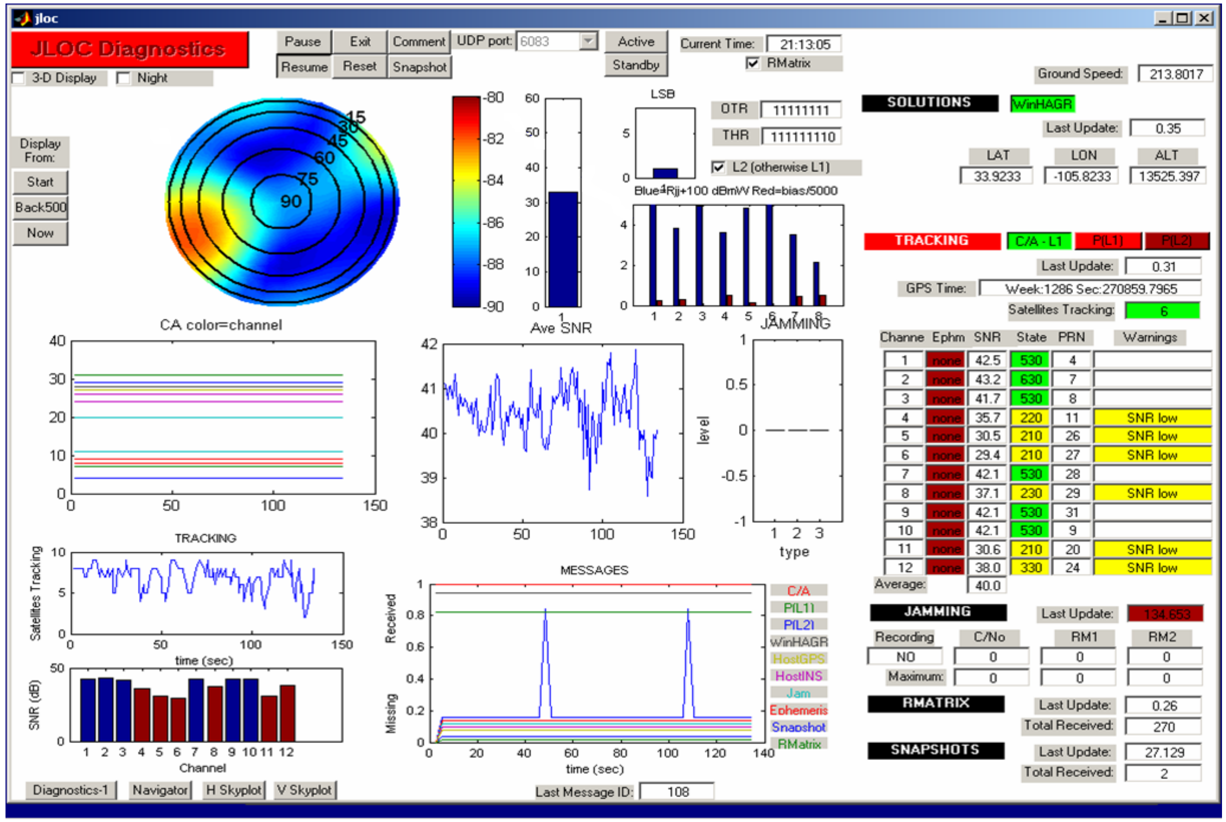
navsys CORPORATION



Simulated JLOC display

JLOC Receiver Unit AOA Sensor





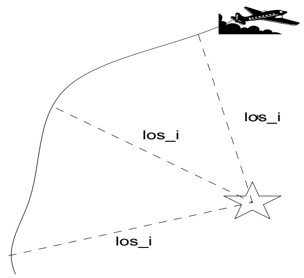
Example JRU real-time display showing AOA of jammer and I/S diagnostics

JLOC AOA Sensor Network Concept

SENSORS	PORTAL	CLIENT

AOA Sensor Network



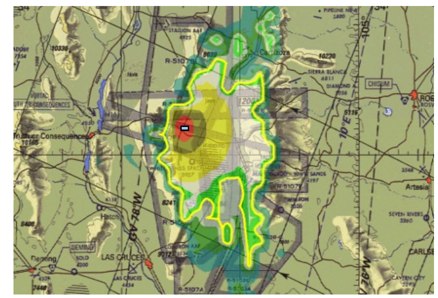


AOA networked geolocation

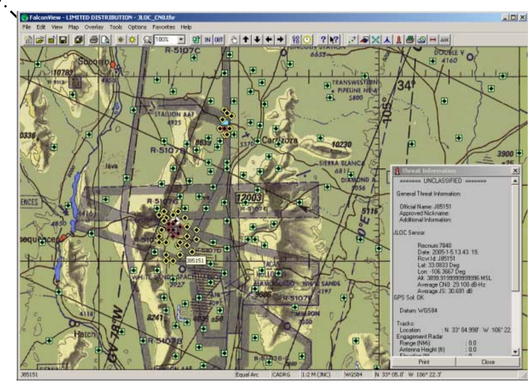
JLOC Master Station

Civil JLOC Portal

INTERNET



JLOC Client



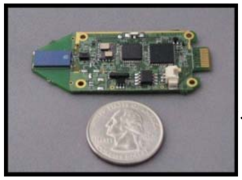
JLOC Client

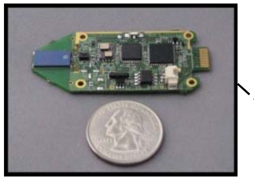
JLOC Portal

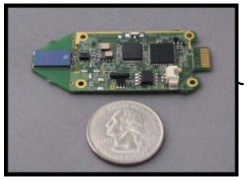
JLOC TDOA Sensor Network Concept

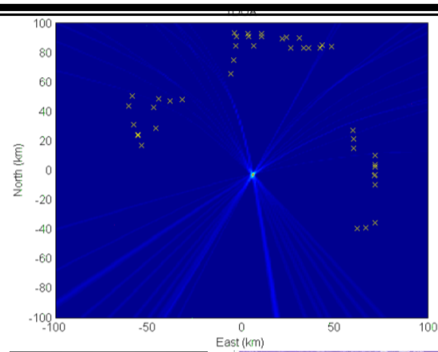
SENSORS	PORTAL	CLIENT

JLOC Snapshot
TDOA Sensor
Network







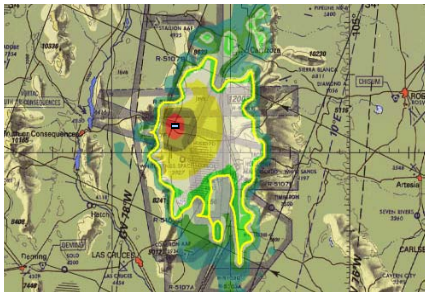


TDOA precise geolocation

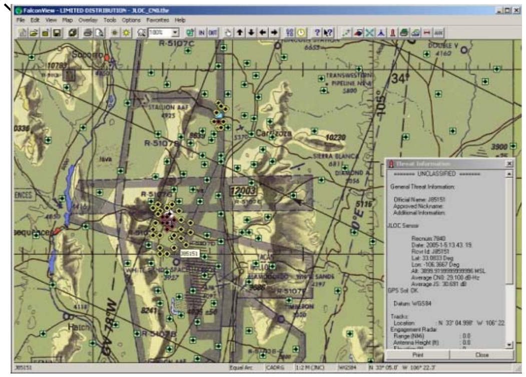
JLOC Master Station

Civil JLOC Portal

INTERNET



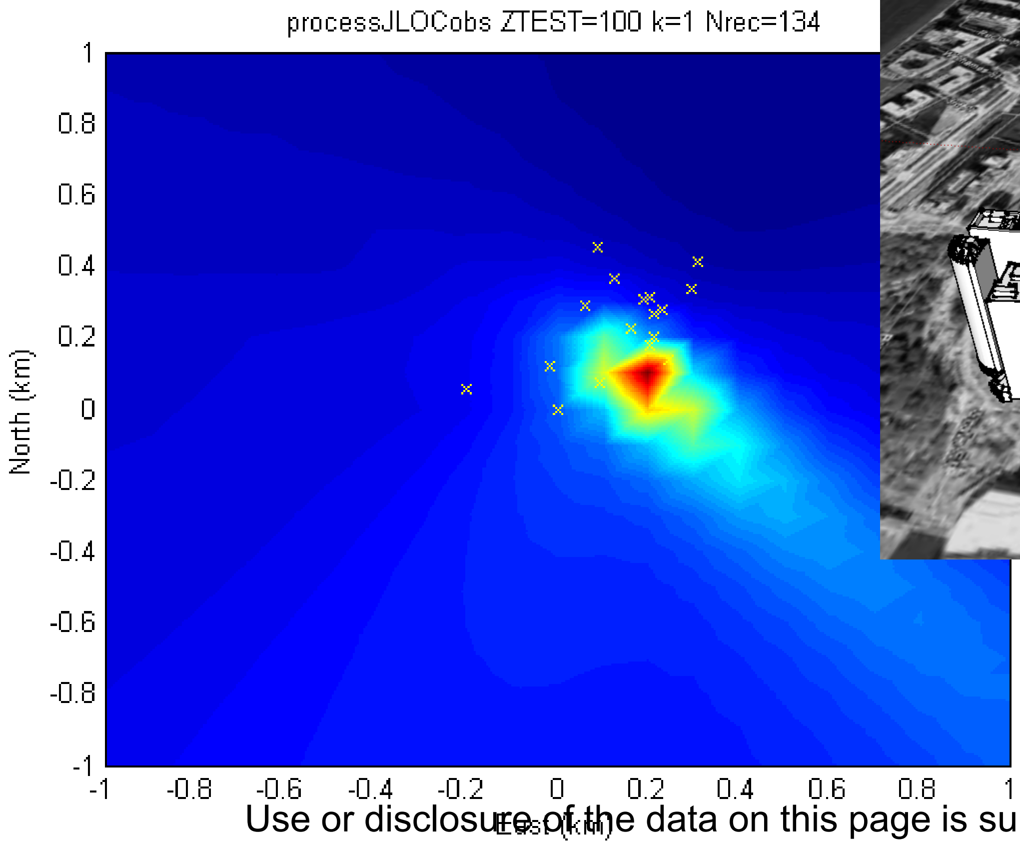
JLOC Client

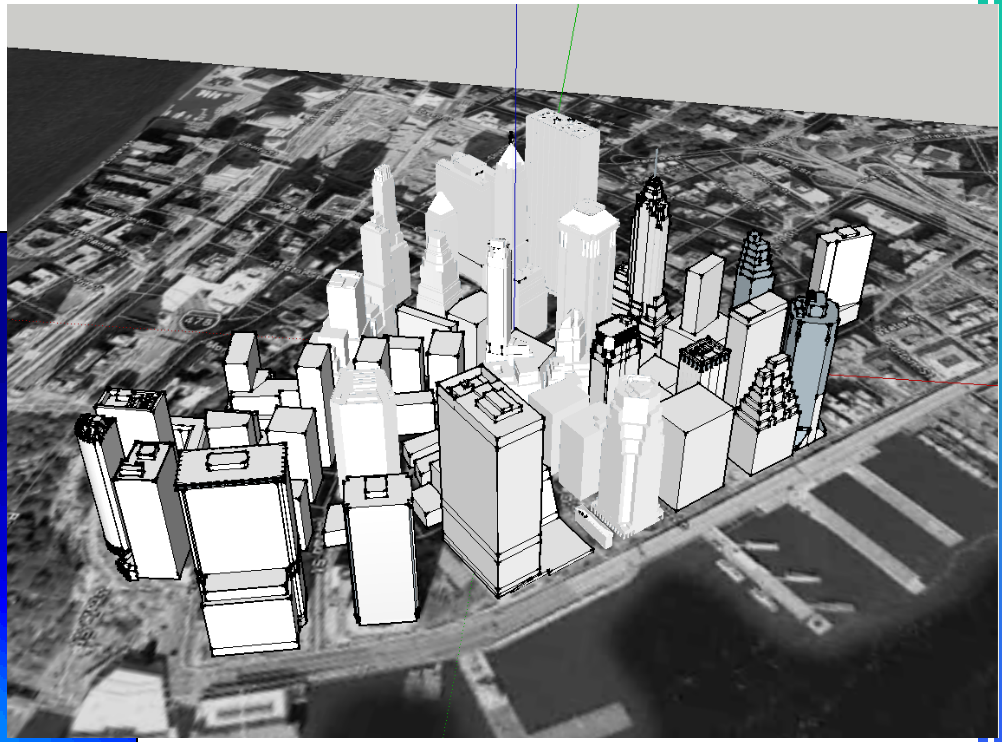


JLOC Client

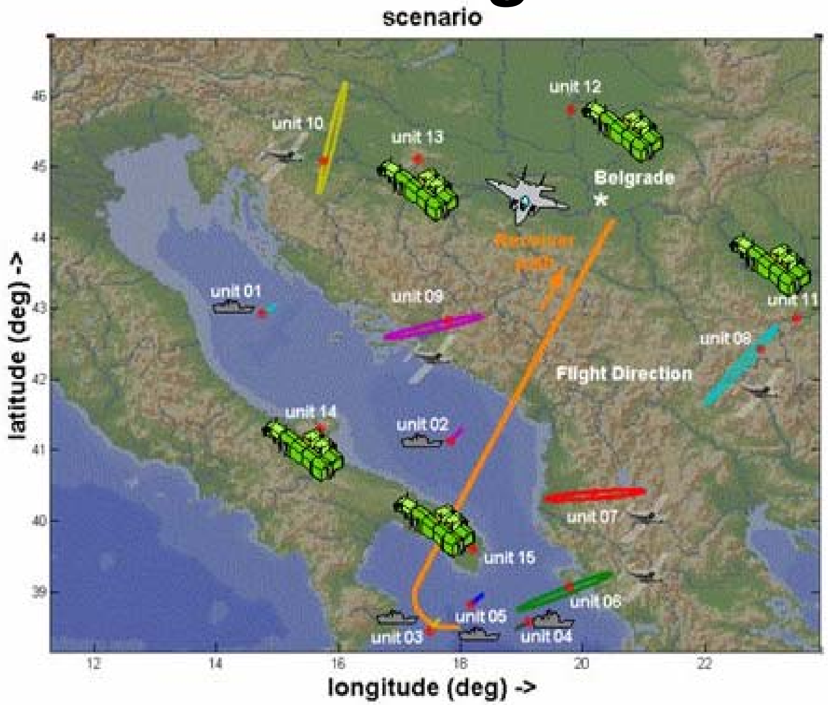
JLOC Portal

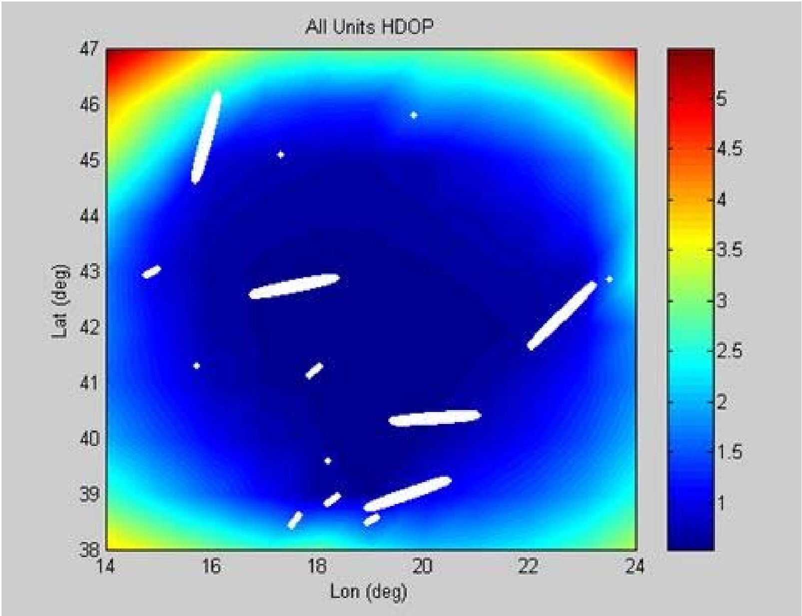
Simulation Results showing TIDGET TDOA Sensor Geolocation





Link-16 RELNAV can be used as a Navigation Back-Up to GPS





- Link-16 RELNAV performance can be improved using existing terminals
- Robust time back-up for network allows operation independent of GPS if needed

Conclusion

- US military is heavily dependent on PNT to support precision operations
- GPS can be degraded, denied or destroyed
- Network augmentation can enhance GPS performance and provide SA on GPS attacks
- Airborne networks can provide back-up PNT services independent of GPS
- All airborne networks need to include RELNAV services (similar to Link-16) but with precision PNT capability

BackUp

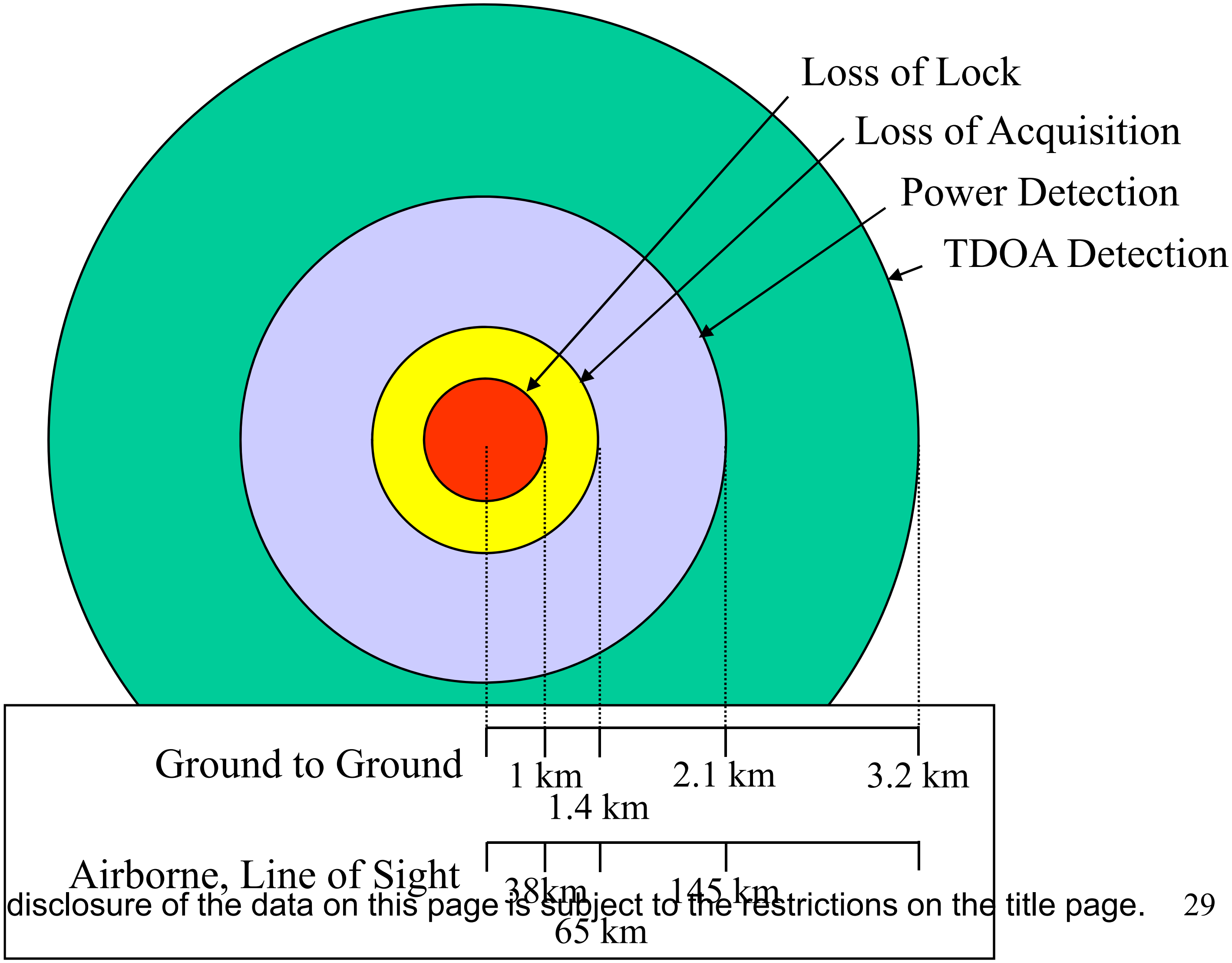
JLOC Program Objectives

- **Situational Awareness** of jammer effects to the warfighter for use in mission planning and execution
  - **Detect** GPS interference by exploiting GPS user equipment as JLOC sensors
  - **Locate** precisely the sources of interference by processing the GPS JLOC sensor data
  - **Disseminate** jammer alerts and reports
- The **JLOC** system approach:
  - Use various **sensors** and reporting systems to **collect information** about GPS jamming and interference
  - **Analyze** the navigation **denial impacts** of this data and centralizes jamming/interference information
  - **Publish** alerts, reports, and effectiveness plots essential **to warfighters** and mission planners reliant on GPS.

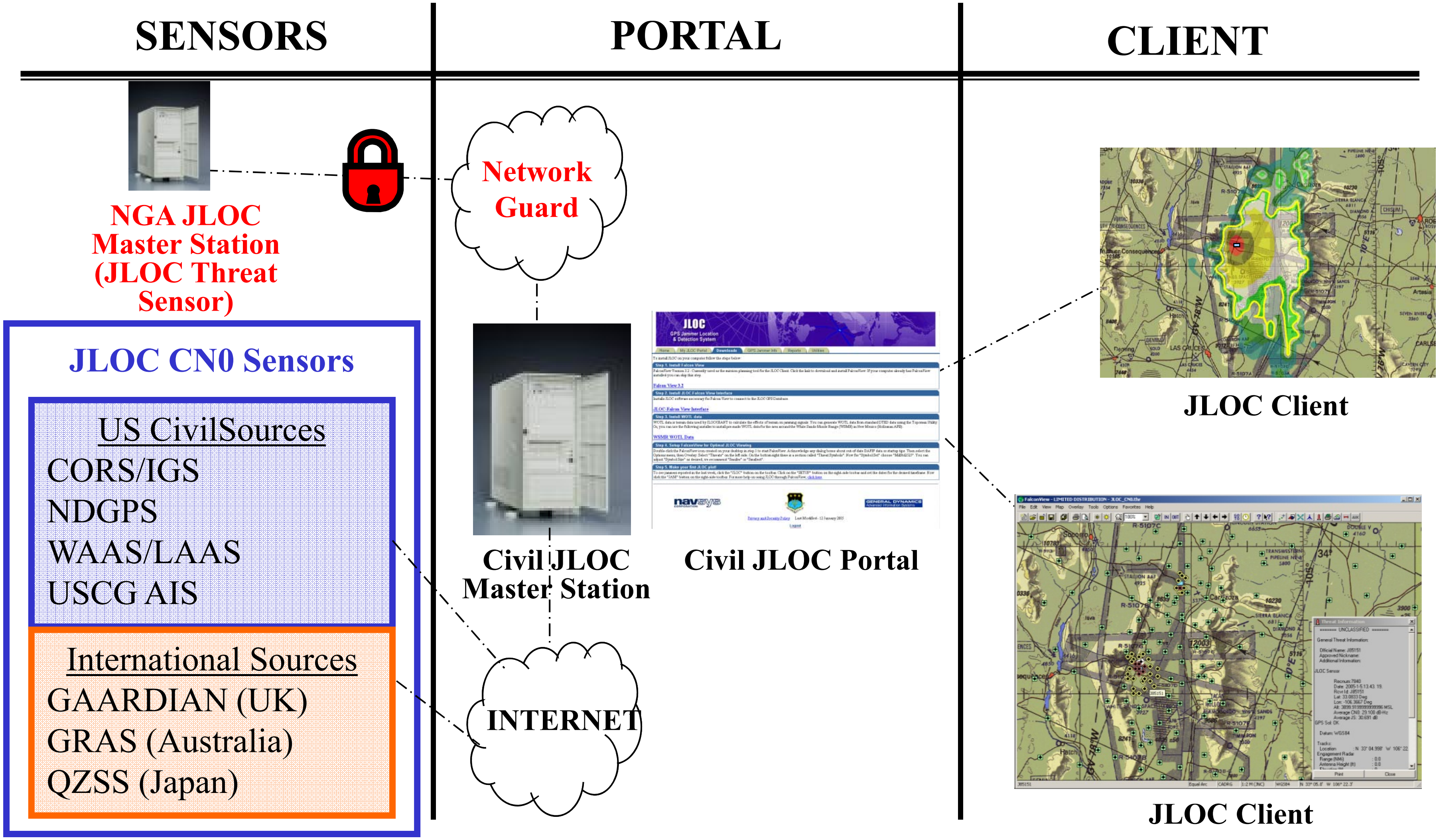
GPS JLOC History

- ‘98: AFRL initial JLOC contract awarded
  - Developed JLOC system design and lab units
- ’00: GATOR Space Battlelab Initiative: JLOC prototype testing at White Sands & Woomera
  - Built prototype JLOC system for field testing
  - Located jammers from ground and airborne units using conventional and modified GPS UE
- ’04: AF TENCAP JLOC Phase III contract
  - Built and tested operational JLOC system
- ’07: JLOC Operational Capability
  - JLOC Master Station located at NGA’s Monitor Station Network Control Center (MSNCC)

JLOC Client Predicts Jammer Effects from Calculated J/S



Examples of Potential Civil JLOC Feeds

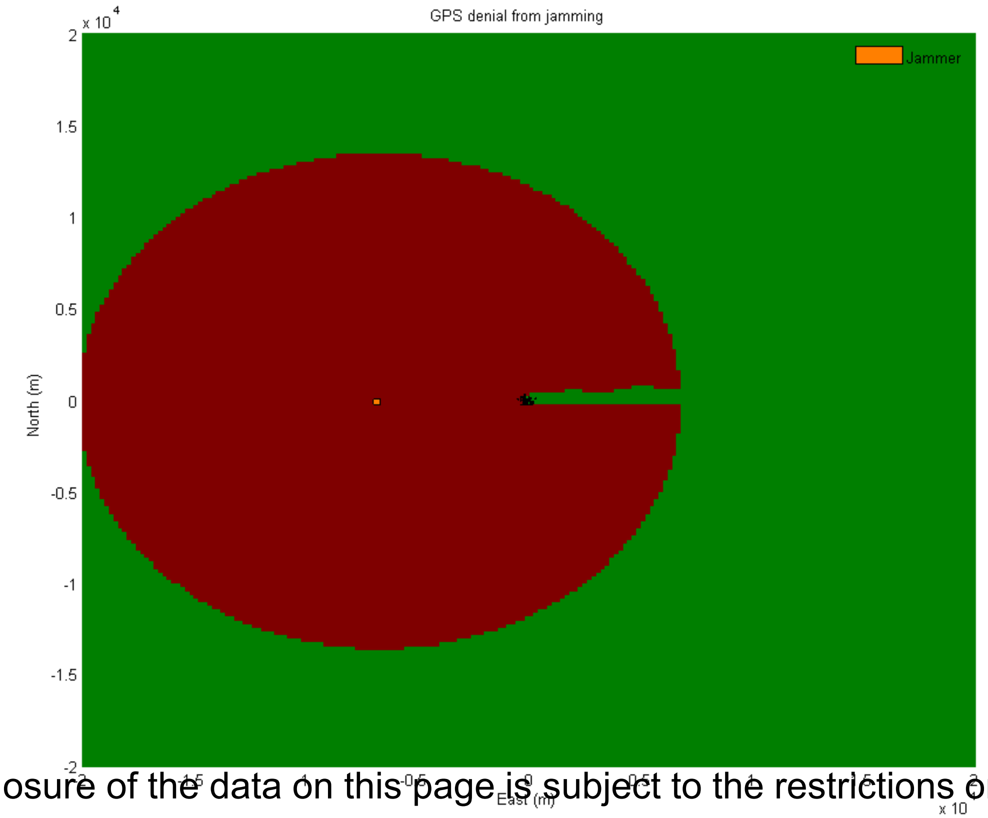


Example Jammer Simulation

- 1 watt jammer from London Eye with receiver J/S= 41 dB
- Cigarette size battery pack gives 10 hrs jammer operation

Scale:

20 x 20 km



Google Sketch-Up Simulation with Jammer Propagation