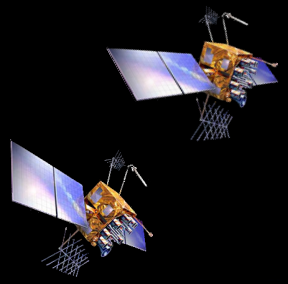
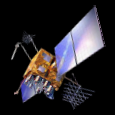


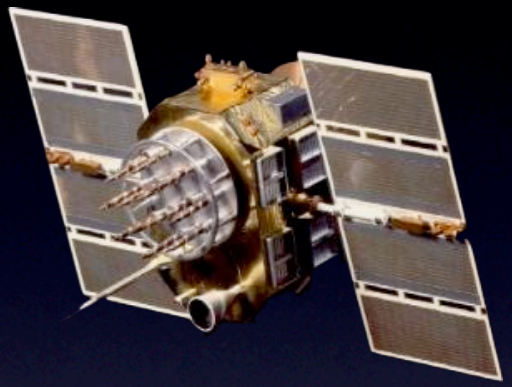


LGSP: A Lightweight GNSS Support Protocol for Military and Civil Applications

Mike Tyson, BCompSc
Dr. Carlo Kopp, MIEEE, SMAIAA, PEng

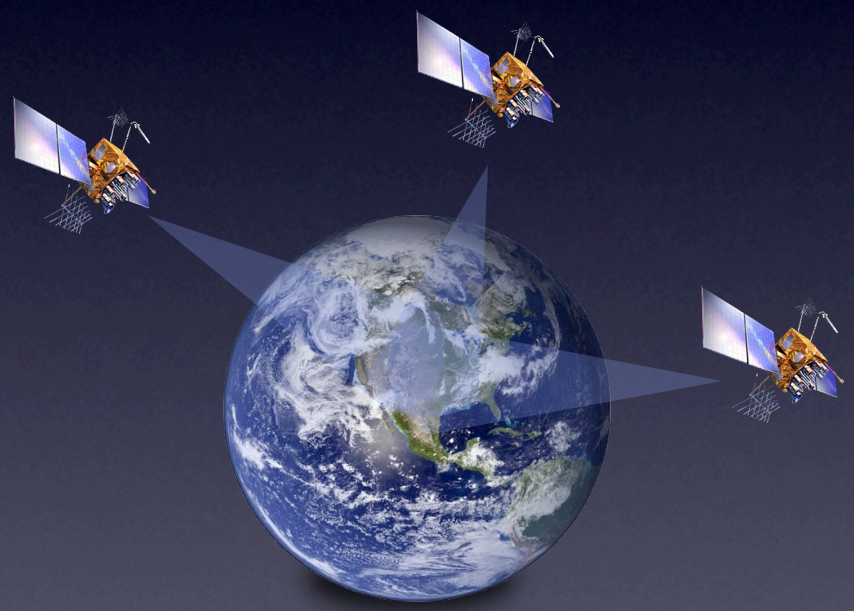
Overview

- Background
  - Global Navigation
  - Augmentation
- Rationale
  - Shortcomings in traditional communication model
  - Alternative: IP
- LGSP advantages
- Messaging
- Conclusion



Global Navigation Satellite Systems

- Orbiting satellites transmit signals to Earth
- Receivers analyse signals from several satellites to generate a position estimate.
- U.S.'s Global Positioning System (GPS) is the most mature and well-known GNSS.

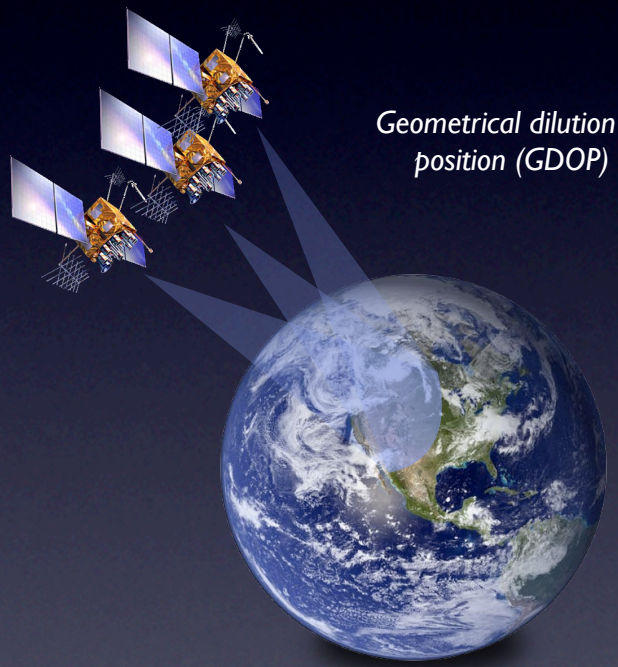


Global Navigation Satellite Systems

- Used in
  - Land, air & sea navigation
  - Surveying
  - Geology
  - Accurate positioning for military applications
  - Mobile telephony applications (Recently, E-911 mandate introduced, requiring emergency call-related positioning)

GNSS Precision

- Accuracy is affected by factors such as
  - tropospheric and ionospheric delays
  - clock drift
  - out-of-date orbital data
  - geometrical dilution of position



Local Area DGPS (eg. LAAS)

- A precisely-surveyed ground station (GS) receives GPS signals and generates a position estimate
- GS calculates discrepancy between known location and position estimate
- GS broadcasts discrepancy over radio, which is used by receivers to adjust their position estimate

Wide Area DGPS (eg. WAAS)

- Many precisely surveyed wide area ground reference stations (WRS) observe the GNSS signal
- A wide area master station (WMS) analyses the data from the WRSs and generates correction information
- The WMS uploads the correction message to a geosynchronous satellite
- Message is broadcast from satellite on the GPS L1 frequency
- Receivers use correction information to correct position

DGPS over Radio: Shortcomings

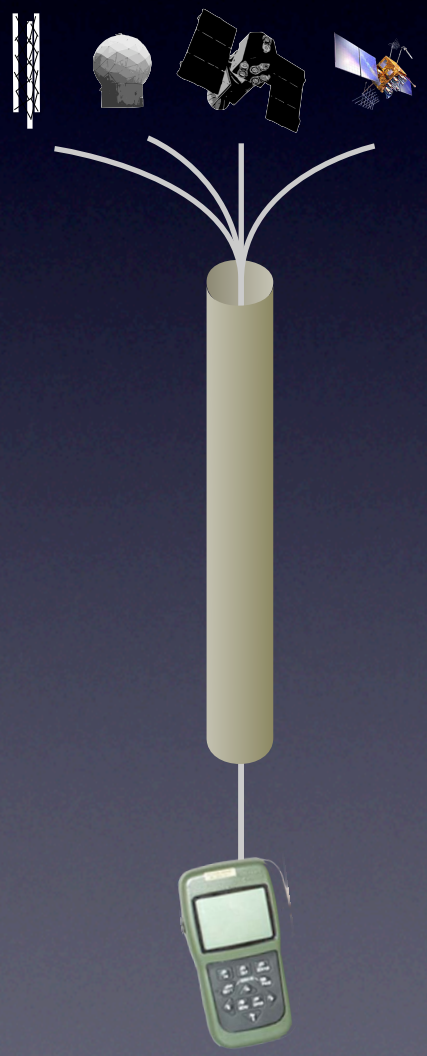
- Operating over a radio link, all DGPS systems require a dedicated, discrete channel
- Increases cost
  - Monetary hardware cost
  - Power consumption
  - Hardware reliability
  - Heat dissipation
- Sub-optimal use of radio spectrum (limited resource)
  - Interference issues
- Vulnerability to jamming, other fading effects
- Low data rate typical - slow update rates

Another option: DGPS over IP

- Many devices with GNSS functionality already have access to an IP channel (JTRS, WiMAX, GPRS, IEEE802.11, etc)
- Typically more robust, faster, more affordable than dedicated radio links
- Bidirectional
- Lower costs, while increasing robustness and flexibility

Lightweight GNSS Support Protocol (LGSP)

- The Lightweight GNSS Support Protocol (LGSP) provides for transport of a variety of GNSS support data over an Internet Protocol (IP) channel, including
  - Local Area DGPS (eg. LAAS)
  - Wide Area DGPS (eg. WAAS)
  - GPS almanac data
  - GPS navigation data

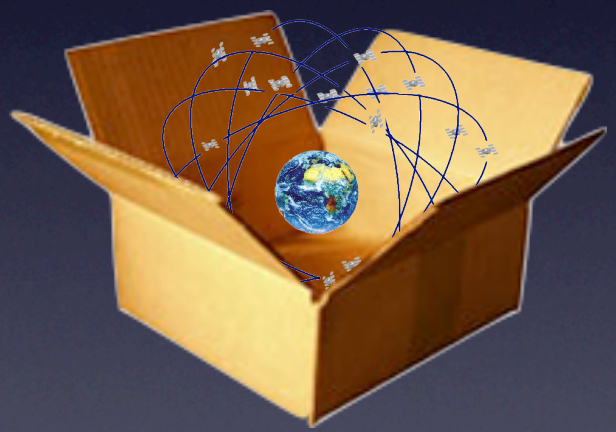


Some Advantages of LGSP

- A pre-existing, robust IP channel can be used for acquisition of GNSS data - Automatically protected by any jam-resistance provided by the IP channel
- GPS start-up time can be reduced as almanac data can be fetched over a high-bandwidth IP link, instead of downloading from the slow satellite link (complete download over satellite link takes 12.5 minutes!)
- Availability of GPS increased, as almanac can still be retrieved when satellite link is weak

LGSP Messaging

- LGSP specification defines messaging formats for:
  - GPS family messaging (eg. GPS NAV messages, almanac pages, LAAS and WAAS messages)
  - messaging for the European Galileo system (including EGNOS correction messages), and
  - messaging for the Russian GLONASS system.
- Can carry a large variety of GNSS support information



Other LGSP Features

- Sophisticated channel protection for use over rudimentary/insecure channels: Encryption and Forward Error correction
  - Provides ‘best effort’ protection even when running over ‘casualty mode’ channels
- Redundant hierarchical architecture with mirroring
  - Increases robustness and availability
  - Load balancing
- Multiply-redundant backup server provisions
- Multicast streaming mechanism for distributing short life-span data

ECCM/EPM - Jam Resistance

- Resistance to jamming is conferred by the Physical and Datalink Layer designs of the channel which is carrying LGSP traffic.
- In military applications it is envisaged that LGSP will run over established military networks and datalinks.
- Eg: JTIDS/MIDS/LET susceptible to repeater mode jamming which degrades throughput; JTRS expected to be more resilient.
- LGSP optimisations for ECM intensive environments based on the use of stateless transactions allowing rapid recovery from packet loss.
- If heavy jamming of the physical/datalink layers occurs, LGSP will not be driven into an unrecoverable state by loss of packets.

LGSP Summary

- Providing a transport for GNSS support data over an IP channel, instead of a dedicated radio link, allows for usage of channels that are mature and often already in place
  - Lowers cost
  - Increases robustness
  - Increases performance
  - Increases security

LGSP Summary

- LGSP provides an alternate means for obtaining GPS almanac data
  - Much faster start-up times from a cold start
  - Increased availability - almanac can still be retrieved when satellite link is weak
- Expansion messaging modes provided for future evolutions of GNSS

Questions?

U.S. Air Force, “NAVSTAR GPS Space Segment/Navigation User Interfaces,” Interface Specification IS-GPS-200D, U.S. Air Force, 3 2006.

European Space Agency, “The Galilei Project: GALILEO Design Consolidation,” brochure, European Commission, 2003.

Russian Space Agency, “GLONASS Interface Control Document,” Tech. Rep. 5, Russian Space Agency, 2002.

T. Walter and P. Enge, “Modernizing WAAS,” in Proceedings of the ION GPS meeting, (Long Beach, CA), 2004.

R. Loh, V. Wullschleger, B. Elrod, M. Lage, and F. Haas, “The U.S. Wide-Area Augmentation System (WAAS),” Navigation, vol. 42, no. 3, pp. 435–465, 1995.

G. W. Hall, “USCG Differential GPS Navigation Service.” Coast Guard Navigation Center Report.

J. Postel, “Internet Protocol.” RFC791, 9 1981.

J. Place, D. Kerr, and D. Schaefer, “Joint Tactical Radio System,” in Proceedings of the Military Communications Conference, vol. 1, pp. 209–213, 2000.

S. J. Vaughan-Nichols, “Achieving wireless broadband with WiMax,” Computer, vol. 37, pp. 10–13, 6 2004.

European Telecommunications Standards Institute, “Digital Cellular Telecommunications System (Phase 2+), General Packet Radio Service, Service Description, Stage 1.” GSM 0.2.60 v. 6.2.1, 8 1999.

ANSI/IEEE, “802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” tech. rep., ANSI/IEEE, 2000.

Some clipart by US. Mil.

http://www.csse.monash.edu.au/research/san

Mike Tyson: *mtyson@csse.monash.edu.au*

Carlo Kopp: *carlo@csse.monash.edu.au*

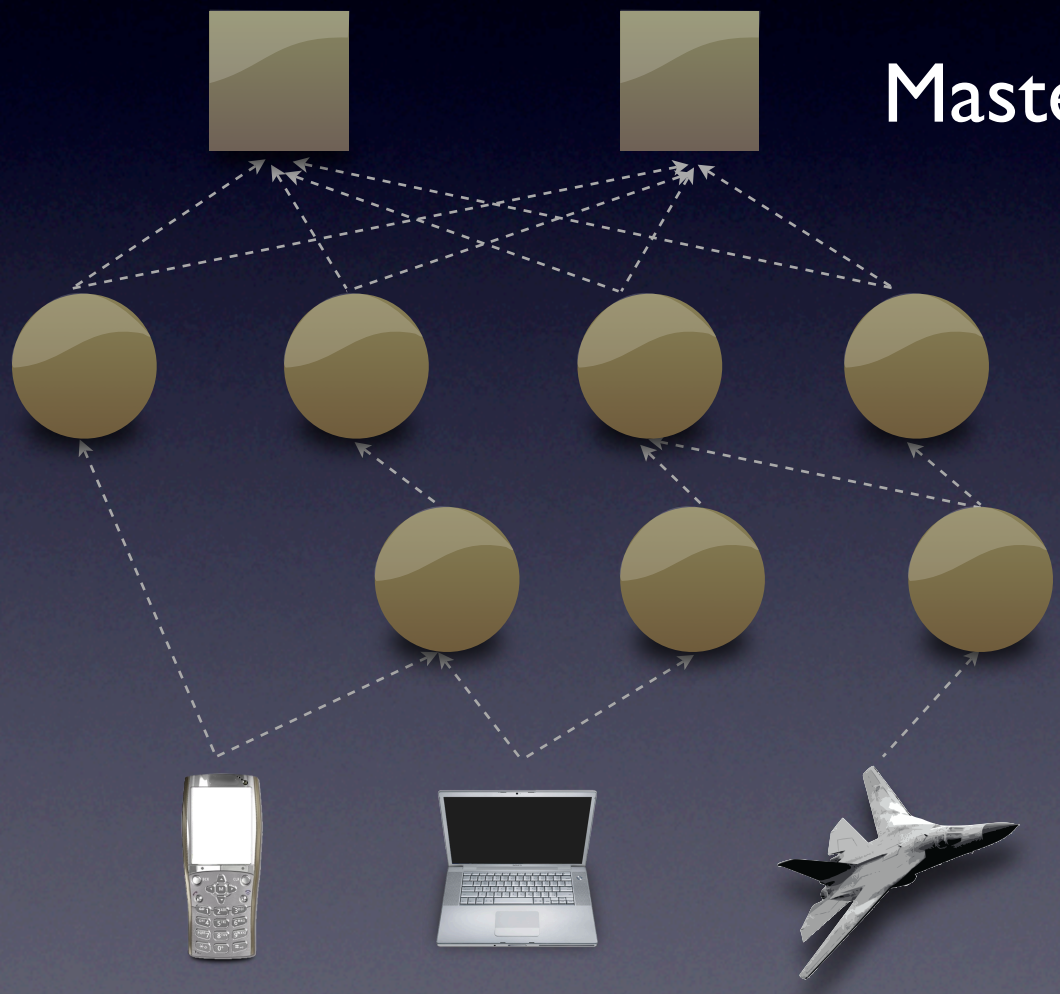
LGSP Protection

- LGSP designed for operation over many different channel types
- Needs adequate protection when operating over rudimentary channels
- Needs to differentiate between user classes in order to provide privileged services

LGSP Protection

- Message exchanges in Protected Mode encapsulated in D-TLS, inside a Forward Error Correction code.
- Authentication provided by D-TLS certificate exchanges

LGSP Architecture Example



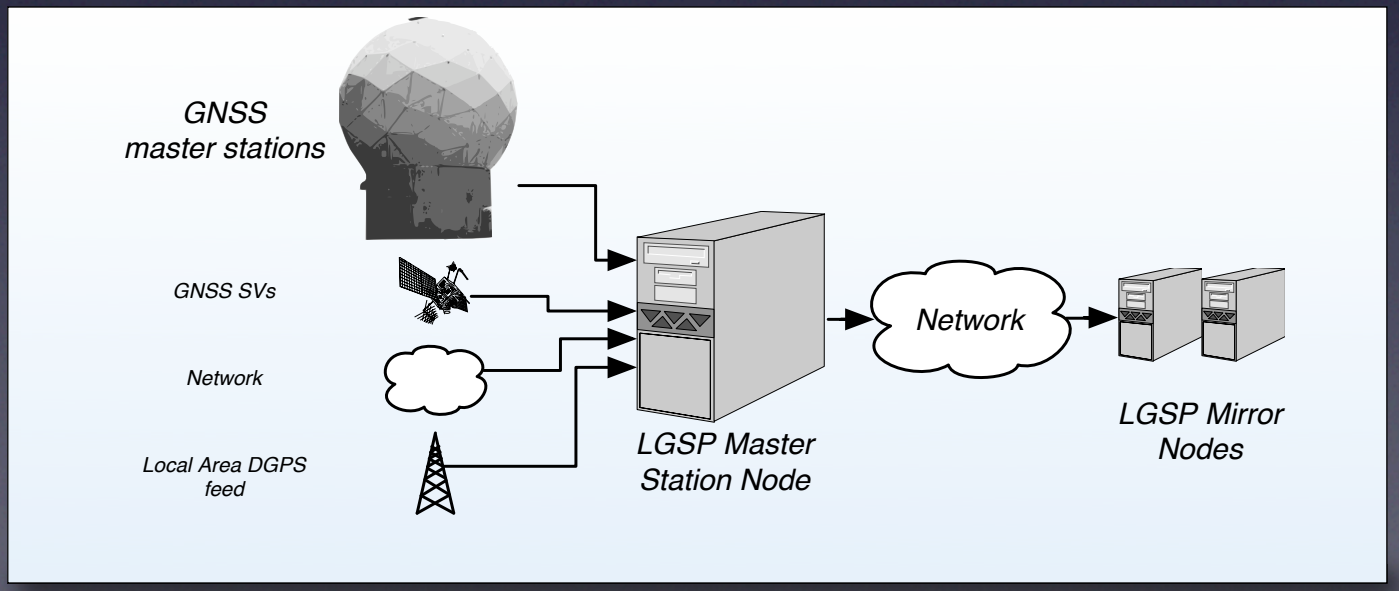
Master Station Nodes

Mirror Nodes

Clients

LGSP Architecture: Master Station Nodes

- LGSP Master Station Nodes
  - Can connect to GNSS master stations, local area DGPS feeds, forward data from GNSS SVs, or auxiliary information from a network source
  - Accept connections only from LGSP Mirror Nodes



LGSP Architecture: Mirror Nodes

- LGSP Mirror Nodes
  - Provide distribution for data from LGSP Master Station nodes (load bearing, security, redundancy)
  - Can also provide local DGPS feed data, and forward data from GNSS SVs, independently of a connection to a LGSP Master Station