

# LGSP: A LIGHTWEIGHT GNSS SUPPORT PROTOCOL FOR MILITARY AND CIVIL APPLICATIONS

Michael Tyson<sup>1</sup> and Carlo Kopp<sup>1</sup>

**Abstract.** We present a Lightweight GNSS (Global Navigation Satellite System) Support Protocol (LGSP), which has been devised at Monash University. LGSP aims to comprehensively address limitations in the traditional GNSS model, such as low signal availability in urban environments, receiver initialisation delays and bandwidth restrictions, by offering an alternative secure distribution channel for GNSS data. This gives compatible receivers an alternate means for acquiring GNSS data, resulting in enhanced robustness, efficiency and availability of GNSS systems. Development of LGSP is nearing completion, and a protocol specification is being released as an Internet Draft to the IETF. This paper presents the rationale behind the development of LGSP and discusses the protocol's architecture, message formats and definitions.

## BACKGROUND

Global Navigation Satellite Systems (GNSS) comprise constellations of orbiting satellites that transmit specific signals to Earth, which a receiver uses to calculate an estimate of its current location. Such systems include the U.S. Navstar Global Positioning System (GPS), the Russian Global Navigation Satellite System (GLONASS), and the fledgling European Galileo. They have proven indispensable for a variety of applications, including land, air and sea navigation, surveying and geology and accurate positioning for a wide range of military applications. [1][2][3][4]

Due to a variety of factors including atmospheric effects such as tropospheric and ionospheric delays, clock drift, out-of-date orbital data and geometrical dilution of precision, the calculated positions typically involve some time variant error. In environments where radio signals from the satellite constellation are impeded, such as in the presence of jamming, or in built-up urban areas, reliable operation may be restricted, or entirely unattainable.

In order to improve precision, various differential schemes have been developed. These mostly employ precisely surveyed ground-based stations, which generate and distribute periodic correction messages for use by compatible receivers.

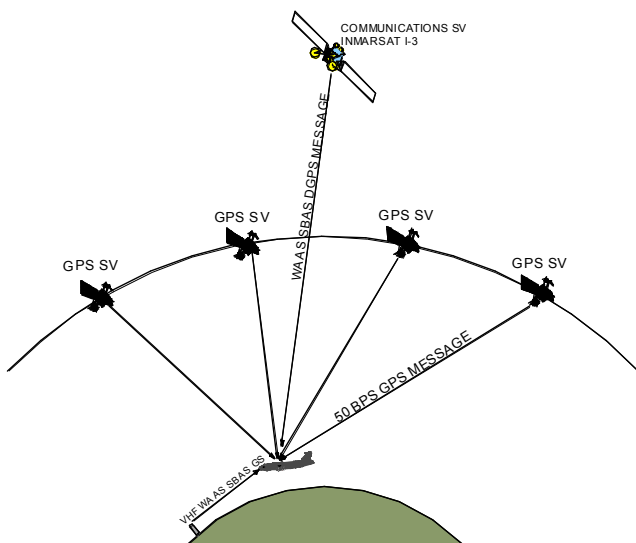


Figure 1. GPS and WAAS SBAS CONOPS.

Such Differential GPS (DGPS) systems can operate in a local geography, essentially generating differential co-ordinates that offer accurate corrections valid within a small area - these are known as Local Area DGPS systems (LADGPS). Alternatively, Wide Area DGPS systems (WADGPS) offer corrections that are valid over a much larger area, generally continental in extent, and typically generate models to represent different sources of error, instead of simple offset co-ordinates (Figure 1). [5][6][7][8]

Typically, Differential GPS messages are broadcast over a specialised radio channel. The widely used WADGPS system known as the Wide Area Augmentation System (WAAS) [6], developed by the Federal Aviation Administration (FAA), uses a number of satellites to broadcast differential information. Most LADGPS systems, such as the FAA's Local Area Augmentation System (LAAS) [5], use a local radio transmitter to distribute corrections.

The use of a specialised radio channel presents a number of drawbacks. Firstly, use of a radio link for DGPS means that a dedicated, discrete channel is required for each system. Hardware for maintaining a radio link represents a significant cost to a DGPS system, both monetarily and in terms of power consumption, hardware reliability and heat dissipation. A dedicated channel also results in relatively sub-optimal use of the available radio spectrum, a finite resource. As wireless technologies become increasingly popular, and radio spectrum usage increases, it will be increasingly important to utilise radio frequency spectrum efficiently. In addition, the widespread use of wireless devices, as well as electronics in general, results in interference issues. Combined with intentional jamming, this presents a developing vulnerability for radio-based DGPS, requiring more robust and complex components, in turn raising the cost of DGPS hardware. Traditional DGPS channels also typically have a low data rate, resulting in slow update rates. Multipath, masking and other radio propagation issues represent yet another impairment, further constraining DGPS systems.

Many GNSS- and DGPS-equipped platforms also contain some other form of wireless connectivity, such as IP (Internet Protocol) [9] wireless via satellite or another high capacity channel like the U.S. Military's Joint Tactical Radio System (JTRS) [10][11] or civilian channels such as WiFi [12], WiMAX [13] or GPRS [14]. Such channels are typically more robust, faster and more affordable than specialised dedicated links, and may also be bidirectional, providing for more flexible operation. By using an existing channel for

<sup>1</sup> Faculty of Information Technology, Monash University, Wellington Road, Clayton, Victoria, Australia, 3800.

DGPS correction update distribution, instead of establishing new dedicated channels, costs can be lowered, while increasing robustness and availability of communications. If a DGPS system makes use of an established link technology, dedicated radio hardware is not required. In addition, existing channels typically provide high availability, jam or interference resistance and reliability, which a DGPS system would benefit from.

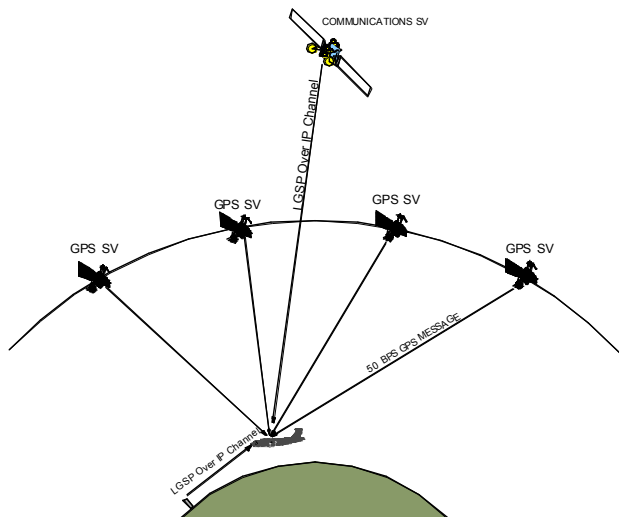


Figure 2. LGSP CONOPS.

Furthermore, by using an IP channel for alternative distribution of GNSS navigation messages, less importance is placed upon an uninterrupted signal from the satellites in the constellation. Characteristically, all GNSS almanac data and navigation messages are received over the radio link from the constellation, placing bounds both on the minimum usable signal strength, and duration of uninterrupted coverage, be it due to interference, jamming or masking. When this data is received via an IP channel instead, the signal from the GNSS constellation is only required for pseudorange measurements, where a Kalman filter can be used to improve robustness. Effectively, this improves the robustness of GNSS receivers, allowing operation in otherwise problematic situations.

### LGSP CONCEPT OF OPERATIONS

Figure 1 shows a traditional, non-LGSP example, with an airborne platform using GPS augmented by WAAS. The platform acquires signals from the visible GPS Satellite Vehicles (SVs) and receives broadcast WAAS DGPS messages from another SV<sup>2</sup>. Trials involving broadcast of WAAS messages from a network of ground-based VHF radio network beacons have also been performed by Air Services Australia [15,16,17].

The WAAS DGPS signals, acquired from a SV transmitting WAAS data or via radio from a ground station, are 250 bit/second messages containing clock offset corrections, ephemeris corrections, ionospheric delay estimates, integrity information or other augmentation data.

Figure 2 depicts a similar scenario, but using an LGSP signal instead of a WAAS signal [24,30,31,32].

<sup>2</sup> The current WAAS configuration makes use of two INMARSAT I-3 satellites [23]

LGSP	
UDP	
IP	
Adaptation Layer	
Link-16	SATCOM

Figure 3. LGSP over IP over Link-16 Network Stack [29].

The airborne platform maintains an IP [9] channel, either via a satellite link, or a radio link to a ground station. In a military context, this could be a JTRS channel [18,19], JTIDS/MIDS (Joint Tactical Information Distribution System / Multifunctional Information Distribution System) [20] with an IP adaptation layer (Figure 3) [29], an IP over IDM (Improved Data Modem) link, or IP over FAB-T (Family of Advanced Beyond Line-of-Sight Terminals) [21]. Alternatively, civilian channels could include WiMAX [13], GPRS [14], WiFi [12] or GSM [22].

Periodically, the platform transmits a data request to an LGSP server over the IP channel. Such a request would typically involve an identification of the data to be returned, such as “the latest almanac data for SV *n*”, or “all WAAS data for the last 10 minutes”. A request could also include a digital certificate for authenticating the user. When operating over an unsecured channel, a request could also include a handshake for establishment of an encrypted session.

Upon receipt of the request, the ground-based LGSP server formulates a response message based on the requested data, and sends it back to the platform over the IP channel. If a poor link results in the loss of either the request or the response message, the airborne platform in the example simply re-transmits the request to restart the process.

After receiving the LGSP message, the platform decodes the encapsulated data for processing. For example, if a block of raw WAAS data was requested, the platform then extracts the WAAS messages from the LGSP reply message, and passes these to a WAAS-compatible software module.

### GNSS MESSAGE SUPPORT

LGSP provides support for most common GNSS message formats, including GPS, GLONASS and Galileo, and several Differential GPS systems. It also contains provisions for future additions.

When supporting an existing GNSS message format, the GNSS message data structure is preserved, encapsulating GNSS messages unchanged within LGSP messages. This allows the received messages at the LGSP client to be de-encapsulated and passed to a compatible device without requiring significant changes to the device.

A number of system protocols have been defined to support a variety of GNSS systems. These include:

- GPS (Global Positioning System)
- WAAS (Wide Area Augmentation System)
- LAAS (Local Area Augmentation System)

- The European Galileo system
- The Russian GLONASS system

Within each of these categories, a number of messages are defined. For example, the GPS system protocol for LGSP defines:

- NAV, CNAV and CNAV-2 message subframes
- NAV, CNAV and CNAV-2 message frames
- NAV, CNAV and CNAV-2 message streams
- Enhanced differential correction message/stream
- Almanac page

## SYSTEM OVERVIEW

LGSP is a client/server protocol which operates over UDP, and does not keep per-session state except where necessary for channel protection purposes. LGSP defines a modular architecture, providing for future expansion and new message types.

LGSP is intended for dual (military and civil) use, but is designed from the outset to be fully featured and functional in a military environment. Thus, LGSP is designed for operation over a wide variety of channel types. These could include secure and robust channels such as the U.S. Military's Joint Tactical Radio System (JTRS) or the Joint Tactical Information Distribution System (JTIDS), or the civilian WiMAX. However, channels may also possess poor security features and/or poor reliability and robustness; such channels include GPRS, WiFi, or various rudimentary satellite or HF band communications protocols.

To cater for this large variation in channel characteristics, LGSP offers both protected and unprotected modes. LGSP's protected mode offers channel protection in the form of encryption, wrapped in a FEC (Forward Error Control) code, and is designed for operation over rudimentary channels lacking adequate protection. Alternatively, LGSP's unprotected mode is designed for more robust and secure channels, such as the military JTRS or JTIDS channels, which already have protection and thus do not require the overhead of additional protection layers.

Other LGSP features include mirroring, load balancing and provisions for multiply redundant backup server operation.

The system architecture of a single LGSP server comprises three elements: One or more source feeds, a server unit, and client units (Figure 4).

Source feeds are incoming sources of data. This can be a radio receiving transmitted DGPS signals such as WAAS [6], for example. Alternatively, a direct communications link to a DGPS station could replace the radio receiver, offering a more reliable and high-bandwidth link. Such a software module would store received messages in a buffer, for subsequent retrieval by clients.

A local geographically surveyed GPS receiver with accompanying software to generate a Local Area DGPS signal could be used as another source feed. Additionally, a GPS receiver can be used to record GPS messages for subsequent distribution.

A direct communications link to a GNSS control centre offers a reliable and flexible high-bandwidth link for direct distribution of GNSS navigation messages. This allows LGSP to offer a high performance distribution channel for navigation data, as well as for supporting GNSS data that may not be feasibly broadcast over the traditional space-based segment, due to bandwidth, latency or security considerations.

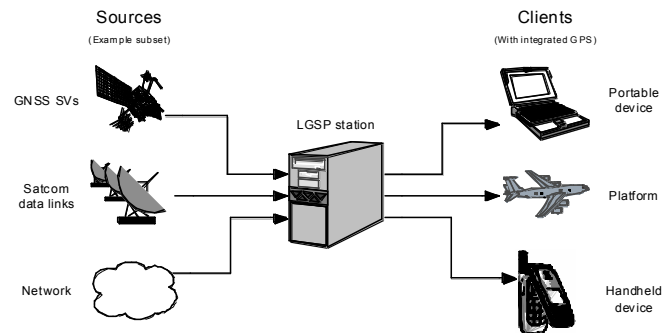


Figure 4. LGSP System Overview.

Wide area differential systems, such as the US Air Force EDGE RRN demonstrator [7] and WAGE [8] system represent other possible sources of data, either via a radio link or a direct connection to a master station.

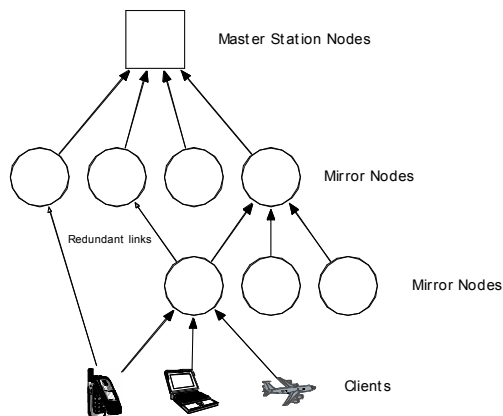
Source feeds are paired with an accompanying software module within the LGSP server software, which provides functionality for storing and later accessing the source data. Each software module implements a source-specific network protocol that is encapsulated within LGSP, and understood by a corresponding software module located in the LGSP client software.

The LGSP server is a unit that assimilates the data incoming from the sources, and provides an interface (LGSP) for dissemination of this data to LGSP clients. The LGSP server is largely stateless, except for provisions for streaming functionality and channel protection, and thus does not attempt to provide guaranteed service in any way. This enhances the protocol's robustness, so that clients operating over unstable channels do not needlessly tie up server resources. No retransmissions are attempted in the case of packet loss when sending to a client. Connectionless UDP datagram communications are used, which ensures that server resources will not be tied up if a client drops out. These features are tailored for best possible performance in the presence of a poor network operating environment, with frequent disconnections and packet loss; such conditions are common in a mobile wireless, especially military scenario.

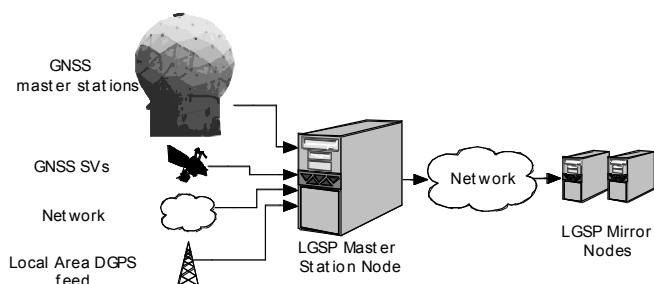
We envisage a hierarchy of LGSP servers with redundancy, similar in concept to that of DNS (Domain Name System) [25,26]. LGSP Master Station Nodes form the top level of the hierarchy, while LGSP Mirror Nodes form the remainder of the tree (Figure 5).

Clients access LGSP Mirror Nodes only. LGSP Master Station Nodes will only accept connections from other LGSP Master Station Nodes, or LGSP Mirror Nodes. This avoids the danger of overloading an LGSP Master Station Node with too many incoming connections, as there will only ever be a relatively small number of LGSP Mirror Nodes connecting to an LGSP Master Station Node at any time.

As in the redundant DNS name server architecture, LGSP clients maintain knowledge of multiple LGSP Mirror Nodes, for redundancy and load balancing purposes. Similarly, LGSP Mirror Nodes themselves can maintain knowledge of multiple LGSP Mirror Nodes and multiple LGSP Master Nodes.



**Figure 5. LGSP Mirror/Master Station Node Hierarchy Example.**



**Figure 6. LGSP Master Station Node Example.**

An LGSP Master Station Node (Figure 6) provides service to LGSP Mirror Nodes, forming the top level of the hierarchy. Master Station Nodes can typically have a connection to a GNSS master station, such as the GPS control segment.

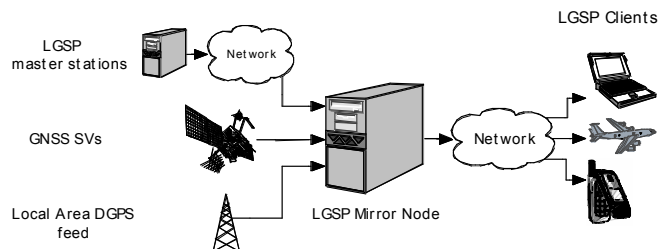
The primary function of LGSP Master Station Nodes is to present a standard interface to access GNSS data from one or more GNSS master stations. This also offers firewall-type functionality to isolate the GNSS master stations. LGSP Master Station Nodes can also source data from elsewhere, such as a Local Area DGPS feed.

LGSP Master Station Nodes will only accept connections from LGSP Mirror Nodes, and reject connections from LGSP clients. LGSP clients only connect to an LGSP Mirror Node to gain access. This avoids possible overloading of the LGSP Master Node, ensuring maximum availability.

LGSP Mirror Nodes (Figure 7) connect to one or more LGSP Master Station Nodes and mirror data to a local cache, which is updated periodically. LGSP Mirror Nodes provide both redundancy and load balancing. A Mirror Node that is geographically proximate to a client accessing it offers reduced latency as communications have less distance to travel, and greater security due to the shorter communication path, resulting in less exposure to malicious parties.

LGSP Mirror Nodes can also obtain data from other sources, such as a Local Area DGPS feed, as described above.

Additionally, an LGSP Mirror Node that loses all connections to other LGSP Mirror Nodes or LGSP Master Nodes can source GNSS data from a GNSS satellite. Such functionality can be considered an 'offline mode' that provides some level of service even in the event of multiple connection failures to LGSP Master Nodes or LGSP Mirror Nodes.



**Figure 7. LGSP Mirror Node Example.**

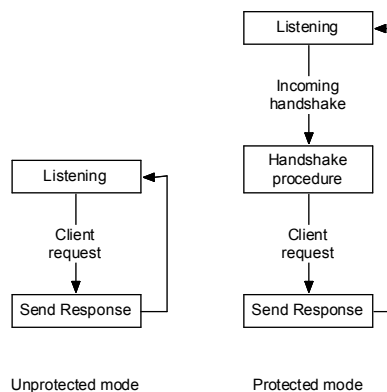
LGSP clients could be human portable devices with integrated GPS navigation systems such as a mobile phone, man portable radio, PDA (Portable Data Assistant) or a laptop, or GPS-equipped platform devices, such as an airborne platform, vehicle or ship.

LGSP clients will be equipped with GPS receiver hardware and other supporting infrastructure. In the case of a platform-based client, the LGSP server software can be integrated into the navigation computer, with few other modifications required, exploiting extant datalinks for LGSP access.

## LGSP COMMUNICATION

LGSP makes data available to clients via two messaging mechanisms: A request/response mechanism, and a multicast streaming mechanism.

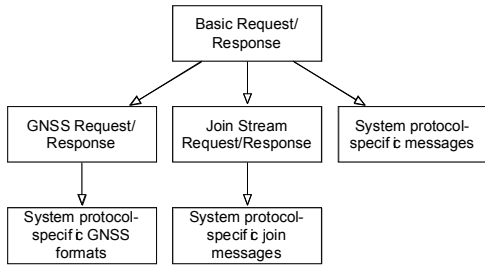
LGSP's request/response mode (Figure 8) is simple, and by not maintaining state between consecutive transactions is able to remain robust and efficient in the face of unreliable connections. As no persistent state is maintained between connections, few resources are expended on maintaining sessions. This is an important property for a protocol that may frequently operate over unreliable channels.



**Figure 8. LGSP Request/Response Mode Flowchart.**

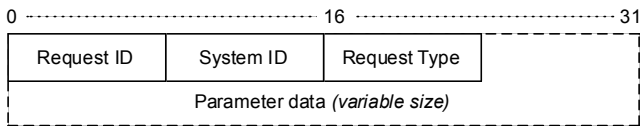
When operating in protected mode, intended for use over channels that lack adequate security or robustness, LGSP request/response transactions are encapsulated in an encryption layer, provided by the datagram variant of Transport Layer Security (D-TLS) [28]. Thus, a handshake

procedure must take place before communication begins (Figure 8), and some state must unavoidably be maintained for each session.



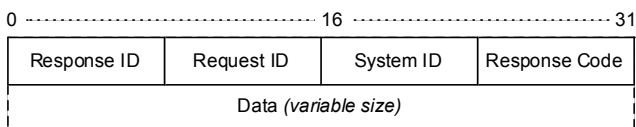
**Figure 9. LGSP Basic Message Format Hierarchy.**

LGSP defines a number of basic request/response messaging formats, which form a hierarchy of abstraction (Figure 9). The basic request and response message formats (Figure 10, Figure 11) form the basis of all LGSP communication.



**Figure 10. LGSP Basic Request Message.**

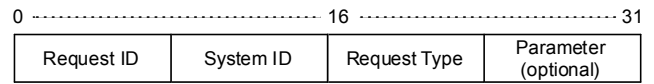
The basic LGSP request (Figure 10) format's Request ID field represents a unique identifier for every request – it is an 8 bit monotonically increasing integer, kept per-session. The System ID field identifies the LGSP system protocol being used (such as GPS, WAAS, or LGSP's management system protocol). The Request Type field identifies the kind of request, valid within the scope of the system protocol identified by the System ID field. This format provides for the addressing of up to 255 system protocols, and up to 255 request types within each system protocol. Following this header is a block of parameter data, which is left undefined at this abstract level.



**Figure 11. LGSP Basic Response Message.**

The basic LGSP response format (Figure 11) begins with a Response ID field that uniquely identifies the response – it is an 8 bit monotonically increasing integer, kept per session. The Request ID field identifies the preceding request, to allow the requesting entity the ability to recognise responses to prior requests. As described above, the System ID field identifies the system protocol in use. The Response Code provides feedback for the outcome of the request, and finally, a block of returned data follows. Again, for these abstract packet formats, the nature of this data is left undefined.

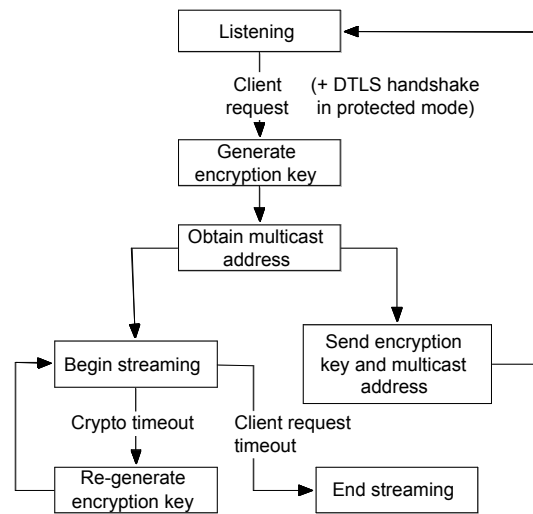
LGSP's multicast streaming mode offers a mechanism to distribute data to a large number of clients, with lower bandwidth and processor resource requirements than would otherwise exist with only a per-client request/response mode.



**Figure 12. LGSP Join Stream Request Message.**

LGSP clients can request to join a stream originating from the requested server (Figure 12). This technique minimises network and processor resources by using secure multicast technologies [RFC3740] to distribute data to all listening nodes, thereby bypassing the need for both repeated 'polling' and separate network connections for each listening node.

This message is standardised for all messaging formats that use streaming, unless extended parameters are required.

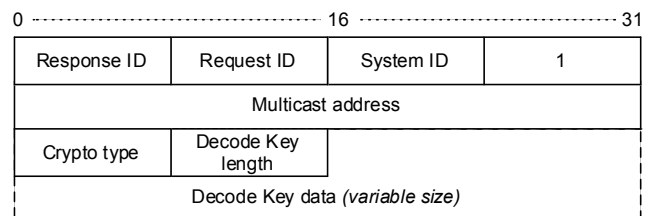


**Figure 13. LGSP Multicast Streaming Mode Flowchart.**

Once the LGSP server receives such a request, it generates an encryption key, and obtains a multicast address to begin broadcasting (Figure 13). The encryption key and address are sent to the requesting LGSP client, and the LGSP server begins streaming.

After receiving a join stream request message (Figure 12), a join stream response message (Figure 14) is sent to the requesting client. This response provides the requester with a multicast address and a key to decode the encrypted stream.

Subsequent joins by other clients simply subscribe the new clients to the created stream.

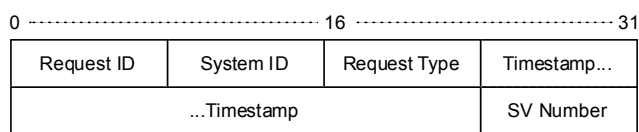


**Figure 14. LGSP Join Stream Response Message.**

After a timeout elapses during which no clients re-request the decode key, the broadcast is stopped, conserving resources.

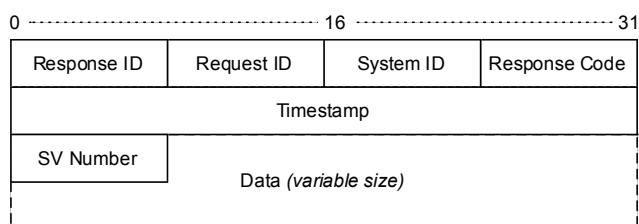
LGSP defines a generic message format for GNSS requests (Figure 15). This message contains a timestamp field and a SV (Satellite Vehicle) number, which gives the ability to

identify particular messages in the system, when coupled with the Request Type identifier.



**Figure 15. LGSP GNSS Request Message.**

The response message for the generic GNSS format (Figure 6) contains a timestamp field and SV number field, allowing identification of particular messages, and a variable size data field for returned data.



**Figure 16. LGSP GNSS Response Message.**

## ONGOING RESEARCH

Development of the Lightweight GNSS Support Protocol is well advanced. Definition of message formats and protocol state transitions are completed, and an Internet Draft was submitted in late July to the IETF, with the intention of publishing a Request For Comments (RFC) document, outlining LGSP as a future military and civil standard.

Future research directions involving LGSP include construction of an LGSP demonstrator platform, and integration into a location-aware smart mobile ad hoc network.

## REFERENCES

- [1] Russian Space Agency, "GLONASS Interface Control Document", 2002
- [2] U.S. Air Force, "NAVSTAR GPS Space Segment/Navigation User Interfaces", 2006
- [3] European Commission, "The Galilei Project: GALILEO Design Consolidation", 2003
- [4] C. Kopp, "GPS Guided Weapons", 1996, URL: <http://www.ausairpower.net/TE-GPS-Guided-Weps.html>
- [5] U.S. Federal Aviation Administration, "Performance Type One Local Area Augmentation System Ground Facility," 2002.
- [6] Loh, R., Wullschleger, V., Elrod, B., Lage, M., and F. Haas, "The U.S. Wide-Area Augmentation System (WAAS)," 1995.
- [7] Blackwell, Moeglein, M., and D. Nakayama, "A global DoD-optimized DGPS for precision-strike", 1995.
- [8] Vittorini, LD., "GPS URE/UE evolutionary improvements and end-user accuracy results", 1998.
- [9] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.
- [10] Place, J., Kerr, D., and D. Schaefer, "Joint Tactical Radio System", 2000.
- [11] Davis, K., "JTRS - An Open, Distributed-Object Computing Software Radio Architecture", 1999.
- [12] ANSI/IEEE, "802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2000.

- [13] Vaughan-Nichols, S., "Achieving wireless broadband with WiMax", 2004.
- [14] European Telecommunications Standards Institute, "Digital Cellular Telecommunications System (Phase 2+), General Packet Radio Service, Service Description, Stage 1", August 1999.
- [15] W. S. Ely, G. K. Grosby, K. W. McPherson, J. M. Stewart, "Flight Testing of the D8PSK/TDMA Datalink Technology for the Ground-based Regional Augmentation System", 15th International Technical Meeting of the Satellite Division of The Institute of Navigation, 2002
- [16] Air Services Australia, "Global Navigation Satellite System (GNSS) Augmentation Audit and Cost Benefit Analysis - Status Report", Air Services Australia report, April 1997
- [17] Murphy, T. "Ground Based Regional Augmentation Systems Architectures and Performance", October 2000
- [18] Place, J., Kerr, D., and D. Schaefer, "Joint Tactical Radio System", 2000.
- [19] Davis, K., "JTRS - An Open, Distributed-Object Computing Software Radio Architecture", 1999.
- [20] Hura, M., McLeod, G., Larson, EV., Schneider, J., Gonzales, D., Norton, DM., Jacobs, J., O'Connell, KM., Little, W., Mesic, R., and L. Jamison, "Interoperability: A Continuing Challenge in Coalition Air Operations", 2000.
- [21] Schiavone, LJ., "Airborne networking - approaches and challenges", 2004.
- [22] Rahnema, M., "Overview of the GSM system and protocol architecture", 1993.
- [23] Walter, T., Enge P., "Modernizing WAAS", *Proceedings of the ION GPS meeting*, 2004
- [24] Tyson, M., Kopp, C., "Defining Functional Requirements for a Lightweight GNSS Support Protocol (LGSP)", *6<sup>th</sup> International Conference on Computer and Information Science*, July 2007
- [25] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.
- [26] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
- [27] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.
- [28] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.
- [29] Stinson, C. W., "Internet Protocol (IP) Over Link-16", *Thesis at the Air Force Institute of Technology*, 2003
- [30] Kopp C., GPS in Networked Systems - Parts 1 and 2, *Defence Today*, Strike Publications, June through September, 2007.
- [31] Tyson M, Kopp C, "The Lightweight Global Navigation Satellite System (GNSS) Support Protocol (LGSP)", *Internet Draft*, 2007
- [32] Tyson M, Kopp C, "Lightweight GNSS Support Protocol (LGSP) Rationale", *Internal document*, 2007

*Michael Tyson, BCompSc (mtyson@csse.monash.edu.au, +61407754124) graduated in 2005 with a Bachelor of Computer Science, First Class Honours, from Monash University's Faculty of Information Technology, Melbourne, Australia, where he is currently undertaking a PhD. Michael's research interests include intelligent adaptive ad-hoc routing, radio propagation environment modelling, mobile station movement tracking and prediction, differential GPS over IP, power consumption optimisation and fairness in mobile ad-hoc networks, and ad-hoc network security.*

*Dr Carlo Kopp, IEEE, SMALAA, PEng graduated from the University of WA in Electrical Engineering with First Class Honours, in 1984. After more than a decade in industry engineering positions he completed an MSc in 1996, and a PhD in 1999, the latter dealing with long range microwave datalink via airborne radar phased arrays, and airborne ad hoc digital networks. He is currently at the Monash University Faculty of IT, with research interests in networking, security and information warfare. His other research interests include military technology and modern strategy.*