Fault Tolerance of the Global Navigation Satellite System using System-Level Diagnosis

Chad C. Lamb
Linda S. DeBrunner
John Fagan
Dept. of ECE
University of Oklahoma
Norman, Oklahoma 73019
(405) 325-4721
FAX: (405) 325-7066

Anindya Das
K. Thulasiraman
Dept. of Computer Science
University of Oklahoma
Norman, Oklahoma 73019
(405) 325-4042

Ralph Sexton
Satellite Navigation Division
Innovative Solutions
International, Inc.
Vienna, VA 22182
(703) 883-8088

Abstract

The Global Navigation Satellite System (GNSS) is a space-based positioning system that can track aircraft, to within a few feet, anywhere in the United States of America. With augmentations based in other countries, the GNSS becomes a truly global positioning system, able to track aircraft anywhere on the globe with accuracies on the order of a few feet. We investigate the application of System-Level Diagnosis (SLD) to the GNSS to assess the diagnosability and fault tolerance of the system. We show, in a deterministic manner, the number of faulty elements that can exist in the system and still allow for the accurate diagnosis of the system. Our deterministic approach is in contrast to other known probabilistic approach.

Introduction

The Global Positioning System (GPS) is a space-based positioning, velocity, and time system that has three major segments: space, control, and the user. The GPS Space Segment is composed of 24 space vehicles (SVs), i.e., satellites in six orbital planes. The SVs operate in circular 10,900 nautical mile orbits with a 12-hour period. The GPS Control Segment has five ground-based monitor stations, three of which have uplink capabilities, and a Control Station operated by the Department of Defense. The monitor stations use a GPS receiver to passively track all satellites in view and thus accumulate ranging data from the satellite signals. The information from the monitor stations is processed by the Control Station to determine satellite orbits and to update the navigation message of each satellite. The GPS User Segment consists of receivers that provide positioning, velocity, and precise timing to the user.

The Global Navigation Satellite System (GNSS), as defined here, is composed of GPS SVs and other augmentations which are added to provide the required accuracy, integrity, and availability for aircraft navigation. We use System-Level Diagnosis (SLD) [1,2] to determine the diagnosability and evaluate the availability of the GNSS. The Department of Transportation (DoT) and the Federal Aviation Administration (FAA) in the United States, along with similar agencies in other countries, have a vested interest in the GNSS and how well it performs for both civil and military applications.

The Global Navigation Satellite System

The GNSS, as shown in figure 1, is composed of the following components: GPS SVs, the Wide Area Augmentation System (WAAS), Air Traffic Control, and the aircraft. Each block in figure 1 represents a subsystem of the GNSS. The system is modeled using nodes to represent individual components and directed edges to represent the flow of information.

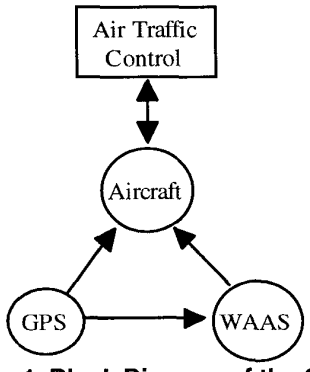


Figure 1 Block Diagram of the GNSS

A graph G = (U, E) represents the entire GNSS, which includes the elements in figure 1 and their subsystems, where U is the set of nodes in G and E is the set of edges of G. A subgraph of G, $G_{t,p} \subset G$, represents the GNSS as seen by the aircraft at some time t and some position p. $G_{t,p} \neq G$ since at any given time or place, the aircraft cannot "see" all the GPS SVs, or some SVs may not be in service (e.g., for scheduled maintenance). We are interested in the diagnosability of $G_{t,p}$ for any t, p.

After generating $G_{t,p}$ we create the test graph for $G_{t,p}$, called $G_{t,p}'$. Then, we perform our diagnosis and determine the diagnosability of the GNSS. In this paper, we investigate the worst case scenario for $G_{t,p}$, which is the situation where the aircraft can "see" the minimum number of GNSS elements. Further investigations will look at the other situations, and provide an overall assessment of the system, e.g., moving averages or standard deviations.

Generating the Test Graph $G_{t,p}'$

Another issue in modeling the GNSS is to identify the failure modes for each node. There are several differences between the graph considered here and the graphs in traditional multiprocessor systems, for which SLD is traditionally applied. All nodes are identical in graphs using traditional SLD, whereas they are not in this application. Furthermore, the edges of G may be faulty, whereas in traditional SLD the edges are generally assumed to be fault-free. Figure 2 shows the different types of nodes, and their associated edges, for the GNSS subsystems. In this paper, we model a link failure in the GNSS as a failure of the sending node, to simplify our model. In the GNSS, there are several different types of links: coaxial cabling, fiber optic cabling, and atmospheric transmissions.

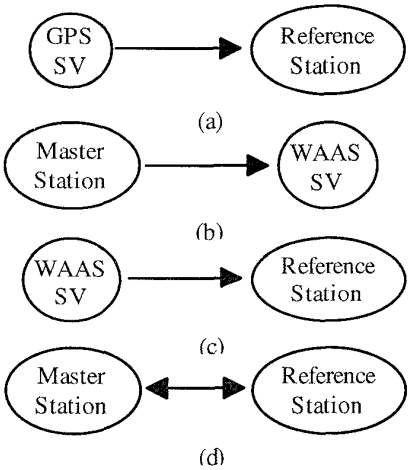


Figure 2 Components of Graph $G_{t,p}$

We use the comparison model, described later, to perform the diagnosis. This model requires bi-directional edges in the graph to perform the tests. Therefore, the GNSS must be modeled with bi-directional edges connecting the nodes to take advantage of this. In figure 2a, the GPS SV is monitored by the Reference Station. The Reference Station is connected to the Master Station (shown in figure 2d), and the Master Station can determine the status of the GPS SV. Therefore, we can model this as a bi-directional edge in the test graph $G_{t,p}'$ to connect the GPS SV nodes and the Reference Station nodes. (In figure 2, the direction of the edges are consistent with the graph $G_{t,p}$, not the test graph $G_{t,p}'$.)

In figure 2b, the Master Station sends information to the WAAS SV, the WAAS SV sends information to the Reference Station (shown in figure 2c), which then sends information back to the Master Station (figure 2d). Therefore, we can model this as a bi-directional edge in the test graph $G_{t,p}'$ to connect the Master Station nodes and the WAAS SV nodes, and similarly the WAAS SV nodes and the Reference Station nodes can share a bi-directional edge in the test graph $G_{t,p}'$. In figure 2d, the Master Station and the Reference Station are connected by a bi-directional edge since they can send information back and forth.

Figure 3 shows the test graph $G_{t,p}'$ for the node pairs in $G_{t,p}$. We use the comparison model [6] in the test graph $G_{t,p}'$, since all nodes are joined by bi-directional edges (Bi-directional edges are necessary to use the comparison model).

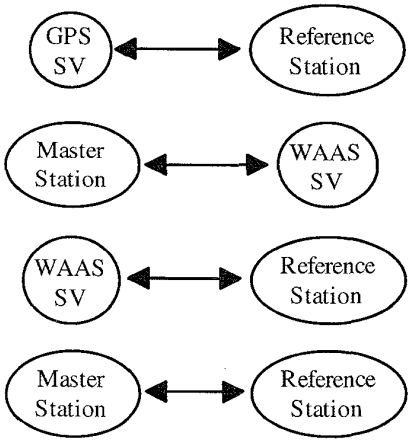


Figure 3 Components of Test Graph $G_{t,p}'$

However, we can simplify the test graph $G_{t,p}'$ by removing the Master Station node since it is inherently redundant and assumed not to fail. We combine the WAAS SV node in figure 3 with the Master Station node, and refer to this combined node as the WAAS node.

At this point, we can introduce the aircraft node into the graph $G_{t,p}'$. The goal of this research is to determine the diagnosability of the GNSS with respect to an aircraft using the system for navigation. Therefore, the aircraft node is the central node. The resulting components of the test graph $G_{t,p}'$ are shown in figure 4.

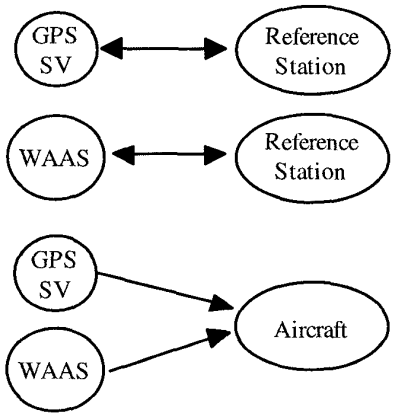


Figure 4 Components of the Modified $G_{t,p}'$

System-Level Diagnosis

To determine the diagnosability of the GNSS, we use the t-in-L_2 diagnosis theory developed in [6]. In this theory, a graph is uniquely diagnosable provided: (1) there are no more than LFC faulty nodes in the local neighborhood set of node x in the graph, and (2) there are no more than ELFC faulty nodes in the extended-local neighborhood set of node x in the graph. The local neighborhood set of node x is composed of the set of nodes whose distance from x is equal to one, while the extended-local neighborhood set of node x is composed of the nodes whose distance from x is less than or equal to two (see [7] for details on graph theory).

t-in-L_2 Diagnosis

The GNSS is diagnosable, that is, every node in the graph $G_{t,p}'$ can be uniquely labeled as faulty or fault-free, provided there are no more than LFC faulty nodes in the local neighborhood set of any node x and no more than ELFC faulty nodes in the extended-local neighborhood set of any node x. While the t-in-L_2 diagnosis theory is applicable to any node in the graph, we are only interested in x = aircraft node.

We must determine the values for LFC and ELFC, since in [6], the t-in-L_2 diagnosis theory is applicable to regular graphs, where a graph is called regular with degree b, if all nodes have the same degree, i.e. degree(x_i) = b, $\forall x_i \in U$. The GNSS is not a regular graph.

To simplify the model of the GNSS, we treat each node in the GNSS as identical nodes in the test graph $G_{t,p}'$. Then, two adjacent nodes are assigned identical tasks, and if their outputs match, then a test result of 0 is generated (a 0-link joins the two nodes). If the outputs do not match then a test result of 1 is generated (a 1-link joins the two nodes). So if two nodes are working properly, then they should produce the same output (and thus generate a 0-link). The collection of all such test outcomes is called a syndrome.

Now, after determining the syndrome, it must be interpreted it so we can label the nodes as faulty or fault-free. We chose the comparison model for this interpretation [1]. Using the comparison model to decode the syndrome, we must determine if x is faulty or fault-free, $\forall x \in U$. If, for example, $x,y \in U$ are joined by a 0-link, then all we know is the output of x matched that of y. For the comparison model, a 0-link signifies that the output of node x and node y matched, so either both x and y are fault-free or both are faulty. x and y could both be faulty in the same way so they produce the same output. Figure 5 shows the comparison model. When two nodes are faulty, the test result is unreliable (1/0) since two faulty nodes may have matched outputs, resulting in a 0-link, or unmatched outputs, resulting in a 1-link.

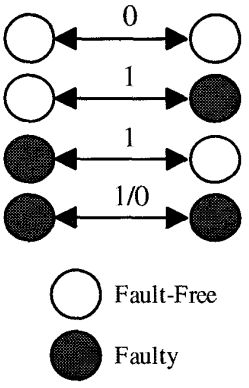
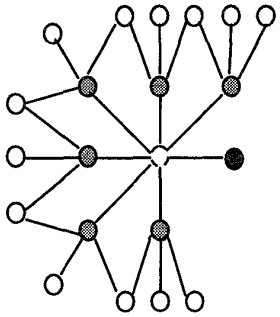


Figure 5 Comparison Model

Next we need to examine the test graph $G_{t,p}'$. We know from [5] that there are at least six GPS SV nodes and from [4] there is at least one WAAS node, $\forall t,p$. From [4] there are at least three Reference Station nodes for each GPS SV node, with some of those being shared. Thus, we have the graph in figure 6. This is a worst case scenario. The assignment of Reference Station nodes to GPS SV nodes was made somewhat arbitrarily, however, the specifics of this connection assignment have little or no impact on the diagnosability of the graph, provided there are at least three Reference Station nodes per GPS SV. We have not shown the connections between the WAAS node and the Reference Station nodes to simplify

the figure, however, these connections exist in the analysis.



GPS Aircraft
WAAS Reference Station
Note: connections between the WAAS node and the Reference Station nodes omitted for clarity

Figure 6 Worst Case $G_{t,p}'$

Diagnosis of GNSS

Let $\overline{N}$ be the set of nodes in L(x) that share a 0-link with x and N be the set of nodes in L(x) that share a 1-link with x. Similarly, $\overline{N}(\overline{N})$ is the set of nodes that share a 0-link with the nodes in $\overline{N}$ (not including the nodes in $\overline{N}$), $\overline{N}(N)$ is the set of nodes that share a 0-link with the nodes in N (not including the nodes in N), $N(\overline{N})$ is the set of nodes that share a 1-link with the nodes $\overline{N}$ (not including the nodes in $\overline{N}$), and N(N) is the set of nodes that share a 1-link with the nodes in N (not including the nodes in N). Let N_i be the node $z_i \in N$ that shares a 1-link with x and $N(N_i)$ be the set of nodes that share a 1-link with z_i, not including the node z_i. Similarly $\overline{N}(N_i)$ is the set of nodes that share a 0-link with z_i.

In the following arguments, the local fault constraint (LFC) is the maximum number of faulty nodes in the local neighborhood set of x, and the extended-local fault constraint (ELFC) is the number of faulty nodes in the extended-local neighborhood set of x, that can be tolerated and still correctly label the faulty and fault-free nodes. We use the notation L(x) to represent the set of nodes whose distance from x is one. We let t denote the maximum number of faults in the local neighborhood set of x and let t(m) denote the maximum number of faults in the extended local neighborhood set of x.

The following lemmas are stated here for completeness. The proofs are given in [6].

Lemma 1

Given a graph G with a local fault constraint (LFC) of no more than t faults in $L(x) \cup \{x\}$, $\forall x \in U$, where $\lfloor \text{degree}(x)/2 \rfloor \le t \le \text{degree}(x) - 1$ and F is the set of faulty nodes in G, then

1. If $|N| > t$, then $x \in F$
2. If $|N| < \text{degree}(x) - t + 1$, then $x \in U - F$.

Lemma 2

Given a regular graph G, with a local fault constraint (LFC) of no more than t faults in $L(x) \cup \{x\}$, $\forall x \in U$, and let F be the set of faulty nodes in G, then

1. If $\exists i$, $|N(N_i)| \ge t$, and
   if $|N| \ge \text{degree}(x) - t + 2$ and for $i = [\text{degree}(x) - t + 2]$ to $|N|$, $|N(N_i)| = \text{degree}(x) - 1$, then $x \in U - F$.
2. If $\exists i$, $|N(N_i)| < [\text{degree}(x) - t]$, then $x \in F$.

Lemma 3

Given a graph G and syndrome S, let F be an allowable fault set for S such that $F \neq U$. Let C (or C′) be the set of nodes that have multiple paths of length 2 with x and are counted twice in the computation of F(x) (or F′(x)). Then, the number of faulty nodes in the extended-local neighborhood set of x, $\forall x \in U$ is:

1. $|F(x)| \ge |N| + |\overline{N}(N)| + |N(\overline{N})| - |C|$, if $x \in U - F$
2. $|F'(x)| \ge 1 + |\overline{N}| + |\overline{N}(\overline{N})| + \sum_{i=1}^{|N|} \min[\,|N(N_i)|, \deg(x) - |N(N_i)|\,] - |C'|$, if $x \in F$.

Theorem 1

Given a graph G and syndrome S, let F be an allowable fault set for S such that $F \neq U$. If there are no more than t = 6 faults in the local neighborhood set of x, where x = aircraft node, and no more than t(m) = 10 faults in the extended-local neighborhood set of x, then G is t-in-L_2 diagnosable.

Proof Outline

In proving the theorem, consider the following conditions:

1. $|N| > t$
2. $\exists i$, $|N(N_i)| < [\text{degree}(x) - t]$
3. $|F(x)| - |C| > t(m)$, where $F(x) = N \cup \overline{N}(N) \cup N(\overline{N})$.

We show that the node x is faulty if and only if at least one of these conditions is true. We use Lemmas 1, 2, and 3 to show this. The sufficiency of these conditions is shown by directly using lemma 1 (2,3) for condition 1 (2,3). To prove the necessity, we assume x is faulty and none of the conditions are true, and we arrive at a contradiction.

From the t-in-L_2 diagnosis theory, we find that the LFC = degree(aircraft node) - 1 = 6, and the ELFC = 10. Therefore, the GNSS can have six faulty nodes in the local neighborhood set of the aircraft (which includes the aircraft node) and at most ten faulty nodes in the extended-local neighborhood set of x (which includes the six faulty nodes in the local neighborhood set of x), and

the system can still diagnosis correctly the faulty and fault-free nodes in the graph.

Conclusions

In summary, the GNSS is the future of aircraft navigation throughout the world. Augmentation systems for GPS are being designed in the United States, Australia, Canada, Europe, Japan, Russia, and other countries. Therefore, there is an immediate need for an evaluation of their performance. To date, there have been very few studies on the performance of the entire system, only subsystem performance evaluations [3,4]. This research evaluates the combined GNSS [5], rather than evaluating the parts individually, using a deterministic approach in system-level diagnosis.

We have shown the GNSS, for the worst case scenario, can have up to 6 faults in the local neighborhood set of x, and up to 10 faults in the extended-local neighborhood set of x, and still accurately label all nodes as faulty or fault-free. Since there are only 7 nodes adjacent to x, an LFC = 6 is a significant percentage of those nodes. If we consider other cases where there are more than 7 nodes adjacent to x, the t-in-L_2 diagnosis theory allows us to have degree(x) - 1 faulty nodes, so the benefit is not lost as the degree of x increases.

Additional research is needed to evaluate the GNSS with additional elements, like GLONASS (the Russian Global Navigation Satellite System) and EGNOS (the European system). Using the approach shown here, the addition of other augmentations requires little more than adding nodes to the test graph.

References

[1] F. P. Preparata, G. Matze, R. T. Chien, "On the Connection Assignment Problem of Diagnosable Systems," *IEEE Trans. Electr. Compt.*, Vol. EC-16, pp. 848-854, 1967.

[2] A. Das, K. Thulasiraman, V. K. Agarwal, K. B. Lakshmanan, "Multiprocessor Fault Diagnosis Under Local Constraints," *IEEE Trans. on Computers*, vol. 42, pp. 984-988, Aug. 1993.

[3] V. Ashkenazi, et al., "Design of a GNSS: Coverage, Accuracy and Integrity," *Proceedings of ION GPS-95*, pp. 463-472, 1995.

[4] W. Poor, T. Albertson, P. Yen, "A Wide Area Augmentation System (WAAS) Service Volume Model and Its Use in Evaluating WAAS Architecture and Design Sensitivities," *Proceedings of ION GPS-95*, pp. 629-637, 1995.

[5] M. Sams, et al., "Optimum Satellite Constellations for Civil Navigation Use," *Proceedings of ION GPS-96*, pp. 1151-1160, 1996.

[6] C. Lamb, *Graph Models and System Diagnosis*, Ph.D. Dissertation, U. of Oklahoma, to appear Dec. 1997.

[7] Frank Harary, *Graph Theory*, Addison-Wesley Publishing, Reading, MA, 1969.