

Availability Analysis of Satellite Positioning Systems for Aviation using the PRISM Model Checker

Yu Lu*, Alice Miller, Chris Johnson

School of Computing Science
University of Glasgow
Glasgow, United Kingdom

* y.lu.3@research.gla.ac.uk

{alice.miller, christopher.johnson}@glasgow.ac.uk

Zhaoguang Peng, Tingdi Zhao

School of Reliability and Systems Engineering
Beijing University of Aeronautics and Astronautics
Beijing, China

ghpeng@dse.buaa.edu.cn

ztd@buaa.edu.cn

Abstract—This paper highlights an application of probabilistic model checking to satellite positioning systems for aircraft guidance. After introducing our formal approach based on using the PRISM model checker, we built a model of a global navigation satellite system (GNSS) based positioning system for a specific flight in the probabilistic π -calculus, a process algebra which supports modelling of concurrency, uncertainty, and mobility. After that, we encode our model into the PRISM language. We then analyse the availability properties that relate to the dependability and overall performance of the underlying system. The aim of our research is to use PRISM to assist industrial designers and developers of the GNSS.

Keywords—GNSS; satellite positioning; aviation; availability analysis; probabilistic model checking

I. INTRODUCTION

Satellite positioning systems are used within the aviation sector extensively. A three-dimensional global navigation satellite system (GNSS) enables an aircraft to determine its position (latitude, longitude, and altitude) anywhere on or above the earth. Data transmitted from a navigation and communication satellite provides the user with the time, the precise orbital position of the satellite and the position of other satellites in the system. In the past, they were only applied for military purposes. However nowadays they are used for a wide range of civil aviation applications, including navigation, communication, tracking, and flight management.

A number of previous EC projects such as GADEROS, GRAIL, LOCASYS, and SATLOC, have proved the feasibility of introducing GNSS in non-critical systems by means of theoretical studies and demonstrations. The current EC project “European Train Control System Advanced Testing and Smart Train Positioning System” (EATS) [1] proposes a novel positioning system based on different techniques that have proved useful from other industry viewpoints such as using information sources from GNSS, UMTS, and GSM. Furthermore, reliability, availability, maintainability, and safety (RAMS) [2]–[4] is proposed as a measure to analyse the dependability of both mission-critical and safety-critical applications.

Availability requirements are identified as the most challenging obstacles towards GNSS aided positioning systems in [2]. Many approaches can be used to analyse the availability properties. Among them, simulation, analytical analysis, and

numerical analysis are popular and practical. Each of them has its advantages and disadvantages that we do not discuss in this paper. We consider probabilistic model checking, a numerical analysis technique based on Markov models. It is a formal method for analysing and verifying quantitative properties of systems such as as time, stochastic behaviour or resources. It is therefore highly suitable for modelling characteristics of our system. The basic idea is to first build a (discrete-time or continuous-time) Markov chain or Markov decision process that captures the behaviour of the system, and then to use the model to analyse precisely specified properties using some temporal logics. This analysis is automatically performed by using the PRISM model checker [5], and it involves a combination of a traversal of the state transition system of the model and numerical computation.

A PRISM specification can be generated directly via a Markov chain variant described using the PRISM reactive modules language [6]. Alternatively, a high level model (using timed automata, or a process algebra, say) can be translated into the PRISM language. According to PRISM’s manual, the latter approach can be more efficient than the former. This is due to the fact that PRISM is a symbolic model checker and the underlying data structures used to represent the system specification may function better when there is a high-level structure and regularity to exploit.

In this paper we first specify the communication between an aircraft and the associated satellites, taking into account their combined mobility. We then analyse the models of the aircraft and satellite set independently before the combined system. Note that behaviour of the system contain a high level of uncertainty (e.g., in signal transmission unreliability due to solar radiation). In all our models we specify the system using the probabilistic π -calculus. Since PRISM only model checks expressions in the reactive modules language, and this does not allow for component mobility, so it is not currently possible to model check the underlying process algebraic models directly. In order to allow for automatic verification using PRISM, the underlying continuous-time Markov chains (CTMCs) semantic models of our specification are first constructed using rules presented in [7].

Our paper is organised as follows. In Section II we describe the underlying GNSS based positioning systems. In Section III the use of probabilistic model checking is introduced. In

Section IV we present our formal model of the system for a navigation mission of a specific aircraft in the probabilistic π -calculus and its associated CTMC model respectively. Then, we analyse availability properties using the PRISM model checker in Section V. The related work is given in Section VI. Finally, in Section VII we conclude the paper and propose future work.

II. GNSS BASED POSITIONING SYSTEMS

A GNSS consists of three major parts: space segment, control segment and user segment. Failure of any subsystem will lead to errors in the final positioning. Fig. 1 illustrates typical GNSS segments. First, the monitor stations (*MS*) measure the pseudo-range of visible satellites and send the data to the master control station (*MCS*). The MCS is responsible for collecting and tracking data from each monitor station and calculating the satellite orbit and clock parameters using a Kalman filter. The results are transmitted to ground antennas (*GA*) and then to the satellites. Under the control of the *MCS*, the clock error, satellite ephemeris, navigation data, etc., are calculated and then transmitted to the corresponding satellite, and at the same time, the information is verified. The satellites transmit data associated with their current states to the users (*U*). The users need to use the position information provided by at least four satellites to determine the position during navigation [8].

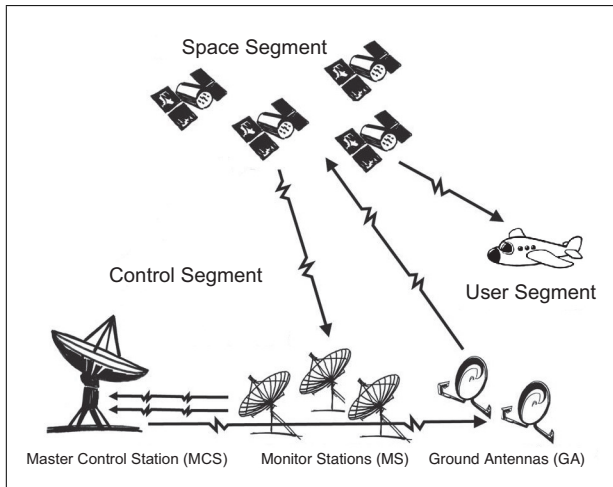


Fig. 1. GNSS Segments.

Errors may exist in the process of information transmission, and if these errors are passed on all the way to the user, the position provided by the navigation system is unusable. The space segment of a standard GNSS is composed of 24 global navigation satellites. The arrangement of the GNSS satellite constellation can guarantee that four or more satellites can be observed at the same time from any location at any time and ensure that the propagation of the satellite signal will not be disturbed by the environment. Therefore, a GNSS based positioning system should be a global and around-the-clock navigation system that continuously provides uninterrupted real-time navigation.

The GNSS control segment is implemented in the form of a number of detecting and measuring systems distributed across

various locations in the world. The control segment continuously monitors and tracks the satellites. The roles of control segment components include: (1) monitoring of the satellite's operation and orbit states; (2) tracking and computation of the orbit parameters of satellites and then sending them to the satellites to be retransmitted to the users via a navigation message; (3) synchronisation of the clocks of satellites; (4) scheduling for satellites when necessary.

First, the monitor stations measure the pseudo-range of visible satellites every 6 seconds, correct them with ionospheric and meteorological data, smooth the measurement to generate data with a time interval of 15 seconds, perform smoothing again to generate data with a 15 min time interval, and finally send the data to the master control station. The master control station is responsible for collecting and tracking data from each monitor station and calculating the satellite orbit and clock parameters using a Kalman filter. The results are transmitted to ground antennas and then to the satellite. Under the control of the master control station, the clock error, satellite ephemeris, navigation data, etc., are calculated and then transmitted to the corresponding satellite, and at the same time, the information is verified. The satellites transmit data associated with their current states to the users. The users need to use the position information provided by the satellites for positioning during navigation. In general, at least four satellites are required to determine the user's position.

In this process, the accuracy of the information that each subsystem provides is critical and depends directly on the navigation accuracy. From the monitor station to the master control station, from the master control station to the ground antenna, from the ground antenna to the satellite, and from the satellite to the user, the entire process is implemented by information transmission. Errors may exist in the process of information transmission, and if these errors are passed on all the way to the user, the position provided by the navigation system is unusable.

III. PROBABILISTIC MODEL CHECKING

Our preliminary research into the verification of satellite systems, in which we restrict our analysis only to a single satellite and a satellite constellation but not a navigation mission, is presented in [9], [10]. In an approach similar to ours [11], a probabilistic model checking approach has been used to analyse the performance of mobile wireless sensor networks. The major difference between this work and ours is that they model the mobile network using the stochastic π -calculus and translate the model into the PRISM language, whereas we model our mobile system using the probabilistic π -calculus and translate the model into the PRISM language using a different set of rules.

Our formal method consists of four stages. First, we model in the probabilistic π -calculus the behaviours of the navigation satellite systems. This model is composed of two separate models characterising the communications between different segments and their mobility. The latter must be able to be modified without changing the former. Second, the global model is translated into the PRISM language, and a corresponding CMC generated using PRISM (stage 1). The availability requirements that the system is required

to satisfy are formalised in some temporal logics (stage 2). These quantitative properties are then checked using PRISM (stage 3). They can be checked according our specific flight navigation mission. Finally, we analyse the results given by PRISM (stage 4).

A. Overview of the Probabilistic π -Calculus

The probabilistic π -calculus (π_{proc}) adds a discrete probabilistic choice operator to the classical π -calculus. This probabilistic operator associates internal actions with probabilities.

Definition 1. *Processes use names to perform actions. The types of actions include:*

- τ : a silent action that corresponds to an internal interaction between sub-processes.
- $x(y)$: an input action in which a process receives a name y on channel x .
- $\bar{x}(y)$: an output action in which a process sends a name y on channel x .
- $\bar{x}(y)$: an bounded output action in which a process sends a bound name y on channel x .

Definition 2. *We assume P and P_i range over terms and α ranges over actions. We assume a countable set of names that range over x, y, x_i , where $i \in \{1, 2, \dots, n\}$. A **process** P is defined in π_{proc} using the following syntax (where I is an index set, $p_i \in (0, 1]$ with $\sum_{i \in I} p_i = 1$, and A is a process identifier):*

- $\alpha ::= \tau \mid x(y) \mid \bar{x}(y)$
- $P ::= \mathbf{0} \mid \alpha.P \mid \sum_{i \in I} P_i \mid \sum_{i \in I} p_i \tau.P_i \mid P|P \mid vxP \mid [x = y]P \mid A(x_1, x_2, \dots, x_i, \dots, x_n)$.

We now give an informal description of π_{proc} . The inactive process $\mathbf{0}$ can perform no actions. Note that there are two types of choice operator: nondeterministic choice $\sum_{i \in I} P_i$ and probabilistic choice $\sum_{i \in I} p_i \tau.P_i$. The first is common in the standard π -calculus, and the second is a new operator in π_{proc} . Branches of the probabilistic choice operator are normally prefixed with τ actions. Thus, the process $\sum_{i \in I} p_i \tau.P_i$ selects an index $i \in I$ with probability p_i , performs a τ action, and then evolves to P_i .

The parallel composition of processes P_i and P_j is $P_i|P_j$, and can be either asynchronous or synchronous (via matching input and output actions). The restriction vxP locally sets the scope of x in process P , so x is treated as a new and unique name within P . The process $[x = y]P$ can evolve into process P only if x and y are equal. Finally, $A(x_1, x_2, \dots, x_i, \dots, x_n)$ corresponds to a process definition clause with the form $P = A(x_1, x_2, \dots, x_i, \dots, x_n)$.

Definition 3. *The operational semantics of π_{proc} are typically expressed in terms of Markov Decision Processes (MDPs) or Probabilistic Automata (PAs). The symbolic semantics of π_{proc} is expressed in terms of probabilistic symbolic transition graphs (PSTGs). These are a simple probabilistic extension of the symbolic transition graphs in [12].*

B. The PRISM Model Checker

In this paper, we use the PRISM probabilistic model checker [5]. Markov models to be verified using PRISM are specified using the PRISM modelling language which is based on the Reactive Modules formalism [6]. A fundamental component of this language is a *module*. A system is represented as the parallel composition of a number of modules. A module is specified as:

module *name* ... **endmodule**

A module definition consists of two parts: one containing variable declarations, and the other *commands*. At any time, the *state* of a model is determined by the current value of all of the variables of all of the components (modules). A variable declaration has the form:

$x : [0..2] \mathbf{init} \ 0;$

In this example, variable x is declared, with range $[0..2]$ and initial value 0. The behaviour of each module is specified using commands, which include a guard and one or more updates of the form:

$[action] \mathit{guard} \rightarrow \mathit{rate} : \mathit{update}$

or,

$[action] \mathit{guard} \rightarrow \mathit{rate}_1 : \mathit{update}_1 + \mathit{rate}_2 : \mathit{update}_2 + \dots$

The (action) label is optional, and is used to force two or more modules to synchronise. Updates in commands are labelled with positive valued rates [5] for CTMCs. The $+$ indicates the usual non-deterministic choice. Within a module, multiple transitions can be modelled either as different individual updates in a command, or as multiple commands with overlapping guards. The following examples:

$\begin{bmatrix} [] \\ [] \end{bmatrix} x = 0 \rightarrow 0.5 : (x' = 0);$
 $\begin{bmatrix} [] \\ [] \end{bmatrix} x = 0 \rightarrow 0.8 : (x' = 1);$

and

$[\] x = 0 \rightarrow 0.5 : (x' = 0) + 0.8 : (x' = 1);$

are equivalent. The guard $x = 0$ indicates that command is only executed when variable x has value 0. The updates $(x' = 0)$ and $(x' = 1)$ and their associated rates indicate that the value of x will remain at 0 with rate 0.5 and change to 1 with rate 0.8. In a CTMC, when multiple possible transitions are available in a state, a race condition occurs [13]. The rate of the synchronised transition is the product of all the individual rates.

C. Continuous Stochastic Logic

In this paper, we use Continuous Stochastic Logic (CSL) [14], [15] to specify availability properties. CSL is inspired by the logic Computation Tree Logic (CTL) [16], and its extensions to discrete time stochastic systems (PCTL) [17], and continuous time non-stochastic systems (TCTL) [18]. There are two types of formulae in CSL: state formulae, which are true or false in a specific state, and path formulae, which are true or false along a specific path.

Definition 4. Let $a \in AP$ be an atomic proposition, $p \in [0, 1]$ be a real number, $\bowtie \in \{\leq, <, >, \geq\}$ be a comparison operator, and $I \subseteq \mathbb{R}_{\geq 0}$ be a non-empty interval. The syntax of CSL formulas over the set of atomic propositions AP is defined inductively as follows:

- $true$ is a state-formula.
- Each $a \in AP$ is a state formula.
- If Φ and Ψ are state formulas, then so are $\neg\Phi$ and $\Phi \wedge \Psi$.
- If Φ is state formula, then so is $\mathcal{S}_{\bowtie p}(\Phi)$.
- If φ is a path formula, then $\mathcal{P}_{\bowtie p}(\varphi)$.
- If Φ and Ψ are state formulas, then $\mathcal{X}_I\Phi$ and $\Phi\mathcal{U}_I\Psi$ are path formulas.

Formula $\mathcal{S}_{\bowtie p}(\Phi)$ asserts that the steady-state probability for a state satisfying Φ meets the bound $\bowtie p$. Similarly, formula $\mathcal{P}_{\bowtie p}(\varphi)$ asserts that the probability measure of the paths satisfying φ meets the bound given by $\bowtie p$. The operator $\mathcal{P}_{\bowtie p}(\cdot)$ replaces the usual CTL path quantifiers \exists and \forall . Intuitively, $\exists\varphi$ represents that there exists a path for which φ holds and corresponds to $\mathcal{P}_{>0}(\varphi)$, and $\forall\varphi$ represents that for all paths φ holds and corresponds to $\mathcal{P}_{>1}(\varphi)$. The temporal operator \mathcal{X}_I is the timed variant of the standard next operator in CTL; the path formula $\mathcal{X}_I\Phi$ asserts that a transition is made to a Φ state at some time point $t \in I$. Operator \mathcal{U}_I is the timed variant of the until operator of CTL; the path formula $\Phi\mathcal{U}_I\Psi$ asserts that Ψ is satisfied at some time instant in the interval I and that at all preceding time instants Φ holds.

One of the most important operators is the P operator, which is used to reason about the probability of an event. The P operator is applicable to all types of models supported by PRISM. It is often useful to compute the actual probability that some behaviour of a model is observed. Thus, a variation of the \mathbf{P} operator to be used in PRISM, i.e., $\mathbf{P}_{=?}[pathprop]$, which returns a numerical rather than a Boolean value (i.e., the probability that $pathprop$ is true). In our paper, we are interested in directly specifying reliability, availability, and maintainability properties which evaluate to a numerical value. For example, we might wish to calculate the probability that process 1 terminates before process 2 does (say). This can be specified as $\mathbf{P}_{=?}![proc2_terminate U proc1_terminate]$, where U is the “until” temporal operator.

Another important operator we use is the \mathbf{R} operator, which specifies a cumulative reward property that associate a reward with each path of a model, but only up to a given time bound. The property $\mathbf{R}_{=?}[C \leq t]$ corresponds to the reward cumulated along a path until t time units have elapsed. For CTMCs, the bound t can evaluate to a real value. Some typical examples of properties using \mathbf{P} and \mathbf{R} operators can be found on the Property Specification section of the PRISM website.

D. Translation Rules

For closed and finite processes (i.e., which do not replicate themselves), the semantics of a probabilistic π -calculus process can be represented by a CTMC [7].

We assume that the set of all names in the system is \mathcal{N} , which is partitioned into disjoint subsets: \mathcal{N}^{fn} , the set of all

free names appearing in processes $P_1, P_2, \dots, P_i, \dots, P_n$, and $\mathcal{N}_1^{bn}, \mathcal{N}_2^{bn}, \dots, \mathcal{N}_i^{bn}, \dots, \mathcal{N}_n^{bn}$, the sets of input-bound names for processes $P_1, P_2, \dots, P_i, \dots, P_n$. The translation rules of a π_{proc} model into the PRISM language, defined in [7], can be summarised as follows.

- Rule 1. Each of the n sub-processes P_i becomes a PRISM module with the same name.
- Rule 2. Module P_i has $|\mathcal{N}^{bn}|+1$ local variables. Each element Q_j^i of $S_i = \{Q_1^i, \dots, Q_k^i\}$, which is the set of the states of process P_i after each of its transitions (In [7], the set of all these states is called the PSTG of P_i), becomes an integer variable s_i whose values vary from 1 to k .
- Rule 3. Each bound name x_j^i of process P_i has a corresponding variable x_j^i with range $0, \dots, |\mathcal{N}^{fn}|$ and it is initialised to 0.
- Rule 4. The model includes $|\mathcal{N}^{fn}|$ integer constants, one for each free name, which are assigned distinct, consecutive non-zero values. If the value of variable x_j^i is equal to one of these constants, then the corresponding bound name has been assigned the appropriate free name (by an input action). On the contrary, $x_j^i = 0$ means that no input to the bound name has occurred yet.
- Rule 5. For each free name x that models a communication channel between processes, we add a constant $rate_x$ whose value is equal to the rate associated to the channel x .
- Rule 6. (*Probabilistic internal transition*). For a transition $Q_i \xrightarrow{M, \tau} \{p_1 : R_1^i, \dots, p_m : R_m^i\}$, we add the command:

$$\square (s_i = Q_i) \ \& \ M \rightarrow p_1 : (s'_1 = R_1^i) + \dots + p_m : (s'_m = R_m^i).$$
- Rule 7. (*Output on free name*). Process P_i outputs y on free name x to P_j . For a transition $P_i \xrightarrow{M, \bar{x}(y)} R_i$, where $x \in \mathcal{N}^{fn}$, we add, for each $j \in \{1, \dots, n\} \setminus \{i\}$, the command:

$$[x_P_i_P_j_y] (s_i = P_i) \ \& \ M \rightarrow (s'_i = R_i).$$

The channel x , sender P_i , receiver P_j , and sent name y are all encoded in the action label. See [7] for details.

- Rule 8. (*Output on bound name*). Process P_i outputs y on bound name x to P_j . For a transition $P_i \xrightarrow{M, \bar{x}(y)} R_i$, where $x \in \mathcal{N}_i^{bn}$, we add, for each $a \in \mathcal{N}^{fn}$ and $j \in \{1, \dots, n\} \setminus \{i\}$, the command:

$$[a_P_i_P_j_y] (s_i = P_i) \ \& \ M \ \& \ (x = a) \rightarrow (s'_i = R_i).$$

This is similar to Rule 7 except that it includes a command for each possible value a of x .

- Rule 9. (*Input on free name*). Process P_j inputs z on free name x from P_i . For a transition $P_i \xrightarrow{M, x(z)} R_i$, where $x \in \mathcal{N}^{fn}$, we add, for each $y \in \mathcal{N} \setminus \mathcal{N}_i^{bn}$ and $j \in \{1, \dots, n\} \setminus \{i\}$, the command:

$$[x_P_j_P_i_y] (s_i = P_i) \ \& \ M \rightarrow (s'_i = R_i) \ \& \ (z' = y).$$

For input actions, an extra assignment ($z' = y$) is added to consider each possible received name y . It models the update of the bound name z to y .

- Rule 10. (*Input on bound name*). Process P_j inputs z on bound name x from P_i . For a transition $P_i \xrightarrow{M,x(z)} R_i$, where $x \in \mathcal{N}_i^{bn}$, we add, for each $a \in \mathcal{N}^{fn}$, $y \in \mathcal{N} \setminus \mathcal{N}_i^{bn}$ and $j \in \{1, \dots, n\} \setminus \{i\}$, the command:

$$[a_P_j_P_i_y] (s_i = P_i) \ \& \ M \ \& \ (x = a) \rightarrow (s'_i = R_i) \ \& \ (z' = y).$$

This rule combines elements of Rules 8 and 9, since a command is added to consider each possible pairing of channel a that x may represent and name y that may be received. See [7] for details.

In addition, Rules 9 and 10 add some commands that need to be removed. More specifically, labels $x_P_i_P_j_y$ appear on a command of each module P_j , but do not appear in any of the commands in module P_i . Therefore, commands with such action labels are removed from P_j .

IV. SYSTEM SPECIFICATION

A. Reference Models

In particular, we analyse a navigation mission for a specific flight, which was from Beijing to Guangzhou, and the entire flight time was 2 hours 35 minutes. The specific time was January 2, 2012 (Beijing time); the flight departed at 12:00 and arrived in Guangzhou at 14:39. The entire flight was guided sequentially by 17 GPS satellites. Although the aircraft could generally receive satellite signals from more than 4 satellites at a time, usually only the signals from the four satellites with the best signals were used by the receiver for calculating the position. According to NASA, 7 out of 17 satellites can be chosen in our study based on their navigation times and the mission of the flight. The Space Vehicle Numbers (SVNs) of these 7 GPS satellites were: *SVN49*, *SVN39*, *SVN55*, *SVN58*, *SVN57*, *SVN51*, and *SVN36* respectively, as illustrated in Fig. 2, and their parameters are shown in Table I.

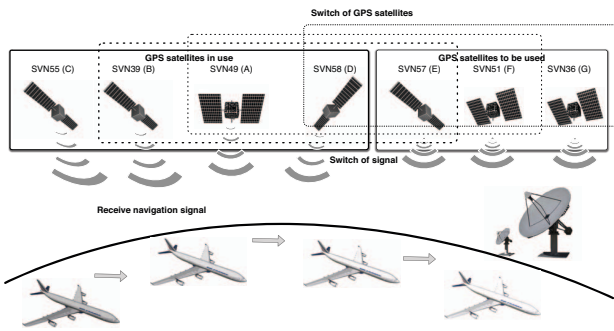


Fig. 2. GPS Constellations for an Air Line.

The reference model comprises 5 processes: U , MS , MCS , GA and a satellite A . Each process transmits information to objects to which it is connected. U receives a satellite signal. A receives information from the GA which it then transmits to the MS and U . The MS receives information from the satellite and transmits it to the MCS . As for the

MS , it analyses the data from the MS and transmits it to the GA . The GA receives the control commands from the MCS and sends them to A . The US National Geospatial-Intelligence Agency (NGA) provides GPS satellites' status data available daily¹.

B. Formal Models

There are two kinds of movement: the physical movement of satellites A, B, \dots, G and the aircraft U , and the virtual movement of communication links between them. But these two are independent. Their combined physical movement gives rise to the virtual movement of the link between them². We consider a GPS satellite constellation corresponding to the reference models in Fig. 3, featuring one GA , MS , and MCS as the control segment (CS), one aircraft U as the user segment, and seven satellites (A, B, \dots, G) as the space segment. We assume that GA and MS can always communicate with the seven satellites via the communication channels at the same time.

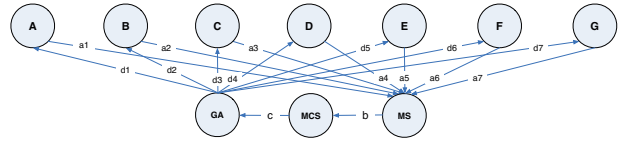


Fig. 3. Reference Model of Control and Space Segments.

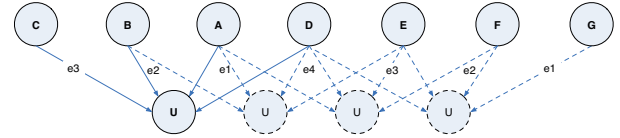


Fig. 4. Reference Model of User and Space Segments.

1) *Control Segment*: Here, navigation information mainly refers to the data describing the on-orbit state of satellites that are transmitted by the navigation satellites. Satellites in this system do not exchange information with one another. In the real world, all GPS satellites are monitored by a set of 6 monitor stations. In this paper, we make the simplifying assumption that there is a single monitor station, which is essentially a combination of the 6 stations. As a result, each satellite transmits information to the monitor station independently and simultaneously.

The π_{prob} model of the monitor stations is: $P_S = P_{SA} | P_{SB} | P_{SC} | P_{SD} | P_{SE} | P_{SF} | P_{SG}$, where $P_{SA}, P_{SB}, P_{SC}, P_{SD}, P_{SE}, P_{SF}$ and P_{SG} denote the communication processes between satellites A, B, \dots, G and the monitor station respectively. Due to space limitations, only the processes associated with satellite A are given here, and all others can be derived similarly. These detailed processes are shown as follows:

$$\begin{aligned} P_{SA} &\triangleq va1.a1(x).([x = m1].P_{SA1} + [x = m2].P_{SA2}) \\ P_{SA1} &\triangleq vb.(\alpha_1 \bar{b}(m1).P_{SA} + (1 - \alpha_1) \bar{b}(m2).P_{SA}) \\ P_{SA2} &\triangleq \bar{b}(m2).P_{SA} \end{aligned}$$

¹<http://www.navcen.uscg.gov/?Do=constellationStatus>

²The links and their movement are obtained using the modelling, simulation, analysis, and operations software Satellite Tool Kit (STK).

TABLE I. PARAMETERS AND AVAILABILITY OF NAVIGATION SATELLITES.

No	SVN	Launch date	Model	Life (years)	Reliability	Navigation interval	Running time (seconds)	Effective time (seconds)	Availability (%)
A	49	24/03/2009	Block IIRM	10.0	0.80	12:00-14:29	8940	8935.069	99.9449
B	39	26/01/1993	Block IIA	7.5	0.70	12:00-13:55	6900	6896.188	99.9447
C	55	17/10/2007	Block IIRM	10.0	0.80	12:00-13:15	4500	4497.518	99.9449
D	58	17/11/2006	Block IIRM	10.0	0.80	12:00-14:35	9300	9294.871	99.9449
E	57	20/12/2007	Block IIRM	10.0	0.80	13:15-14:35	4800	4797.352	99.9449
F	51	11/05/2000	Block IIR	7.5	0.75	13:55-14:35	2400	2398.675	99.9448
G	36	10/03/1994	Block IIA	7.5	0.70	14:29-14:35	360	359.8012	99.9447

where $a1$ and b are private communication channels, and α_1 and $1 - \alpha_1$ are transmission reliability (probability) at which the satellite A sends information $m1$ or $m2$ respectively.

The reference model of the control segment consists of 3 subsystems and 2 channels. The subsystems are a monitor station, a master control station and a ground antenna. The 2 channels are the channel between the monitor station and the master control station, denoted as channel b , and the channel between the master control station and the ground antenna, denoted as channel c . The master control station receives information from the monitor station through b , then transmits it to the ground antenna via c . The π_{prob} model of the master control station is as follows:

$$\begin{aligned} P_M &\triangleq vb.b(x).([x = m1].P_{M1} + [x = m2].P_{M2}) \\ P_{M1} &\triangleq vc.(\alpha_2\bar{c}(m1).P_M + (1 - \alpha_2)\bar{c}(m2).P_M) \\ P_{M2} &\triangleq \bar{c}(m2).P_M \end{aligned}$$

The reference model of the ground antenna is shown in Fig. 3, which includes 9 subsystems and 8 channels. The subsystems include a master control station, a ground antenna and 7 GPS satellites. The 8 channels include channel c between the master control station and the ground antenna and channels $d1, d2, \dots, d7$ between the ground antenna and satellites A, B, \dots, G respectively. As for the monitor station, the ground antenna communicates with the 7 satellites simultaneously. There are 4 ground antennas worldwide that perform the daily routine of transmitting commands to each satellite. We make a similar assumption to the above, in that there is a single ground antenna, which essentially is a combination of the 4 ground antennas.

The π_{prob} model of the ground antenna is: $P_G = P_{GA} | P_{GB} | P_{GC} | P_{GD} | P_{GE} | P_{GF} | P_{GG}$, where $P_{GA}, P_{GB}, P_{GC}, P_{GD}, P_{GE}, P_{GF}$ and P_{GG} denote the communication processes between satellites A, B, C, D, E, F and G respectively, and the ground antenna. As above, navigation satellite A , is used as an example for the π_{prob} specification of the ground antenna:

$$\begin{aligned} P_{GA} &\triangleq vc.c(x).([x = m1].P_{GA1} + [x = m2].P_{GA2}) \\ P_{GA1} &\triangleq vd1.(\alpha_3\bar{d1}(m1).P_{GA} + (1 - \alpha_3)\bar{d1}(m2).P_{GA}) \\ P_{GA2} &\triangleq \bar{d1}(m2).P_{GA} \end{aligned}$$

2) *Space Segment*: The reference model of the space segment consists of 4 subsystems and 3 channels. The 4 subsystems are the ground antenna, the satellites, the monitor station and the user. Seven satellites are analysed, referred to as A, B, \dots, G . These satellites receive information from the ground antenna simultaneously and then transmit the navigation information to the user. In this paper, the user and the monitor station are assumed to receive navigation signals from the satellites simultaneously.

The 3 channels are channel d between the ground antenna and the satellite, channel e between the satellite and the user and channel a between the satellite and the monitor station. The channels between satellites A to G and the user are denoted $e_i (i = 1, 2, 3, 4)$ respectively. The communication channels between the ground antenna and satellites A to G are $d1, d2, \dots, d7$ respectively. Due to space limitations, only the π_{prob} models of A, B, C and G are given in this section. The processes of D, E and F can be modelled similarly.

The π_{prob} model of ground antenna-satellite A -monitor station-user is as follows. The π_{prob} models of ground antenna-satellite B (and C, D)-monitor station-user can be derived similarly.

$$\begin{aligned} P_A &\triangleq vd1.d1(x).([x = m1].P_{A1} + [x = m2].P_{A2}) \\ P_{A1} &\triangleq va1.(\alpha_0\bar{a1}(m1).P_A + (1 - \alpha_0)\bar{a1}(m2).P_A) | P_{A11} \\ P_{A2} &\triangleq \bar{a1}(m2).P_A | P_{A21} \\ P_{A11} &\triangleq ve1.(\alpha\bar{e1}(m1).P_A + (1 - \alpha)\bar{e1}(m2).P_A) \\ P_{A21} &\triangleq \bar{e1}(m2).P_A \end{aligned}$$

3) *User Segment*: The user segment usually refers to the "GNSS receivers" that capture, process and track L-band signals from visible satellites to calculate the aircraft's position, time and velocity (PVT). The navigation mission of the flight was used to study the availability of navigation satellites to accomplish the mission during a specific segment of the flight. The 7 satellites were used for navigation during the flight. Due to the coverage limitation of satellites, the aircraft needs to switch to different satellites for navigation guidance during the flight. Fig. 4 gives the schema of the satellite navigation switching that occurred during the entire flight. As a result, there are 4 satellite groups available for navigation during the entire flight: $\{A, B, C, D\}$, $\{A, B, D, E\}$, $\{A, D, E, F\}$ and $\{D, E, F, G\}$.

The switching occurred between satellites C and E, B and F , and A and G . The switch from C to E occurs at 13:15, as shown in Figure 5. The switch from B to F occurs at 13:55, as shown in Figure 6. The switch from A to G occurs at 14:29, as shown in Figure 7.

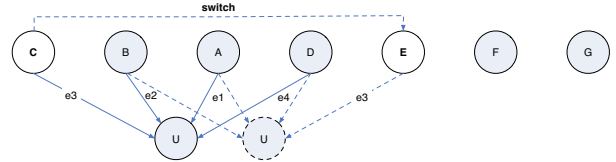


Fig. 5. Switch Satellite C with E

Fig. 5 illustrates the situation when the aircraft sequentially uses satellite groups $\{A, B, C, D\}$ and $\{A, B, D, E\}$ for navigation. First, the aircraft uses satellites C, B, A and D

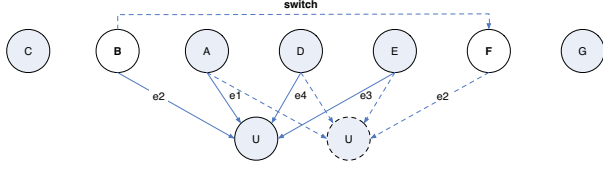


Fig. 6. Switch Satellite B with F.

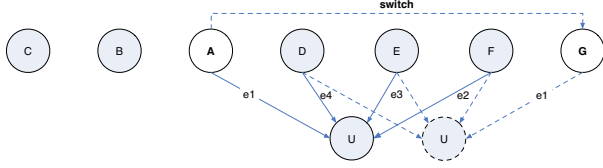


Fig. 7. Switch Satellite A with G.

for navigation; the communication channels between these 4 satellites and the aircraft are $\epsilon_1, \epsilon_2, \epsilon_3$ and ϵ_4 . The π_{prob} model of this process is as follows:

$$\begin{aligned}
P_U &\triangleq P_{U1}.P_{U2}.P_{U3}.P_{U4} \\
P_{U1} &\triangleq P_{C1} \mid P_{B1} \mid P_{A1} \mid P_{D1} \\
P_{C1} &\triangleq ve3.e3(x).([x = m1].P_{C1} + [x = m2].P_{C1}) \\
P_{B1} &\triangleq ve2.e2(x).([x = m1].P_{B1} + [x = m2].P_{B1}) \\
P_{A1} &\triangleq ve1.e1(x).([x = m1].P_{A1} + [x = m2].P_{A1}) \\
P_{D1} &\triangleq ve4.e4(x).([x = m1].P_{D1} + [x = m2].P_{D1})
\end{aligned}$$

Fig. 6 shows the scenario when the airplane changes from using satellite group $\{A, B, D, E\}$ to group $\{A, D, E, F\}$, and Fig. 7 shows the scenario when the airplane changes from using satellite group $\{A, D, E, F\}$ to group $\{D, E, F, G\}$. Similarly, when satellites $\{A, D, E, F\}$ or $\{D, E, F, G\}$ are used, the corresponding π_{prob} models become:

$$\begin{aligned}
P_{U3} &\triangleq P_{A3} \mid P_{D3} \mid P_{E3} \mid P_{F3} \\
P_{A3} &\triangleq ve1.e1(x).([x = m1].P_{A3} + [x = m2].P_{A3}) \\
P_{D3} &\triangleq ve4.e4(x).([x = m1].P_{D3} + [x = m2].P_{D3}) \\
P_{E3} &\triangleq ve3.e3(x).([x = m1].P_{E3} + [x = m2].P_{E3}) \\
P_{F3} &\triangleq ve2.e2(x).([x = m1].P_{F3} + [x = m2].P_{F3})
\end{aligned}$$

and:

$$\begin{aligned}
P_{U4} &\triangleq P_{D4} \mid P_{E4} \mid P_{F4} \mid P_{G4} \\
P_{D4} &\triangleq ve4.e4(x).([x = m1].P_{D4} + [x = m2].P_{D4}) \\
P_{E4} &\triangleq ve3.e3(x).([x = m1].P_{E4} + [x = m2].P_{E4}) \\
P_{F4} &\triangleq ve2.e2(x).([x = m1].P_{F4} + [x = m2].P_{F4}) \\
P_{G4} &\triangleq ve1.e1(x).([x = m1].P_{G4} + [x = m2].P_{G4})
\end{aligned}$$

respectively.

C. Encoding π_{prob} models into the PRISM language

The π_{prob} processes are encoded into the PRISM language in order to perform quantitative verification via probabilistic model checking. Translation from π_{prob} models of the GNSS based positioning system to their representation in PRISM follows the translation rules given in Section 3.3. The model between satellite A and the monitor station is used as an example to illustrate the translation. The π_{prob} model of the communication between satellite A and the monitor station is:

$$\begin{aligned}
P_{SA} &\triangleq va1.a1(x).([x = m1].P_{SA1} + [x = m2].P_{SA2}) \\
P_{SA1} &\triangleq vb.(\alpha_1 \bar{b}(m1).P_{SA} + (1 - \alpha_1) \bar{b}(m2).P_{SA}) \\
P_{SA2} &\triangleq \bar{b}(m2).P_{SA}
\end{aligned}$$

First, the π_{prob} process is broken down into the following sub-processes, to facilitate the translation:

$$\begin{aligned}
P &\triangleq (va1)(vb)(P1 \mid P2 \mid P3 \mid P4) \\
P1 &\triangleq a1(m1).P3.0 \\
P2 &\triangleq a1(m2).P4.0 \\
P3 &\triangleq \alpha_1 \bar{b}(m1).0 + (1 - \alpha_1) \bar{b}(m2).0 \\
P4 &\triangleq \bar{b}(m2).0
\end{aligned}$$

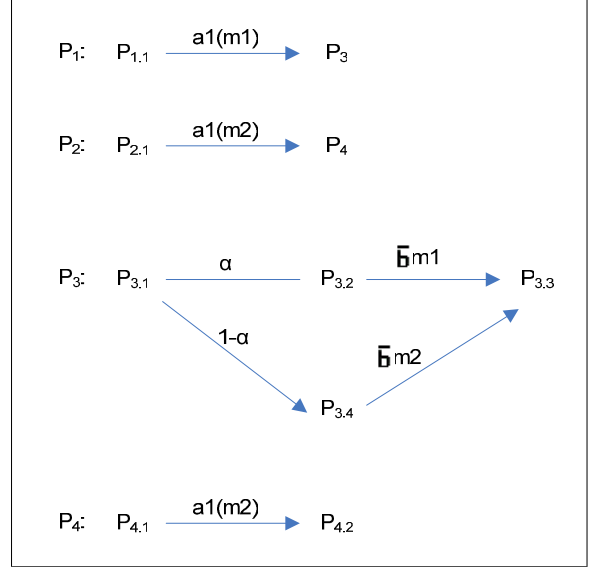


Fig. 8. A PSTG of the π_{prob} process of interaction between A and MS.

Then, the process is converted into a graphical representation, namely a PSTG. The converted PSTG of the process of the satellite A-monitor station system is as shown in Fig. 8. Finally, the PSTG of the system is translated into the PRISM language according to the transition rules. The transition process is as follows. For process $P1$, we use rule 9 (*Input on free name*). For a transition $P_i \xrightarrow{M, x(z)} R_i$, we add the command $[x_P_j_P_i_y] (s_i = P_i) \& M \rightarrow (s'_i = R_i) \& (z' = y)$. So the corresponding PRISM module of $P1$ can be described as:

```

module P1
S1 : [1, 2] init 1;
X : [m1, m2] init 0;
[] (S = 1) -> (S' = 2) & (x' = m1)
endmodule

```

For process $P2$, we use rule 9 to obtain the following module:

```

module P2
S1 : [1, 2] init 1;
X : [m1, m2] init 0;
[] (S = 1) -> (S' = 2) & (x' = m2)
endmodule

```

For process $P3$, we first use translation rule 6 (*Probabilistic internal transition*). For a transition $Q_i \xrightarrow{M, \vec{x}} \{p_1 : R_1^i, \dots, p_m : R_m^i\}$, we add the command: $[] (s_i = Q_i) \& M \rightarrow p_1 : (s'_1 = R_1^i) + \dots + p_m : (s'_m = R_m^i)$. Then, we use rule 7 (*Output on free name*). For a transition $P_i \xrightarrow{M, \vec{x}(y)} R_i$, we add the command: $[x_P_i_P_j_y] (s_i = P_i) \& M \rightarrow (s'_i = R_i)$.

So the corresponding PRISM module of $P3$ can be derived:

```

module P3
S1 : [1..4] init 1;
X : [m1, m2] init 0;
[] (S = 1) -> a : (S' = 2) :
[] (S = 2) & (x = m1) -> (S' = 3) :
[] (S = 1) -> (1 - a) : (S' = 4) :
[] (S = 4) & (x = m2) -> (S' = 3) :
endmodule

```

For process $P4$, the command is executed in accordance with rule 9, and the following PRISM commands can be obtained:

```

module P4
S1 : [1, 2] init 1;
X : [m1, m2] init 0;
[] (S = 1) -> (S' = 2) & (x' = m2) :
endmodule

```

The translation of π_{prob} models of the remaining 6 satellites to their corresponding set of PRISM modules, the information transmission between the monitor station and the master control station, the information transmission between the master control station and the navigation satellites and the navigation information output from the navigation satellites to the user can be derived similarly using the translation rules.

V. QUANTITATIVE ANALYSIS

A. Availability Properties

Although the accuracy of satellite positioning in the aviation environment is in general sufficient, it is its availability that limits the system dependability and overall performance. Availability properties relate to the reliability and maintainability of GNSS. Traditionally, it is the probability that the system is operating at a satisfactory level and can be committed at the start of a navigation mission when the mission is called for at an unknown and random point in time. For repairable satellites, we usually use the term Mean Time between Failure (MTBF). MTBF is the average time from one failure to the next, and also includes the repair time.

Mean Time To Repair (MTTR), is the time taken to repair a failed satellite. System designers should aim to allow for a high MTTR value and still achieve the reliability requirements. Availability is a mathematical function of MTBF and MTTR. We assume that there is negligible delay before a failed satellite begins to be repaired. The availability factor can be computed using the following formula, and it is obvious that a GNSS positioning system that can offer high availability is more desirable than one that offer lower availability.

$$Availability = \frac{MTBF}{MTBF + MTTR} \quad (1)$$

Furthermore, we proposed a modified concept for the GNSS availability properties associated with the underlying specification. The current approach involves prediction of the “mean” availability over the system lifetime, assuming that the system is in a steady state. This approach is not suited to the specification of GNSS positioning systems, where the objective is to guarantee what can be obtained from the system during short periods of time that are meaningful to users, and that this short term availability will be maintained during the lifetime of the system. This requires a modification of the availability

concept, as it is currently understood. Thus, we propose and distinguish availability properties as belonging to one of the following five types:

- 1) How often do failures occur that require corrective maintenance?
- 2) How often is preventative maintenance performed?
- 3) How quickly can indicated failures be isolated and repaired?
- 4) How quickly can preventive maintenance tasks be performed?
- 5) How long do logistics support delays contribute to down time?

The properties defining these types are typically specified using CSL as introduced in Section III (C). Simple examples of such properties are “if a satellite fails, repair occurs within a given time with a probability of 98% ”(property type 3): $P_{\geq 0.98}[fail(s_i) \mathbf{U}^{\leq t} repair(s_i)]$, $\forall i = 1, \dots, 7$; and “what is the worst-case expected time taken for a backup satellite to be launched?” (property type 5): $R_{max=?}^{time}[F "launch"]$.

B. Satellite Positioning for Aviation

As shown in Fig. 9, the GNSS enabled positioning system constitutes a cycle of signal (data) transmission between sub-systems. The satellite transmits the signal to the monitor station, the monitor station transmits the signal to the master control station, the master control station then transmits the signal to the ground antenna, and finally, the ground antenna uploads the information to the satellite.

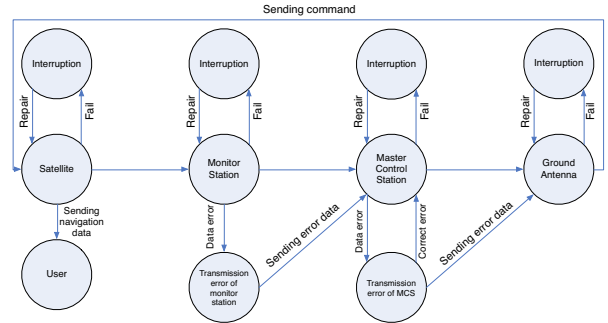


Fig. 9. Signal Transmission of Satellite Positioning Systems

Due to the impact of various factors, the monitor station, master control station, or ground antenna may fail during the operation of the system, resulting in a temporary interruption of the operation, which will resume after repair. Similarly, the satellite can also fail during operation and not transmit signals properly. In this section, failures due to satellite ageing were considered in the satellite analysis. Once failure occurs, new satellites must be launched to replace the failed satellites. The reliability data of the monitor station, master control station, ground antenna and satellite are shown in Table II.

During the signal transmission from the monitor station to the master control station as well as from the master control station to the ground antenna, abnormal signal transmission may occur, resulting in errors in information and corresponding anomalies in the subsequent update information for the

TABLE II. RELIABILITY OF SPACE AND CONTROL SEGMENTS.

Systems	MTBF (hours)	MTTR
Satellite	depends on the model	6 months
Monitor Station	156000	25.2 minutes
Master Control Station	1248	52.3 minutes
Ground Antenna	2310	4.2 hours

satellites. This can affect the navigation safety of users if the situation is severe. If anomalies occur in signal transmission, the master control station can correct the signal after a certain period of time.

Based on a preliminary investigation, it is assumed in our analysis that the information exchange among the satellites, monitor station and ground antenna does not itself generate information anomalies, but its reliability is a direct consequence of the reliabilities of the satellites and ground antenna. It is additionally assumed that information anomalies can only occur in the signal transmission between the master control station and the monitor station. These assumptions and related data are based on relevant reports³ on GPS, as summarised in Table III.

TABLE III. TRANSMISSION RELIABILITY OF SEGMENTS.

Systems	Transmission reliability
Satellite-Monitor Station	depends on reliability of satellites
Monitor Station-Master Control Station	0.99999
Master Control Station-Ground Antenna	0.99999
Ground Antenna-Satellite	depends on reliability of ground antennas

Where available, the data used for quantitative analysis in this study were collected from the official published data [19]. In other cases we used data for similar systems. The satellite models involved in the GPS satellite availability analysis of this section are Block-IIA, Block-IIR and Block-IIRM. A CTMC model was constructed based on the analysis of the relationships in the navigation system so that a quantitative analysis could be performed to check the model.

C. Preliminary Results and Discussion

Quantitative analysis was performed on the 7 satellites involved in the system using the PRISM model checker. As the satellites are independent of each other, probabilistic model checking is run on each satellite separately according to its respective characteristics. The starting point of the analysis on each satellite was the time on which the satellite was launched. The availability analysed is the satellites for the navigation mission from the beginning until the end of the mission. The data on the GPS satellites' availability obtained from the quantitative analysis can be shown in Table I.

The availability of various GPS satellites was greater than 99.944% under the set rules. Satellites *A*, *C*, *D* and *E* were the latest model, Block-IIRM, and had the largest availability for navigation: the probability of these satellites being available for navigation during the mission was 99.9449%. The model of satellite *F* is Block-IIR, and its probability of being available for navigation during the mission was 99.9448%. The model of satellites *B* and *G* is Block-A, and its availability is 99.9447%.

The above results indicate that satellites of the same model had the same availability. Model Block-IIRM had the largest availability for navigation, followed by Block-IIR and then Block-A. The availability data indicates that the navigation time and the duration of use of a GPS satellite do not have large impacts on the satellite's availability. Rather, the factor that had the greatest effect on navigation was the design life and reliability of the navigation satellite.

TABLE IV. AVAILABILITY OF THE NAVIGATION MISSION.

Channels	Satellite transition	Channel available time (s)	Aggregated available time	Availability of navigation
channel 1	D-D	9294.8710	37179.4767s	99.9448%
channel 2	A-G	9294.8707		
channel 3	B-F	9294.8638		
channel 4	C-E	9294.8710		

The availability of the GPS constellation of seven satellites are shown in Table IV, and the availability reaches 99.9448%. We are neglecting environmental factors, so our measure of availability to may be slightly greater than when they are included. An actual mission will involve multiple satellites, and each channel has multiple backup satellites. Thus, once a failure occurs, the channel will be switched to a backup satellite. Therefore, the availability of GNSS in practice will be larger than that shown in our analysis. Moreover, the presence of multiple satellites will potentially increase the overall availability along an air line, but the increase of available satellites does not necessarily guarantee an improved user-satellites geometry due to the similar orbital arrangement of most GNSS satellites.

To validate the reliability of the evaluation data, we referred to some of the literature and official reports from the civil aviation sector. The U.S. Federal Aviation Administration (FAA) releases quarterly reports on the performance analysis of the system based on the operation of the GPS in each quarter to ensure the navigation safety of global aviation [20]. According to the monitoring reports released by the FAA, the availability of each individual GPS satellite has been approximately 99.96% [20]. This number is very close to that obtained in our analysis and is in line with the estimated value of this study, confirming, from one line of evidence, the feasibility and applicability of our approach.

VI. RELATED WORK

Prediction of satellite navigation availability is very useful for numerous applications such as airplane navigation missions and in-car navigation systems. Simulation is nowadays widely used to analyse performance and predicate availability for a variety of satellite systems [21]–[24]. In [21], software simulation based on a Markov model of a GPS constellation of 24 satellites is used to obtain availability estimates of GNSS in Taiwan. In [22], an automated method for predicting the number of satellites available to a GPS receiver, at any point on the Earth's surface at any time is described. In [23], the availability of a navigation and communication satellite system (NCSS) is studied to examine the feasibility of using a NCSS constellation in Australia. A performance model was proposed in [24] to evaluate the availability of satellite systems over geographic grid averaging areas over a given period of time.

³Global Positioning System (GPS) Performance Quarterly Report

Availability characteristics for GPS and GPS augmented by geostationary satellites (GSs) are compared in [25]. Availability is determined for users in the contiguous zone in United States, based on the planned operational GPS constellation and various GS deployments. In [26], a method for determining the availability of three different GPS services (positioning, supplemental navigation, and sole means navigation) is described for both two-dimensional and three-dimensional applications. A 21-satellite and a 24-satellite constellation are considered. In the companion paper [27], state probability analyses of 21- and 24-satellite constellations based on a Markov chain model are discussed.

VII. CONCLUSIONS AND FUTURE WORK

In this paper we present a formal approach to analyse the availability properties of GNSS based positioning systems. We have modelled some aspects (e.g., communication, movement, unreliable transmission) of the system for navigating a specific flight in the probabilistic π -calculus, a process algebra which supports modelling of concurrency, uncertainty, and mobility. Then we encode our process algebraic models into the PRISM language. Finally, we analyse the availability properties that relate to the dependability and overall performance of the underlying system.

Although nowadays satellite positioning is commonly used in the aviation sector, it is still to gain a foothold in other industries such as the rail industry. One major barrier that presents its application to railway safety is the lack of evidence that the concept and theory for the verification of railway applications with introduction of GNSS is applicable based on the joint use of aviation and railway standards and requirements. Up to now availability analysis is non-trivial because difficult situations exist on the railways due to the limitations of the GNSS coverage in urban canyons, tunnels, and forest areas. For future work, we plan to add a fourth environment segment that simulates such difficult situations to the GNSS.

ACKNOWLEDGMENT

This research was partially supported by the European Commission (EC) EATS project (FP7-TRANSPORT-314219). The author Yu Lu was funded by the Scottish Informatics and Computer Science Alliance (SICSA).

REFERENCES

- [1] S. Arrizabalaga, J. Mendizabal, S. Pinte, J. Sánchez, J. González, J. Bauer, M. Themistokleous, and D. Lowe, "Development of an Advanced Testing System and Smart Train Positioning System for ETCS applications," in *Proc. 5th Transport Research Arena Conference (TRA'15)*, 2014.
- [2] C. W. Johnson, "Innovation vs Safety: Hazard Analysis Techniques to Avoid Premature Commitment in the Early Stage Development of National Critical Infrastructures," in *Proc. 32nd International Systems Safety Conference*, 2014.
- [3] Y. Lu, Z. Peng, A. Miller, T. Zhao, and C. Johnson, "Timed Fault Tree Models of the China Yongwen Railway Accident," in *Proc. 8th Asia Modelling Symposium (AMS'14)*. IEEE, 2014.
- [4] Z. Peng, Y. Lu, A. Miller, C. Johnson, and T. Zhao, "Risk assessment of railway transportation systems using timed fault trees," *Quality and Reliability Engineering International*, 2014.
- [5] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: Probabilistic Model Checking for Performance and Reliability Analysis," *ACM SIGMETRICS Performance Evaluation Review*, vol. 36, no. 4, pp. 40–45, 2009.
- [6] R. Alur and T. A. Henzinger, "Reactive Modules," *Formal Methods in System Design*, vol. 15, no. 1, pp. 7–48, 1999.
- [7] G. Norman, C. Palamidessi, D. Parker, and P. Wu, "Model Checking Probabilistic and Stochastic Extensions of the π -Calculus," *IEEE Transactions on Software Engineering*, vol. 35, no. 2, pp. 209–223, 2009.
- [8] Y.-W. Lee, Y.-C. Suh, and R. Shibasaki, "A simulation system for GNSS multipath mitigation using spatial statistical methods," *Computers & Geosciences*, vol. 34, no. 11, pp. 1597–1609, 2008.
- [9] Z. Peng, Y. Lu, A. Miller, C. Johnson, and T. Zhao, "A Probabilistic Model Checking Approach to Analysing Reliability, Availability, and Maintainability of a Single Satellite System," in *Proc. 7th European Modelling Symposium (EMS 2013)*. IEEE, 2013, pp. 611–616.
- [10] Z. Peng, Y. Lu, A. Miller, T. Zhao, and C. Johnson, "Formal Specification and Quantitative Analysis of a Constellation of Navigation Satellites," *Quality and Reliability Engineering International*, 2014.
- [11] R. Abo and K. Barkaoui, "A Performability Analysis of Mobile Wireless Sensor Networks with Probabilistic Model Checking," in *Proc. 7th Wireless Advanced (WiAd'11)*. IEEE, 2011, pp. 283–288.
- [12] M. Hennessy and H. Lin, "Symbolic bisimulations," *Theoretical Computer Science*, vol. 138, no. 2, pp. 353–389, 1995.
- [13] M. Kwiatkowska, G. Norman, and D. Parker, "Stochastic Model Checking," in *Proc. 7th International Conference on Formal Methods for Performance Evaluation (SFM'07)*. Springer, 2007, pp. 220–270.
- [14] C. Baier, J.-P. Katoen, and H. Hermanns, "Approximative Symbolic Model Checking of Continuous-Time Markov Chains," in *Proc. 10th International Conference on Concurrency Theory (CONCUR'99)*. Springer, 1999, pp. 146–161.
- [15] A. Aziz, K. Sanwal, V. Singhal, and R. Brayton, "Model-Checking Continuous-Time Markov Chains," *ACM Transactions on Computational Logic*, vol. 1, no. 1, pp. 162–170, 2000.
- [16] E. A. Emerson, "Temporal and modal logic," in *Handbook of Theoretical Computer Science*. Elsevier, 1990, pp. 996–1072.
- [17] H. Hansson and B. Jonsson, "A Logic for Reasoning about Time and Reliability," *Formal Aspects of Computing*, vol. 6, no. 5, pp. 512–535, 1994.
- [18] R. Alur, C. Courcoubetis, and D. Dill, "Model-Checking for Real-Time Systems," in *Proc. 5th Annual IEEE Symposium on Logic in Computer Science (LICS'90)*. IEEE, 1990, pp. 414–425.
- [19] W. Marquis and M. Shaw, "GPS III: Bringing New Capabilities to the Global Community," *Inside GNSS*, pp. 34–48, September 2011.
- [20] FAA, "Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Analysis Report," 2013.
- [21] H.-S. Wang and P.-C. Hsiao, "GNSS Availability Analysis in Taiwan - a Markov Model Approach," in *Proc. National Technical Meeting of ION*, 2006, pp. 759–769.
- [22] G. Taylor, J. Li, D. Kidner, C. Brunson, and M. Ware, "Modelling and prediction of GPS availability with digital photogrammetry and LiDAR," *International Journal of Geographical Information Science*, vol. 21, no. 1, pp. 1–20, 2007.
- [23] K. Kubik, Y. Feng, and T. Tang, "An Availability Study for a Nav-Com Satellite System (NCSS) in Australia," in *Proc. 9th National Space Engineering Symposium*, 1994, pp. 59–66.
- [24] C. Kelley and M. Dessouky, "Minimizing the Cost of Availability of Coverage from a Constellation of Satellites: Evaluation of Optimization Methods," *Systems Engineering*, vol. 7, no. 2, pp. 113–122, 2004.
- [25] W. S. Phlong and B. D. Elrod, "Availability Characteristics of GPS and Augmentation Alternatives," *Navigation*, vol. 40, no. 4, pp. 409–428, 1993.
- [26] J.-M. Durand, T. Michal, and J. Bouchard, "GPS Availability, part I: Availability of Service Achievable for Different Categories of Civil Userspart i: Availability of Service Achievable for Different Categories of Civil Users," *Navigation*, vol. 37, no. 2, pp. 123–139, 1990.
- [27] J.-M. Durand and A. Caseau, "GPS Availability, Part II: Evaluation of State Probabilities for 21 Satellite and 24 Satellite Constellations," *Navigation*, vol. 37, no. 3, pp. 285–296, 1990.