Reliability Engineering and System Safety 144 (2015) 95–116

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

How reliable is satellite navigation for aviation? Checking availability properties with probabilistic verification

Yu Lu [a], Zhaoguang Peng [b,c,*], Alice A. Miller [a], Tingdi Zhao [c], Christopher W. Johnson [a]

[a] School of Computing Science, University of Glasgow, Glasgow, United Kingdom
[b] China Ceprei Laboratory, Guangzhou, China
[c] School of Reliability and Systems Engineering, Beijing University of Aeronautics and Astronautics, Beijing, China

ARTICLE INFO

Article history:
Received 11 September 2014
Received in revised form
15 July 2015
Accepted 19 July 2015
Available online 29 July 2015

Keywords:
Satellite systems
Formal methods
Model checking
Reliability
Availability
Probabilistic verification

ABSTRACT

This paper highlights a promising application of the analysis technique of probabilistic verification. We prove that it is able and suitable to analyse GNSS based positioning in aviation sectors for aircraft guidance. In particular, the focus is a widely used formal method called probabilistic model checking, and its generalisation to the analysis of quantitative aspects of a specific civil flight. We construct a formal model of the GNSS based positioning system for this application in the probabilistic π-calculus, a process algebra which supports modelling of concurrency, uncertainty, and mobility. After that, we encode our model in language of the PRISM symbolic probabilistic model checker. We then formalise and analyse the logical properties that relate to the dependability of the underlying system to check the system reliability and availability. We demonstrate how model specification and verification techniques can be successfully applied to the reliability and availability analysis of our case study.

1. Introduction

Satellite positioning systems are used within the transport industries such as marine, rail, and aviation sectors extensively. For example, in aviation, 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, satellites were only deployed for military purposes. However nowadays they are used for a wide range of civil aviation applications, including navigation, communication, tracking, and flight management.

Our work has been inspired by a number of previous European Commission (EC) projects such as GADEROS, GRAIL, LOCASYS, and SATLOC. These projects have proved the feasibility of introducing GNSS in non-critical systems by means of theoretical studies and demonstrations. The current EC project 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) analysis [2] is used to study the dependability properties of the technical solution in the critical applications, which aims to verify the proposed solution.

Availability requirements are identified as the most challenging obstacles towards GNSS aided positioning systems in [2]. Many approaches [3–6] can be used to analyse availability properties. Among them, simulation, analytical analysis, and quantitative analysis are popular and practical. Each approach has its advantages and disadvantages that we do not discuss in this paper. We consider probabilistic verification, a quantitative analysis technique based on Markov models. It is a formal verification technique for analysing and verifying quantitative properties of a system's design, such as time, stochastic behaviour or resources. It is therefore highly suitable for modelling characteristics of our underlying system.

The mobility of an aircraft and satellites is universally recognised as an essential parameter for analysing the availability of satellite navigation systems. Our first task is to specify the communication between the airplane and satellites and their combined mobility. The second task is rendering these two models independently, in order to study the availability of the system in terms of different mobility models without changing the communication models.

In an example illustrated in Fig. 1 (a), some cars are on the road, and each is connected by a unique wavelength to a single transmitter. The transmitters have fixed connections to a central control. On some events such as signal fading, a car may be switched to another

* Corresponding author.
E-mail addresses: y.lu.3@research.gla.ac.uk (Y. Lu), zgpeng@buaa.edu.cn (Z. Peng), alice.miller@glasgow.ac.uk (A.A. Miller), ztd@buaa.edu.cn (T. Zhao), christopher.johnson@glasgow.ac.uk (C.W. Johnson).

http://dx.doi.org/10.1016/j.ress.2015.07.020

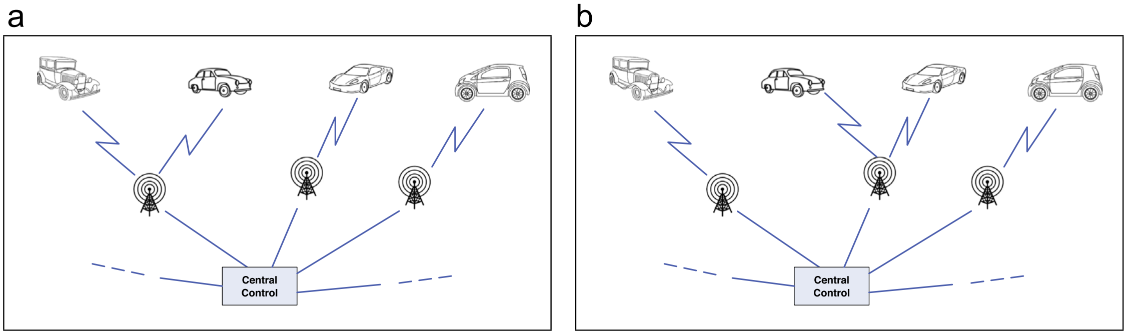

Fig. 1. Component mobility.

transmitter. We distinguish two types of movement: the physical movement of vehicles and virtual movement of communication links between vehicles and transmitters. The two types of movements are independent, but the physical movement of a vehicle may give rise to the virtual movement of its link to a transmitter (Fig. 1(b)).

In our study, we mainly deal with this kind of relationship between the movement of satellites and aircraft, and we study how the physical movement of both satellites and aircraft give rise to the mobility of links between them. As well as mobility, the π-calculus can be used to model parallel composition, alternative composition and sequential composition. Properties of the modelled system can be verified by studying the underlying labelled transition system. For this purpose, we specify the underlying models using the probabilistic π-calculus, an extension of the π-calculus [7,8] for modelling mobile systems.

Therefore, 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 contains a high level of uncertainty (e.g., in signal transmission unreliability due to solar radiation, etc.). Since PRISM only model checks expressions in the reactive modules language, and this does not allow for component mobility, 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 Markov Decision Processes (MDPs) semantic models of our specification are first constructed using rules presented in [9].

The basic idea is to first build a Markov models that captures the behaviour of the system, and then to use the model to analyse precisely specified properties using temporal logics. This analysis is automatically performed using the model checker PRISM [10], using 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 [11]. 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.

Our paper is organised as follows. In Section 2 we describe the underlying satellite navigation systems. In Section 3 the application of probabilistic verification is introduced. In Section 4 we present our formal specifications of a satellite navigation system for a specific navigation mission and their associated Markov decision processes respectively. Then, we verify availability properties using PRISM in Section 5. In Section 6 we discuss related work on analysing availability of satellite systems. Finally, in Section 7 we conclude.

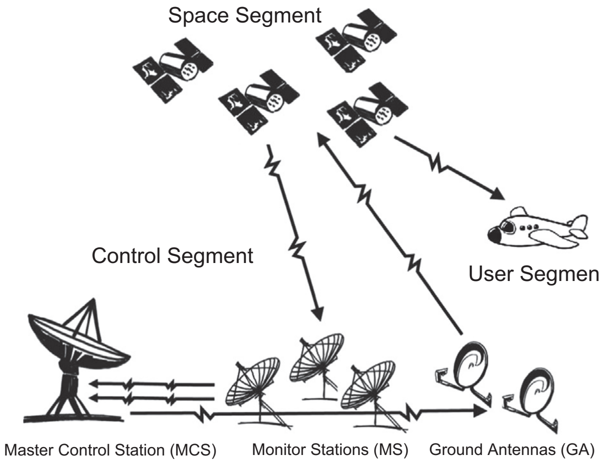

Fig. 2. Three segments of a GNSS system.

2. GNSS-based navigation systems

A GNSS-based navigation system consists of three major parts: the space segment, control segment and user segment. Recent theoretical research and standards have added a fourth environment segment to the satellite navigation system. The Galileo navigation system includes the environment segment in the composition of its navigation system. Although not explicitly mentioned, the environment segment is implied in the GPS system. To be conservative, the three traditional segments were used in this paper as the components of the study, and the environmental segment was treated as an influencing factor on the system. Failure of any subsystem will lead to errors in the final positioning. Fig. 2 is a schematic diagram of GNSS segments.

First, the monitor stations measure the pseudo-range of visible satellites every 6 s, correct them with ionospheric and meteorological data, smooth the measurement to generate data with a time interval of 15 s, 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 estimator [12]. 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. According to [13], in general, at least four satellites are required to determine the user's position.