CRITICAL STATES DETECTION WITH BOUNDED PROBABILITY OF FALSE ALARM AND APPLICATION TO AIR TRAFFIC MANAGEMENT [1]

M.D. Di Benedetto [*] **, S. Di Gennaro** [*] **and A. D'Innocenzo** [*]

[*] *Department of Electrical and Information Engineering and Center of Excellence DEWS, University of L'Aquila.*
E.mail: {dibenede, digennar, adinnoce}@ing.univaq.it

Abstract: The analysis of error propagation in an Air Traffic Management (*ATM*) environment is addressed. The theory of Hybrid Systems is used to model the error evolution, an observability problem for a Markov Chain with discrete output symbols associated to the transitions is stated, and a runtime observer is proposed for estimating the probability of a given discrete state to be active. Sufficient conditions are given for characterizing the decidability of the addressed observability problem. The results are related to previous works on location observability of deterministic hybrid systems, and are used to analyze an *ATM* case study, the "*clearance to change the flight plan*".

Keywords: Failure Detection, Markov Chains, Air Traffic Management

1. INTRODUCTION

Hybrid systems are a powerful tool for the analysis and control of Air Traffic Management (*ATM*) systems, as shown in the IST European Project HYBRIDGE (see http://www.nlr.nl/public/hosted–sites/hybridge). Each agent, in an *ATM* environment, executes a sequence of operations that may be characterized by different dynamics (Di Benedetto *et al.*, 2005): this is a typical hybrid context. Moreover, since we are dealing with human agents, the behavior is non–deterministic. The non–determinism of human agents is mainly due to *Situation Awareness*, which is defined in (Endsley, 1995), (Stroeve *et al.*, 2003) as "*the perception of elements in the environment, the comprehension of their meaning, and the projection of their status in the near future*". *Situation Awareness* may be wrong for wrong perception of relevant information, wrong interpretation of perceived information, or wrong prediction of a future state and propagation of error due to agents communication. Moreover, statistic data retrieved by the analysis of real cases of *ATM* procedures may be used to define specific error probability in *ATM* operations, thus it is reasonable to introduce a stochastic framework to analyze error propagations. In the context of error detection analysis, partially observable discrete event systems have been extensively studied in fault detection and supervisory control problems. (Yoo and Lafortune, 2001) analyze the diagnosability of partially observable discrete event systems, and propose a polynomial verification method. (Hadjicostis, 2002) discusses a probabilistic methodology for detecting functional changes in the state transition mechanism of a deterministic finite-state machine (FSM). Results are achieved by computing the deviation between the expected observations and the actual measurements, assuming to know an appropriate statistical characterization of the FSM input. In (Kennedy *et al.*, 1987) a decision feedback equalizer (DFE) operating on a noisy channel is considered, and it is shown how the results concerning a noiseless channel can be extended to yield tight bounds on the stationary error probability performance for the noisy case. Similar approaches were developed in (Aghasaryan *et al.*, 1997; Boubour *et al.*, 1997) for Petri nets. Observability of hybrid systems has been also analyzed in (Balluchi *et al.*, 2002), where a definition of observability of the current state (*current location observability*) has been provided and a procedure for the construction of an observer of the discrete and continuous states is proposed, and in (D'Innocenzo *et al.*, 2006), where *current location observability* of hybrid automata has been studied.

[1] This work was partially supported by European Commission under Project IST NoE HyCON contract n. 511368.

The above definitions of diagnosability and observability do not require a real time state estimation, while in safety-critical applications such as *ATM*, we need to determine the actual state of the system immediately, as a delay can lead to unsafe or even catastrophic behavior of the system. For this reason, we focus here on the concept of observability in prescribed time horizon, and we introduce a stochastic framework to model and test *Situation Awareness* error evolution in *ATM* operations. In Section 2, we define a class of stochastic Hybrid Systems. In Section 3, we propose a definition of observability with bounded probability of false alarm for this class of systems. We propose a design method for a runtime estimator of the discrete state of $\mathcal{S}$ on the basis of the measured outputs, and we give conditions for the system to be observable. In Section 4, we state sufficient conditions such that observability is decidable. In Section 5, we relate our results to previous works on location observability of deterministic hybrid systems (De Santis *et al.*, 2005). In Section 6 we present a case study, the *Clearance to change the flight plan*, where the developed methodologies are used to yield a conditioned probability distribution of the *SA* error evolution. Section 6 offers conclusions and tips for further work.

2. DEFINITIONS AND SETTING

We define a Markov Hybrid System as a tuple $\mathcal{S} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta, \Pi, \Pi_0)$ where:

- $Q = q_1, \cdots, q_N$ is the discrete state set;
- X is the continuous state space;
- Q_0 is the set of initial discrete states;
- X_0 is the set of initial continuous states;
- U is the continuous input space;
- Y is the continuous output space;
- S_q associates linear continuous dynamics A_q, B_q, C_q to each discrete state $q \in Q$;
- Σ is the finite set of input symbols;
- $E \subseteq Q \times \Sigma \times Q$ is a collection of edges;
- Ψ is the finite set of output symbols;
- η: $E \rightarrow \Psi$ is the output function;
- Π is a transition probability matrix with $\Pi_{ij} = \mathcal{P}[q(k+1) = q_j \mid q(k) = q_i]$ for each k;
- Π_0 is an initial probability distribution $(\mathcal{P}[q(0) = q_1] \cdots \mathcal{P}[q(0) = q_N])$, where $\Pi_{0i} = 0$ if $q_i \notin Q_0$.

A Markov Hybrid System is similar to a Hybrid Markov chain as proposed in (Shi *et al.*, 2004). However, in our model no guard functions are considered, and we do not assume that the embedded Markov Chain is irreducible and positive recurrent.

To define the executions of $\mathcal{S}$, we introduce a hybrid time basis $\tau = \{I_k\}_{k\geq 0} \in \mathcal{T}$ as a finite or infinite sequence of intervals $I_k = [t_k, t'_k]$ such that (Lygeros *et al.*, 1999)

(1) I_k is closed if τ is infinite; I_k might be right–open if it is the last interval of a finite sequence τ;
(2) $t_k \leq t'_k$ for all k and $t'_{k-1} \leq t_k$ for $k > 0$.

The cardinality $|\tau|$ of the hybrid time basis is the number of intervals I_k in τ.

An execution of $\mathcal{S}$ is a collection $\chi = (\tau, x, q)$, with x, q satisfying the continuous and discrete dynamics of $\mathcal{S}$. A string $\rho = q_0, \cdots, q_s$ is an execution of the discrete state q of $\mathcal{S}$ with a finite number of transitions $|\rho| - 1 = s$ if $q_0 \in Q_0$ and $\forall I_k \in \{I_1, \cdots, I_s\}, (q_{k-1}, q_k) \in E$. The discrete state execution is ruled by a discrete time Markov chain.

Let $\Upsilon(Q_0)$ be the set of all executions ρ of the discrete state of $\mathcal{S}$ with a finite number of transitions. Given $q \in Q$, let $\Upsilon_q(Q_0)$ be the set of all executions $\rho \in \Upsilon(Q_0)$ such that the last visited state is $q_s = q$. We associate to each execution ρ the observed output as the string $p = P(\rho) = \psi_1 \cdots \psi_s$ where $\psi_k = \eta(q(I_{k-1}), q(I_k))$ for $k = 1, \cdots, s$. We define $\mathcal{L}(\mathcal{S}) = \{P(\rho) \mid \rho \in \Upsilon(Q_0)\}$ the set of output strings that can be generated by all executions of the system $\mathcal{S}$. Given an output string $p = \psi_1 \cdots \psi_s$, we define

$$Reach_{\mathcal{S}}(Q_0, p) := \{q \in Q \mid \exists \rho \in \Upsilon_q(Q_0), P(\rho) = p\}$$

the set of all states that can be reached from an initial state in Q_0 and such that the observed output string is p.

Let $\mathcal{H} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta)$ be a Hybrid System defined by the same tuple of $\mathcal{S}$, except for the stochastic matrices Π and Π_0. The space of all executions of $\mathcal{S}$ and that of $\mathcal{H}$ coincide. However, the discrete execution is non deterministic on $\mathcal{H}$, while on $\mathcal{S}$ it is subtended by a probability space, denoted $(\Omega, \mathcal{F}, \mathcal{P})$, on which the stationary Markov chain $q(I_0), q(I_1), q(I_2), \cdots$ is defined. Ω is the space Υ of all executions ρ of the discrete space, and $\mathcal{F}$ the associated sigma–algebra. $\mathcal{P}$ is uniquely defined by the transition probability matrix Π and the initial probability distribution Π_0. Let $\pi_i(I_k) :\, = \mathcal{P}[q(I_k) = q_i]$ and $\pi(I_{k+1}) = \Pi^T \pi(I_k)$ the corresponding dynamics. We now introduce a well known formalism that will be necessary in the following sections:

Let a Markov Hybrid System $\mathcal{S} = (Q \times X, Q_0 \times X_0, U, Y, S_q, \Sigma, E, \Psi, \eta, \Pi, \Pi_0)$ and the subsets $Q' \subset Q$, $E' \subset E \cap (Q' \times Q')$ be given; $\mathcal{S}' = (Q' \times X, Q'_0 \times X_0, U, Y, S_q, \Sigma', E', \Psi', \eta', \Pi', \Pi'_0)$ is the subsystem induced by (Q', E') on S, where (Π', Π'_0) are normalized stochastic matrices.

3. P–OBSERVABILITY OF A DISCRETE STATE

In this section, we propose a definition of observability for a Markov Hybrid System, with respect to a given discrete state. We then propose a constructive procedure for an estimator of the discrete state and a verification procedure for observability. Finally, give conditions such that P–Observability is decidable.

Given a Markov Hybrid System $\mathcal{S}$, our goal is to use the discrete output string to compute the probability distribution of the current discrete state conditioned to a subset of trajectories, namely all the trajectories whose output is the measured output. Consider the probability space $(\Omega, \mathcal{F}, \mathcal{P})$. When an output string $p = \psi_1 \cdots \psi_s$ is generated up to time t_s, it is possible to define the set $\mathcal{G}(p) \subseteq \Omega$ of executions $\rho \in \Upsilon(Q_0)$ such that $P(\rho) = p$. $\mathcal{G}(p)$ is given by $\mathcal{G}_k(p)$ for $k = s$, where

$$\mathcal{G}_0(p) = \Omega$$

$$\mathcal{G}_k(p) = \mathcal{G}_{k-1}(p) \cap \left(\bigcup_{q \in Reach_{\mathcal{S}}(Q_0, p|_k)} \Upsilon_q(Q_0) \right)$$