

Non-Concurrent Error Detection and Correction in Switched Linear Controllers

Shreyas Sundaram and Christoforos N. Hadjicostis

University of Illinois at Urbana-Champaign

Abstract. In this paper, we consider protection schemes for linear time-invariant (LTI) controllers in switched systems. These controllers are often digital in nature and, as such, are subject to internal hardware malfunctions (faults). A discrete-time (DT) LTI system is usually protected against faults by embedding the state-space of the original system into the state-space of a higher dimensional redundant system. These embeddings preserve the state evolution of the original system in some encoded form, but enable error detection and correction through *concurrent* parity checks (i.e., parity checks that are performed at the end of each time step). In this paper, we present a systematic method of constructing linear embeddings for protecting switched DT LTI controllers. These methodologies allow an external mechanism to detect and identify transient state-transition faults through *non-concurrent* (e.g., periodic) parity checks. The resulting error detection and correction procedures can then be performed periodically, thereby relaxing the requirements on the reliability of the checking mechanism.

1 Introduction

The concept of *switching* in the design of control systems has been the subject of recent intensive research, partially due to its applicability to a wide range of problems [1–5]. For instance, when facing modeling uncertainty, switching controllers provide performance that is not obtainable through a single controller (e.g., *nonholonomic systems* cannot be asymptotically stabilized through the use of a continuous feedback law, making switched control an attractive option [5]).

In switched control, one obtains the desired behavior from a plant by using logic-based decisions to dynamically switch between controllers in the control loop. Figure 1 shows the block diagram for a system with switched control. Such schemes have been studied extensively, aiming to ensure that desirable system properties such as stability, reachability and controllability are maintained [6–9]. The controllers and control strategies in these systems often arise in an inherently discrete-time setting, as in the case where micro-controllers are used to regulate continuous plants [10].

As systems become more complex, the issue of *fault tolerance* becomes important. For example, it has been demonstrated that harsh conditions, such as lightning and electromagnetic radiation, are a source of upsets in digital flight

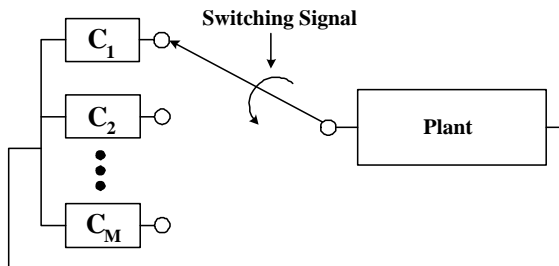


Fig. 1. Switched Control

control systems [11, 12]. Recent research has investigated methods of estimating the state of a system in the presence of intermittent sensor or measurement failures [13, 14]. In this paper, we broadly define fault tolerance as the ability of a system to detect and rectify internal faults which cause the system to be in an incorrect state. In particular, we are interested in protecting against internal faults in discrete-time switched control mechanisms. A traditional approach to fault tolerance has been to use *modular redundancy*, i.e., replicate fault-prone components in the system and use a voting scheme to determine the correct state or behavior [15]. In an effort to find more efficient methods for fault tolerance, the use of arithmetic codes [16] and algorithm-based fault tolerance (ABFT) schemes [17] have also been studied extensively in the context of computing systems. In addition, for discrete-time systems, researchers have developed techniques that map the state-space of the system to a higher-dimensional state-space of a redundant system. This mapping is constructed in a way that preserves the state evolution of the original system, but with the added capability to perform error detection and correction. These techniques typically require *concurrent* checks (i.e., checks at the end of each discrete-time step).

A method for performing *non-concurrent* checks (e.g., periodic checks) was presented in [18] for discrete-time linear time-invariant (DT LTI) dynamic systems. Here, we extend the concepts presented in that paper to the realm of switched DT LTI systems. The proposed scheme for protecting switched discrete-time systems allows for periodic checking for errors in the family of controllers, thereby providing increased reliability and requiring relatively low overhead.

This paper is organized as follows. Section 2 provides mathematical background on our systems of interest. Section 3 describes how to design a switched system with non-concurrent fault detection and correction capabilities. We provide an example of our method in Sect. 4 and conclude in Sect. 5 with a summary of our results and directions for future work.

2 Background

Consider a DT LTI system in the form

$$x[k + 1] = Ax[k] + Bu[k] , \quad (1)$$

where $x[k] \in \mathbb{R}^n$ is the state vector at time step k , $u[k] \in \mathbb{R}^m$ is the input at time step k , and A and B are constant real-valued matrices of appropriate dimensions.

In [19], a DT LTI system is protected against transient faults that corrupt one or more of its state variables at a particular time step t , by embedding it into a larger redundant system \mathcal{H} of dimension $\eta = n + d, d > 0$. The embedding is such that under fault-free conditions, all information about the initial system can be retrieved from \mathcal{H} , and vice-versa. More specifically, if $x[k]$ represents the state vector in (1), and $x_h[k]$ represents the state vector in \mathcal{H} , *linear* decoding and encoding can be performed through a pair of matrices \mathbf{L} and \mathbf{G} that are chosen to satisfy (for all k)

$$x[k] = \mathbf{L}x_h[k] , \quad (2)$$

$$x_h[k] = \mathbf{G}x[k] , \quad (3)$$

at least under proper initialization and fault-free conditions. In other words, the state evolution of the redundant system \mathcal{H} is captured by

$$x_h[k + 1] = \mathcal{A}x_h[k] + \mathcal{B}u[k] , \quad (4)$$

where \mathcal{A} and \mathcal{B} are chosen so that (2) and (3) are satisfied.

The above approach was extended in [18] to allow non-concurrent error detection and correction in DT LTI dynamic systems. Assuming (without loss of generality) that the system starts operation at time step 0, this paper presented a method to perform the first error check at some time step N . Specifically, [18] showed that matrices \mathcal{A} and \mathcal{B} in (4) can be chosen so that if a total of D transient faults take place between time steps 0 and $N - 1$, and affect state variables i_1, i_2, \dots, i_D by initial additive errors of v_1, v_2, \dots, v_D respectively, an error check that depends only on the corrupted state at time step N is sufficient to determine which states were corrupted, and to obtain the time step and error value by which they were affected.

This work is further extended in this paper to protect switched DT LTI systems.

3 Application to Switched Systems

3.1 Notation and Preliminaries

Consider a DT LTI switched system \mathcal{S} in the form

$$x[k + 1] = \mathbf{A}_{\sigma[k]}x[k] + \mathbf{B}_{\sigma[k]}u[k] , \quad (5)$$

where $\sigma[k] \in \Omega = \{1, 2, \dots, M\}$ represents the switching path among the M systems, $x[k] \in \mathbb{R}^n$ is the state vector at time step k , and $u[k] \in \mathbb{R}^m$ is the input at time step k . At any given time step k , the $(\mathbf{A}_{\sigma[k]}, \mathbf{B}_{\sigma[k]})$ matrices are taken to be constant real-valued matrices of appropriate dimensions.

If the system is allowed to run for N time steps, the state at the end of time step $N - 1$ (beginning of time step N) is easily calculated to be

$$x[N] = \left(\prod_{i=0}^{N-1} \mathbf{A}_{\sigma[i]} \right) x[0] + \left(\prod_{i=1}^{N-1} \mathbf{A}_{\sigma[i]} \right) \mathbf{B}_{\sigma[0]} u[0] + \cdots \\ \cdots + \mathbf{A}_{\sigma[N-1]} \mathbf{B}_{\sigma[N-2]} u[N-2] + \mathbf{B}_{\sigma[N-1]} u[N-1] . \quad (6)$$

3.2 Embeddings of Switched Systems

We start with the switched system \mathcal{S} in (5). To protect against transient state-transition faults, we will map the n -dimensional state-space of \mathcal{S} into a larger state-space of dimension $\eta = n + d, d > 0$. This system, denoted by \mathcal{H} , will be given by

$$x_h[k+1] = \mathcal{A}_{\sigma[k]} x_h[k] + \mathcal{B}_{\sigma[k]} u[k], \quad \sigma[k] \in \Omega = \{1, 2, \dots, M\} , \quad (7)$$

where the initial state $x_h[0]$, and all $\eta \times \eta$ transition matrices $\mathcal{A}_{\sigma[k]}$ and $\eta \times m$ input matrices $\mathcal{B}_{\sigma[k]}$ will be chosen such that, under fault-free conditions, \mathcal{H} provides complete information about the original system \mathcal{S} , and vice-versa. As in the single system case described in the previous section, we restrict ourselves to linear encoding and decoding mappings, i.e., we require that there exist matrices \mathbf{L} and \mathbf{G} such that, when $x_h[0] = \mathbf{G}x[0]$ and under fault-free conditions, we have $x[k] = \mathbf{L}x_h[k]$ and $x_h[k] = \mathbf{G}x[k]$ for all k . Faults that cause the state $x_h[k]$ to lie outside the column space of \mathbf{G} can be detected through the use of a *parity check* of the form $\mathbf{s}[k] \equiv \mathbf{P}x_h[k]$, where \mathbf{P} is an appropriate parity check matrix of dimension $d \times \eta$. More specifically, by selecting \mathbf{P} to be full row-rank and satisfy $\mathbf{P}\mathbf{G} = \mathbf{0}$, we can check for errors in $x_h[k]$ by performing the calculation $\mathbf{P}x_h[k]$ and ensuring that it is identically zero.

Theorem 1. *In the setting described above, the switched system \mathcal{H} in (7) is a redundant implementation for the switched system \mathcal{S} in (5) (i.e., it satisfies (2) and (3) for all time steps k) if and only if there exists an $\eta \times \eta$ transformation matrix \mathcal{T} and a standard redundant switched system \mathcal{H}_r with state evolution given by*

$$x_r[k+1] = \mathcal{A}_{r_{\sigma[k]}} x_r[k] + \mathcal{B}_{r_{\sigma[k]}} u[k], \quad \sigma[k] \in \Omega = \{1, 2, \dots, M\} , \quad (8)$$

where

$$\mathcal{T}^{-1} \mathcal{A}_{\sigma[k]} \mathcal{T} = \begin{bmatrix} \mathbf{A}_{\sigma[k]} & \mathbf{A}_{12_{\sigma[k]}} \\ \mathbf{0} & \mathbf{A}_{22_{\sigma[k]}} \end{bmatrix} \equiv \mathcal{A}_{r_{\sigma[k]}} , \quad (9)$$

$$\mathcal{T}^{-1} \mathcal{B}_{\sigma[k]} = \begin{bmatrix} \mathbf{B}_{\sigma[k]} \\ \mathbf{0} \end{bmatrix} \equiv \mathcal{B}_{r_{\sigma[k]}} , \quad (10)$$

$$\mathbf{L}\mathcal{T} = [\mathbf{I}_n \ \mathbf{0}] \equiv \mathbf{L}_r , \quad (11)$$

$$\mathcal{T}^{-1} \mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{0} \end{bmatrix} \equiv \mathbf{G}_r \quad (12)$$

$$\mathbf{P}\mathcal{T} = [\mathbf{0} \ \mathbf{I}_d] \equiv \mathbf{P}_r . \quad (13)$$

In the above theorem, $\mathbf{A}_{\sigma[k]}$ and $\mathbf{B}_{\sigma[k]}$ are the matrices from the original system \mathcal{S} , and $\mathcal{A}_{\sigma[k]}$ and $\mathcal{B}_{\sigma[k]}$ are the matrices from the redundant implementation \mathcal{H} . The $d \times d$ matrices $\mathbf{A}_{22\sigma[k]}$ describe the added redundant dynamics associated with the system that is active at time step k . The $n \times d$ matrices $\mathbf{A}_{12\sigma[k]}$ describe the coupling between the redundant and original states at time step k . Associated with this standard redundant system \mathcal{H}_r , we have the decoding, encoding and parity check matrices given by \mathbf{L}_r , \mathbf{G}_r and \mathbf{P}_r respectively.

The proof of Theorem 1 is similar to the proof for the single system case given in [19], and is omitted here. Note that we are completely free to choose matrices $\mathbf{A}_{12\sigma[k]}$ and $\mathbf{A}_{22\sigma[k]}$; thus, there are many redundant implementations of \mathcal{S} for a given \mathbf{L} and \mathbf{G} . Later in this paper, we will discuss how to choose $\mathbf{A}_{22\sigma[k]}$ to allow non-concurrent error detection and correction.

3.3 Transient State-Transition Faults and Error Propagation

As mentioned earlier, our goal is to design a redundant switched system \mathcal{H} so that we can protect the original switched system \mathcal{S} against transient state-transition faults. For now, we assume that a transient fault during the calculation of the next state at time step $k - 1$ causes an error in exactly one of the state variables in the next state vector. It will become clear from our discussion that this assumption can be relaxed, but we adopt it now for pedagogical purposes.

Assume (without loss of generality) that our system begins operation with $x_h[0] = \mathbf{G}x[0]$ and that the first non-concurrent check is performed at the end of time step $N - 1$ (i.e., at the beginning of time step N). If a single error occurs in our system at time step $k = N - t - 1$, $0 \leq t \leq N - 1$, and affects the i th state variable by an additive error value v , the erroneous state vector at the beginning of time step $k = N - t$ will be given by

$$x_f[N - t] = x_h[N - t] + ve_i \text{ ,} \quad (14)$$

where $x_h[N - t]$ is the state that \mathcal{H} would be in at the beginning of time step $N - t$ under fault-free conditions, and e_i is an η -dimensional vector with a “1” as its i th entry and “0” everywhere else. Note that through an appropriate choice of v and e_i , this additive error model can be used to handle any fault that corrupts a single state variable.

If we were to perform a (concurrent) parity check at the end of time step $N - t - 1$ (beginning of time step $N - t$), we would get the syndrome

$$\mathbf{s}[N - t] \equiv \mathbf{P}x_f[N - t] = \mathbf{P}ve_i = v\mathbf{P}(:, i) \text{ ,}$$

where $\mathbf{P}(:, i)$ denotes the i th column of the parity check matrix \mathbf{P} . In the above expansion, we have used the fact that $\mathbf{P}x_h[k] = \mathbf{P}\mathbf{G}x[k] = 0$ for all k . Assuming that no further errors occur in the interval $[N - t, N - 1]$, we can use (6) to

obtain the erroneous state of system \mathcal{H} at the end of time step $N - 1$:

$$x_f[N] = \left(\prod_{i=N-t}^{N-1} \mathcal{A}_{\sigma[i]} \right) x_f[N-t] + \left(\prod_{i=N-t+1}^{N-1} \mathcal{A}_{\sigma[i]} \right) \mathcal{B}_{\sigma[N-t]} u[N-t] + \dots \\ \dots + \mathcal{A}_{\sigma[N-1]} \mathcal{B}_{\sigma[N-2]} u[N-2] + \mathcal{B}_{\sigma[N-1]} u[N-1] .$$

Substituting our expression for the erroneous state variable from (14) into the above equation, we obtain

$$x_f[N] = x_h[N] + v \left(\prod_{i=N-t}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_i ,$$

where $x_h[N]$ is the error-free state that \mathcal{H} would have been in at the beginning of time step N , had there been no fault. Clearly, the parity check that is performed at the end of time step $N - 1$ will yield the syndrome

$$\mathbf{s}[N] \equiv \mathbf{P}x_f[N] = v\mathbf{P} \left(\prod_{i=N-t}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_i \quad (15)$$

because $\mathbf{P}x_h[N] = \mathbf{P}\mathbf{G}x[N] = 0$.

Theorem 2. *Let switched system \mathcal{S} have a redundant implementation \mathcal{H} , whose corresponding standard redundant switched system \mathcal{H}_r satisfies*

$$\mathcal{T}^{-1} \mathcal{A}_{\sigma[k]} \mathcal{T} = \begin{bmatrix} \mathbf{A}_{\sigma[k]} & \mathbf{A}_{12\sigma[k]} \\ 0 & \mathbf{A}_{22\sigma[k]} \end{bmatrix} \equiv \mathcal{A}_{r_{\sigma[k]}}$$

for all $\sigma[k] \in \Omega = \{1, 2, \dots, M\}$. The non-concurrent syndrome $\mathbf{s}[N]$ due to a single transient state-transition fault that occurs during the execution of time step $N - t - 1$ and corrupts the i th state variable by an additive value v is equal to

$$\mathbf{s}[N] \equiv \mathbf{P}x_f[N] = v \left(\prod_{i=N-t}^{N-1} \mathbf{A}_{22\sigma[i]} \right) \mathbf{P}e_i .$$

Proof. From (15), the syndrome $\mathbf{s}[N]$ will be given by

$$\begin{aligned} \mathbf{s}[N] &= v\mathbf{P} \left(\prod_{i=N-t}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_i \\ &= v\mathbf{P} \left(\prod_{i=N-t}^{N-1} \mathcal{T} \mathcal{A}_{r_{\sigma[i]}} \mathcal{T}^{-1} \right) e_i \\ &= v\mathbf{P}\mathcal{T} \left(\prod_{i=N-t}^{N-1} \mathcal{A}_{r_{\sigma[i]}} \right) \mathcal{T}^{-1} e_i \\ &= v\mathbf{P}\mathcal{T} \begin{bmatrix} * & * \\ 0 & \prod_{i=N-t}^{N-1} \mathbf{A}_{22\sigma[i]} \end{bmatrix} \mathcal{T}^{-1} e_i \end{aligned}$$

$$\begin{aligned}
&= v \mathbf{P}_r \begin{bmatrix} * & \\ 0 & \prod_{i=N-t}^{N-1} \mathbf{A}_{22\sigma[i]}^* \end{bmatrix} \mathcal{T}^{-1} e_i && \text{(from (13))} \\
&= v \left(\prod_{i=N-t}^{N-1} \mathbf{A}_{22\sigma[i]} \right) [0 \quad \mathbf{I}_d] \mathcal{T}^{-1} e_i \\
&= v \left(\prod_{i=N-t}^{N-1} \mathbf{A}_{22\sigma[i]} \right) \mathbf{P} e_i . && \text{(from (13))}
\end{aligned}$$

In the above calculations, the symbol $*$ stands for arbitrary matrices of appropriate dimensions. We have made use of the fact that all matrices $\mathcal{A}_{r,\sigma[k]}$ are upper-triangular, so their product is also an upper-triangular matrix. The bottom d rows of this product only depend on the matrices $\mathbf{A}_{22\sigma[k]}$, which describe the redundant dynamics in the standard implementation \mathcal{H}_r associated with \mathcal{H} . \square

Notice that if all $\mathbf{A}_{22\sigma[k]}$ are chosen to be identical (i.e., some constant matrix \mathbf{A}_{22}) then the syndrome at time step N will be

$$\mathbf{s}[N] \equiv \mathbf{P} x_f[N] = v \mathbf{A}_{22}^t \mathbf{P} e_i ,$$

which is independent of the switching sequence.

We can now generalize the above results to the case of multiple faults within the interval $[0, N-1]$. We assume that a total of D transient faults occur at time steps $N-t_1-1, N-t_2-1, \dots, N-t_D-1$, originally corrupting state variables i_1, i_2, \dots, i_D by initial additive errors of v_1, v_2, \dots, v_D respectively. We also assume (without loss of generality) that $0 \leq t_D \leq t_{D-1} \leq \dots \leq t_1 \leq N-1$. The erroneous state at the end of time step $N-t_2-1$ will be

$$x_f[N-t_2] = x_h[N-t_2] + v_1 \left(\prod_{i=N-t_1}^{N-t_2-1} \mathcal{A}_{\sigma[i]} \right) e_{i_1} + v_2 e_{i_2} .$$

Similarly, the state at the end of time step $N-t_3-1$ will be

$$x_f[N-t_3] = x_h[N-t_3] + v_1 \left(\prod_{i=N-t_1}^{N-t_3-1} \mathcal{A}_{\sigma[i]} \right) e_{i_1} + v_2 \left(\prod_{i=N-t_2}^{N-t_3-1} \mathcal{A}_{\sigma[i]} \right) e_{i_2} + v_3 e_{i_3} .$$

Continuing in this manner for the rest of the errors, we obtain the following expression for the erroneous state at the end of time step $N-1$:

$$\begin{aligned}
x_f[N] &= x_h[N] + v_1 \left(\prod_{i=N-t_1}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_1} + v_2 \left(\prod_{i=N-t_2}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_2} + \dots \\
&\quad \dots + v_D \left(\prod_{i=N-t_D}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_D} \\
&= x_h[N] + \sum_{j=1}^D \left\{ v_j \left(\prod_{i=N-t_j}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_j} \right\} .
\end{aligned}$$

This leads us to the following generalization of Theorem 2.

Theorem 3. *Let switched system \mathcal{S} have a redundant implementation \mathcal{H} , whose corresponding standard redundant switched system \mathcal{H}_r satisfies*

$$\mathcal{T}^{-1} \mathcal{A}_{\sigma[k]} \mathcal{T} = \begin{bmatrix} \mathbf{A}_{\sigma[k]} & \mathbf{A}_{12_{\sigma[k]}} \\ 0 & \mathbf{A}_{22_{\sigma[k]}} \end{bmatrix} \equiv \mathcal{A}_{r_{\sigma[k]}}$$

for all $\sigma[k] \in \Omega = \{1, 2, \dots, M\}$. The non-concurrent syndrome $\mathbf{s}[N]$ due to D transient state-transition faults that occur during time steps $N - t_1 - 1, N - t_2 - 1, \dots, N - t_D - 1$, and corrupt state variables i_1, i_2, \dots, i_D by initial additive errors of v_1, v_2, \dots, v_D respectively is equal to

$$\mathbf{s}[N] \equiv \mathbf{P} \mathbf{x}_f[N] = \sum_{j=1}^D \left\{ v_j \left(\prod_{i=N-t_j}^{N-1} \mathbf{A}_{22_{\sigma[i]}} \right) \mathbf{P} e_{i_j} \right\} .$$

Notice that if all $\mathbf{A}_{22_{\sigma[k]}}$ are chosen to be identical (i.e., some constant matrix \mathbf{A}_{22}) then the syndrome at time step N will be

$$\mathbf{s}[N] \equiv \mathbf{P} \mathbf{x}_f[N] = \sum_{j=1}^D \left\{ v_j \mathbf{A}_{22}^{t_j} \mathbf{P} e_{i_j} \right\} , \quad (16)$$

which is independent of the switching sequence.

The proof of Theorem 3 mirrors the earlier proof, and is omitted here.

3.4 Multiple Error Detection, Identification and Correction

We now present a method to construct a redundant implementation \mathcal{H} of the switched system \mathcal{S} given by (5) so that we can perform non-concurrent error detection, identification and correction of multiple errors. For simplicity, we will choose $\mathbf{A}_{22_{\sigma[k]}} = \mathbf{A}_{22}$ for all $\sigma[k] \in \Omega = \{1, 2, \dots, M\}$, where \mathbf{A}_{22} is a constant $d \times d$ matrix to be determined.

From (16), we can see that if D transient state-transition faults occur at time steps $0 \leq N - t_1 - 1 \leq N - t_2 - 1 \leq \dots \leq N - t_D - 1 \leq N - 1$, and corrupt state variables i_1, i_2, \dots, i_D by initial additive errors of v_1, v_2, \dots, v_D respectively, then the syndrome at the end of time step $N - 1$ will be a linear combination of D columns of the $d \times N\eta$ syndrome matrix

$$\mathbf{S} = [\mathbf{P} \quad \mathbf{A}_{22} \mathbf{P} \quad \mathbf{A}_{22}^2 \mathbf{P} \quad \dots \quad \mathbf{A}_{22}^{N-1} \mathbf{P}] . \quad (17)$$

In order to detect D or less errors in the interval $[0, N - 1]$, we need all linear combinations of any subset of D columns of \mathbf{S} to be nonzero. To be able to uniquely identify the originally affected variables (i_1, i_2, \dots, i_D), the values by which they were initially corrupted (v_1, v_2, \dots, v_D), and the time steps during which the errors took place ($N - t_1 - 1, N - t_2 - 1, \dots, N - t_D - 1$), we need

all linear combinations of any subset of D columns of \mathbf{S} to be different from a linear combination of any other subset of D columns of \mathbf{S} . To see why this condition is required, assume that we have two different subsets of D columns of \mathbf{S} , $\{s_{l_1}, s_{l_2}, \dots, s_{l_D}\}$ and $\{s'_{l_1}, s'_{l_2}, \dots, s'_{l_D}\}$, such that $\sum_{j=1}^D \alpha_j s_{l_j} = \sum_{j=1}^D \beta_j s'_{l_j}$. In this case, the corresponding two sets of errors cannot be distinguished by the syndrome $\mathbf{s}[N]$.

Later on we describe how the redundant system can be constructed so that detection and identification of D (or less) errors is possible; for now, assuming that the system is constructed in this way, the following procedure describes how errors can be detected, identified and eventually corrected.

1. At the end of time step $N - 1$, calculate $\mathbf{s}[N] = \mathbf{P}x_f[N]$.
2. Find the unique linear combination of D' ($D' \leq D$) columns of the syndrome matrix \mathbf{S} that results in $\mathbf{s}[N] = \sum_{i=1}^{D'} \alpha_i \mathbf{S}(:, l_i)$. It is possible to use a modified version of the Peterson-Gorestein-Zeigler (PGZ) decoding algorithm to efficiently determine the D' errors based on the syndrome $\mathbf{s}[N]$, without resorting to an exhaustive search. The details are presented in [18], and are omitted here. We can now identify the unique combination of errors of the form v_j, e_{i_j} , and $t_j, j \in \{1, 2, \dots, D'\}$ (the j th error takes place during time step $N - t_j - 1$ and originally affects the (i_j) th state variable by an initial value v_j), such that $\mathbf{s}[N] = \sum_{j=1}^{D'} v_j \mathbf{A}_{22}^{t_j} \mathbf{P}e_{i_j}$ as follows:

$$v_j = \alpha_j \quad , \quad i_j = 1 + [(l_j - 1) \bmod \eta] \quad , \quad t_j = \frac{l_j - i_j}{\eta} \quad .$$

3. Declare that D' errors have taken place in the interval $[0, N - 1]$.
4. If the switching sequence over the last N cycles is known, we can perform error correction by setting

$$x_h[N] = x_f[N] - \sum_{j=1}^{D'} \left\{ v_j \left(\prod_{i=N-t_j}^{N-1} \mathcal{A}_{\sigma[i]} \right) e_{i_j} \right\} \quad ,$$

where $x_f[N]$ is the current erroneous state at time step N . In the specific case where the switching pattern $\sigma[k]$ is periodic (as in [9], for example) of period N , this error correction can be done by precomputing the $N - 1$ matrices

$$\left\{ \mathcal{A}_{\sigma[N-1]} \quad , \quad \mathcal{A}_{\sigma[N-1]} \mathcal{A}_{\sigma[N-2]} \quad , \quad \dots \quad , \quad \prod_{j=1}^{N-1} \mathcal{A}_{\sigma[j]} \right\} \quad ,$$

and selecting the appropriate ones to use in the correction step.

Due to the fact that the syndrome matrix in (17) is the same as the one in [18], we can adapt the construction given there to this case. More specifically, we would like to choose the matrices \mathbf{A}_{22} and \mathbf{P} in such a way that the syndrome matrix \mathbf{S} has the rank properties required for error detection and identification

(namely, for correction of up to D errors, any subset of $2D$ columns of \mathbf{S} are linearly independent). We start by recalling the definition of the Vandermonde matrix.

Definition 1. Let $\mathbf{V}(w_1, w_2, \dots, w_\rho)$ denote the $2D \times \rho$ matrix

$$\mathbf{V}(w_1, w_2, \dots, w_\rho) = \begin{bmatrix} w_1 & w_2 & \dots & w_\rho \\ w_1^2 & w_2^2 & \dots & w_\rho^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{2D-1} & w_2^{2D-1} & \dots & w_\rho^{2D-1} \\ w_1^{2D} & w_2^{2D} & \dots & w_\rho^{2D} \end{bmatrix} .$$

It is well-known that Vandermonde matrices of the form $\mathbf{V}(w_1, w_2, \dots, w_{2D})$ are invertible if and only if $w_i \neq 0$ for $1 \leq i \leq 2D$ and $w_i \neq w_j$ for $1 \leq i < j \leq 2D$. We are now in position to prove the following theorem.

Theorem 4. Let switched system \mathcal{S} have a redundant implementation \mathcal{H} , whose corresponding standard redundant switched system \mathcal{H}_r satisfies (for all $\sigma[k] \in \Omega = \{1, 2, \dots, M\}$)

$$\mathcal{T}^{-1} \mathcal{A}_{\sigma[k]} \mathcal{T} = \begin{bmatrix} \mathbf{A}_{\sigma[k]} & \mathbf{A}_{12\sigma[k]} \\ \mathbf{0} & \mathbf{A}_{22} \end{bmatrix} \equiv \mathcal{A}_{r_{\sigma[k]}}$$

for a constant matrix \mathbf{A}_{22} . Any D or less errors due to transient faults in the interval $[0, N-1]$ will be detected and identified by a parity check at the end of time step $N-1$ if the following conditions are satisfied:

1. The corresponding standard redundant switched system (as given in (8)-(13) of Theorem 1) satisfies the following conditions:
 - (a) The number of additional state variables is $d = 2D$.
 - (b) The $2D \times 2D$ matrix \mathbf{A}_{22} is of the form

$$\mathbf{A}_{22} = \mathbf{M}^{-1} \mathbf{A} \mathbf{M} ,$$

where (i) $\mathbf{A} = \text{diag}(w, w^2, w^3, \dots, w^{2D-1}, w^{2D})$ is a $2D \times 2D$ diagonal matrix and (ii) $\mathbf{M} = \mathbf{V}(w_{n+1}, w_{n+2}, \dots, w_n)$ is a $2D \times 2D$ Vandermonde matrix.

2. The $\eta \times \eta$ transformation matrix \mathcal{T} that is used to transform from the standard redundant switched system \mathcal{H}_r to the redundant switched system \mathcal{H} is given by

$$\mathcal{T} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{C} & \mathbf{I}_{2D} \end{bmatrix} ,$$

where the $2D \times n$ matrix \mathbf{C} is chosen so that

$$\mathbf{C} = -\mathbf{M}^{-1} \mathbf{V}(w_1, w_2, \dots, w_n) .$$

3. The real numbers w and w_1, w_2, \dots, w_η are chosen so that
- (a) $w_i \neq 0$ for $1 \leq i \leq \eta$;
 - (b) $w_i \neq w_j$ for $1 \leq i < j \leq \eta$;
 - (c) $w^t w_i \neq w^{t'} w_j$ for $1 \leq i, j \leq \eta$ and $0 \leq t < t' \leq N - 1$.

Proof. We start with the standard redundant switched system \mathcal{H}_r given by (8)-(13), and set $x_h[k] = \mathcal{T}x_r[k]$, where $\mathcal{T} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{C} & \mathbf{I}_{2D} \end{bmatrix}$. This yields a redundant implementation with the following state evolution:

$$x_h[k+1] = \underbrace{\begin{bmatrix} \mathbf{A}_{\sigma[k]} - \mathbf{A}_{12\sigma[k]} \mathbf{C} & \mathbf{A}_{12\sigma[k]} \\ \mathbf{C} \mathbf{A}_{\sigma[k]} - \mathbf{C} \mathbf{A}_{12\sigma[k]} \mathbf{C} - \mathbf{A}_{22} \mathbf{C} & \mathbf{C} \mathbf{A}_{12\sigma[k]} + \mathbf{A}_{22} \end{bmatrix}}_{\mathbf{A}_{\sigma[k]} = \mathcal{T} \mathbf{A}_{r_{\sigma[k]}} \mathcal{T}^{-1}} x_h[k] + \underbrace{\begin{bmatrix} \mathbf{B}_{\sigma[k]} \\ \mathbf{C} \mathbf{B}_{\sigma[k]} \end{bmatrix}}_{\mathbf{B}_{\sigma[k]} = \mathcal{T} \mathbf{B}_{r_{\sigma[k]}}} u[k]. \quad (18)$$

Note that the parity check matrix for \mathcal{H} is given by $\mathbf{P} = \mathbf{P}_r \mathcal{T}^{-1} = [-\mathbf{C} \ \mathbf{I}_{2D}]$, where $\mathbf{C} = -\mathbf{M}^{-1} \mathbf{V}(w_1, w_2, \dots, w_\eta)$. The syndrome matrix \mathbf{S} in (17) consists of submatrices of the form $\mathbf{A}_{22}^t \mathbf{P}$. With the choice of \mathbf{P} and \mathbf{A}_{22} from the theorem, it is shown in [18] that

$$\mathbf{A}_{22}^t \mathbf{P} = \mathbf{M}^{-1} \mathbf{V}(w_1 w^t, w_2 w^t, \dots, w_\eta w^t), \quad (19)$$

so that the syndrome matrix \mathbf{S} can be expressed as

$$\mathbf{S} = \mathbf{M}^{-1} \mathbf{V}(w_1, \dots, w_\eta, w_1 w, \dots, w_\eta w, \dots, w_1 w^{N-1}, \dots, w_\eta w^{N-1}).$$

Note that all the parameters in the above syndrome matrix are unique, due to the restrictions on parameters $w, w_1, w_2, \dots, w_\eta$ as given in Condition 3 of the theorem. This guarantees that any $2D$ or less columns are independent, which implies that we can detect and identify any combination of D' ($D' \leq D$) errors in the interval $[0, N-1]$. The same approach can also detect, but not necessarily identify, $2D$ or less errors in the interval $[0, N-1]$. \square

4 Example

Consider a switched system \mathcal{S} of the form given in (5), which switches between two linear systems, described by matrix pairs $(\mathbf{A}_1, \mathbf{B}_1)$ and $(\mathbf{A}_2, \mathbf{B}_2)$, and a switching path $\sigma[k] \in \Omega = \{1, 2\}$, $k \geq 0$. The system has $n = 3$ state variables and $m = 1$ input (i.e., $x[k] \in \mathbb{R}^3$, $u[k] \in \mathbb{R}$), and the two pairs of matrices are given by

$$\mathbf{A}_1 = \begin{bmatrix} -1/2 & 1 & 0 \\ 1/4 & 0 & 1 \\ 1/5 & 0 & 0 \end{bmatrix}, \quad \mathbf{B}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix};$$

$$\mathbf{A}_2 = \begin{bmatrix} -1/5 & 1 & 0 \\ 1/3 & 0 & 1 \\ 1/9 & 0 & 0 \end{bmatrix}, \quad \mathbf{B}_2 = \begin{bmatrix} 1.5 \\ 1 \\ 0 \end{bmatrix}.$$

We wish to protect the system \mathcal{S} in a way that allows us to detect and identify two or less transient state-transition faults in the interval $[0, 9]$ (i.e., $D = 2$ and $N = 10$). According to Theorem 4, we need $d = 2D = 4$ extra state variables to provide such protection, giving us a total of $\eta = n + d = 3 + 4 = 7$ state variables. We choose the parameters w_i , $1 \leq i \leq 7$, to be

$$\{w_1, w_2, w_3, w_4, w_5, w_6, w_7\} = \{-1, 1, -3, 3, -5, 5, 7\} ,$$

and set $w = \frac{1}{2}$. Note that this choice of parameters satisfies Condition 3 of Theorem 4. With these parameters, the Vandermonde matrix \mathbf{M} and the diagonal matrix Λ are

$$\mathbf{M} = \mathbf{V}(w_4, w_5, w_6, w_7) = \begin{bmatrix} 3 & -5 & 5 & -7 \\ 9 & 25 & 25 & 49 \\ 27 & -125 & 125 & -343 \\ 81 & 625 & 625 & 2401 \end{bmatrix} ,$$

$$\Lambda = \text{diag}(w, w^2, w^3, w^4) = \begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1/8 & 0 \\ 0 & 0 & 0 & 1/16 \end{bmatrix} .$$

Matrix \mathbf{C} is set to

$$\mathbf{C} = -\mathbf{M}^{-1}\mathbf{V}(w_1, w_2, w_3) = \begin{bmatrix} 0.3000 & -0.4000 & 0.4000 \\ -0.1800 & 0.0800 & -0.7200 \\ -0.0800 & 0.0800 & -0.1200 \\ 0.0571 & -0.0286 & 0.1714 \end{bmatrix} .$$

The transformation matrix \mathcal{T} is

$$\mathcal{T} = \left[\begin{array}{c|c} \mathbf{I}_n & \mathbf{0} \\ \mathbf{C} & \mathbf{I}_{2D} \end{array} \right] = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0.3000 & -0.4000 & 0.4000 & 1 & 0 & 0 & 0 \\ -0.1800 & 0.0800 & -0.7200 & 0 & 1 & 0 & 0 \\ -0.0800 & 0.0800 & -0.1200 & 0 & 0 & 1 & 0 \\ 0.0571 & -0.0286 & 0.1714 & 0 & 0 & 0 & 1 \end{array} \right] ,$$

and is used to obtain the parity check matrix given by (13):

$$\mathbf{P} = [\mathbf{0}|\mathbf{I}_4] \mathcal{T}^{-1} = [-\mathbf{C}|\mathbf{I}_4] = \left[\begin{array}{ccc|cccc} -0.3000 & 0.4000 & -0.4000 & 1 & 0 & 0 & 0 \\ 0.1800 & -0.0800 & 0.7200 & 0 & 1 & 0 & 0 \\ 0.0800 & -0.0800 & 0.1200 & 0 & 0 & 1 & 0 \\ -0.0571 & 0.0286 & -0.1714 & 0 & 0 & 0 & 1 \end{array} \right] .$$

We are now ready to construct the standard redundant transition matrices given by equations (9)-(10). We choose the coupling matrices $\mathbf{A}_{12_{\sigma[k]}} = \mathbf{0}$ for

all $\sigma[k] \in \Omega$, and keep the redundant matrix $\mathbf{A}_{22_{\sigma[k]}} = \mathbf{A}_{22}$ for all $\sigma[k] \in \Omega$. Following the construction in Theorem 4, the \mathbf{A}_{22} matrix is given by

$$\mathbf{A}_{22} = \mathbf{M}^{-1} \mathbf{A} \mathbf{M} = \begin{bmatrix} 0.6043 & -0.4395 & 0.9277 & -0.3254 \\ -0.0837 & 0.5801 & -0.0371 & 0.8460 \\ -0.1036 & 0.1289 & -0.0742 & 0.0995 \\ 0.0305 & -0.1535 & 0.0140 & -0.1727 \end{bmatrix} .$$

The transition matrices of the redundant implementation are given by (18) and are shown below:

$$\mathcal{A}_1 = \left[\begin{array}{ccc|cccc} -0.5000 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0.2500 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0.2000 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline -0.3376 & 0.4934 & -0.7910 & 0.6043 & -0.4395 & 0.9277 & -0.3254 \\ 0.0442 & -0.2327 & 0.3816 & -0.0837 & 0.5801 & -0.0371 & 0.8460 \\ 0.0787 & -0.1230 & 0.1883 & -0.1036 & 0.1289 & -0.0742 & 0.0995 \\ -0.0272 & 0.0756 & -0.1200 & 0.0305 & -0.1535 & 0.0140 & -0.1727 \end{array} \right] ,$$

$$\mathcal{A}_2 = \left[\begin{array}{ccc|cccc} -0.2000 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0.3333 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0.1111 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline -0.3165 & 0.4934 & -0.7910 & 0.6043 & -0.4395 & 0.9277 & -0.3254 \\ 0.0609 & -0.2327 & 0.3816 & -0.0837 & 0.5801 & -0.0371 & 0.8460 \\ 0.0720 & -0.1230 & 0.1883 & -0.1036 & 0.1289 & -0.0742 & 0.0995 \\ -0.0277 & 0.0756 & -0.1200 & 0.0305 & -0.1535 & 0.0140 & -0.1727 \end{array} \right] ,$$

$$\mathcal{B}_1 = [1 \ 0 \ 1 | 0.7000 \ -0.9000 \ -0.2000 \ 0.2286]^T ,$$

$$\mathcal{B}_2 = [1.5 \ 1 \ 0 | 0.0500 \ -0.1900 \ -0.0400 \ 0.0571]^T .$$

From (17) and (19), the syndrome matrix for non-concurrent error detection and correction in this system is given by

$$\mathbf{S} = \mathbf{M}^{-1} [\mathbf{S}_0 \ \mathbf{S}_1 \ \mathbf{S}_2 \ \cdots \ \mathbf{S}_9] ,$$

where $\mathbf{S}_t = \mathbf{V}(-w^t, w^t, -3w^t, 3w^t, -5w^t, 5w^t, 7w^t)$, $w = \frac{1}{2}$. The modified syndrome matrix is given by

$$\mathbf{S}' = \mathbf{M} \mathbf{S} = [\mathbf{S}_0 \ \mathbf{S}_1 \ \mathbf{S}_2 \ \cdots \ \mathbf{S}_9] .$$

Once the redundant system is constructed, let us assume it is operating under some switching sequence $\sigma[k] \in \Omega$, and some input $u[k]$. Let us also assume that two transient faults take place in the interval $[0, 9]$ as follows.

1. Fault 1 takes place during time step 1, and corrupts the fifth state variable with an additive initial error of value 0.4.
2. Fault 2 takes place during time step 7, and corrupts the fourth state variable with an additive initial error of value 0.95.

The syndrome at the end of time step 9 (beginning of time step 10) is given by

$$\mathbf{s}[10] = \mathbf{P}x_f[10] = [0.2783 \quad -0.0650 \quad -0.0588 \quad 0.0230]^T$$

and the modified syndrome is given by

$$\mathbf{s}'[10] = \mathbf{M}\mathbf{s}[10] = [0.7047 \quad 0.5345 \quad 0.4008 \quad 0.3006]^T .$$

Note that the syndrome does not depend on the actual input *or* switching sequence that is applied to the system, as long as the faults take place at the same time steps and originally affect the same state variables by the same initial additive errors. The only way we can write our modified syndrome as a linear combination of at most two columns of \mathbf{S}' is given by

$$\mathbf{s}'[10] = 0.4\mathbf{S}_8(:, 5) + 0.95\mathbf{S}_2(:, 4) .$$

Therefore, we conclude that there have been two faults: one affecting the fifth state variable at time step 1 ($= 10 - 8 - 1$) by an additive error of 0.4, and one affecting the fourth state variable at time step 7 ($= 10 - 2 - 1$) by an additive error of 0.95. A systematic method of determining the above linear combination is presented in [18].

5 Conclusions

In this paper, we have presented a methodology for providing fault tolerance to discrete-time controllers in switched LTI systems through non-concurrent (e.g., periodic) error detection and correction. Specifically, we showed how to embed the state-space of the controllers into a larger redundant state-space, so that all information about the initial system is preserved, but with the added capability to detect and identify transient faults that affect state variables. The ability to perform error detection non-concurrently allows the reliability constraints of the error-checking mechanism to be relaxed.

There are a number of interesting directions for future research in this area:

1. How can we make use of the flexibility in the coupling dynamics between the original and redundant state variables (given by matrix $\mathbf{A}_{12_{\sigma[k]}}$ in Theorem 1)?
2. How can we design systems that are optimal in terms of minimizing the number of redundant arithmetic operations that are performed (instead of minimizing the number of redundant state variables)?
3. When working in the realm of real numbers, finite-precision issues must be considered during the design of the redundant system. How can we choose redundant dynamics in our system to provide robustness in the face of these issues?

Furthermore, it will be interesting to study various methods of mapping this system into hardware.

References

1. Morse, A.S., ed.: Control Using Logic-Based Switching. Springer-Verlag (1997)
2. Zefran, M., Burdick, J.: Design of switching controllers for systems with changing dynamics. In: Proc. 37th IEEE Conf. on Decision and Control. Volume 2. (1998) 2113–2118
3. Hespanha, J., Liberzon, D., Morse, A.: Logic-based switching control of a nonholonomic system with parametric modeling uncertainty. Systems and Control Letters, Special Issue on Hybrid Systems **38** (1999) 167–177
4. Hespanha, J.: Logic-Based Switching Algorithms in Control. PhD thesis, Yale University (1998)
5. Liberzon, D.: Switching in Systems and Control. Birkhauser (2003)
6. Ge, S.S., Sun, Z., Lee, T.H.: Reachability and controllability of switched linear discrete-time systems. IEEE Transactions on Automatic Control **46** (2001) 1437–1441
7. Liberzon, D., Morse, A.: Basic problems in stability and design of switched systems. IEEE Control Systems Magazine **19** (1999) 59–70
8. Xie, G., Zheng, D., Wang, L.: Controllability of switched linear systems. IEEE Transactions on Automatic Control **47** (2002) 1401–1405
9. Ezzine, J., Haddad, A.H.: Controllability and observability of hybrid systems. International Journal of Control **49** (1989) 2045–2055
10. Sangiovanni-Vincentelli, A.: Embedded system design and hybrid systems. In Morse, A.S., ed.: Control Using Logic-Based Switching. Springer-Verlag (1997) 17–38
11. Gray, W.S., Gonzalez, O.R., Dogan, M.: Stability analysis of digital linear flight controllers subject to electromagnetic disturbances. IEEE Transactions on Aerospace and Electronic Systems **36** (2000) 1204–1218
12. Gray, W.S., Patilkulkarni, S., Gonzalez, O.R.: Towards hybrid models of recoverable computer control systems. In: Proc. 2002 Digital Avionics Systems Conference. (2002) 13.C.2–1–9
13. Babaali, M., Egerstedt, M., Kamen, E.W.: An observer for linear systems with randomly-switching measurement equations. In: Proc. 2003 American Control Conference. (2003) 1879–1884
14. Smith, S.C., Seiler, P.: Optimal pseudo-steady-state estimators for systems with Markovian intermittent measurements. In: Proc. 2002 American Control Conference. (2002) 3021–3027
15. von Neumann, J.: Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components. Princeton, NJ: Princeton Univ. Press (1956)
16. Rao, T.R.N., Fujiwara, E.: Error-Control Coding for Computer Systems. Englewood Cliffs, NJ:Prentice-Hall (1989)
17. Huang, K.H., Abraham, J.A.: Algorithm-based fault tolerance for matrix operations. IEEE Transactions on Computers **33** (1984) 518–528
18. Hadjicostis, C.N.: Non-concurrent error detection and correction in fault-tolerant discrete-time LTI dynamic systems. IEEE Transactions on Circuits and Systems **50** (2003) 45–55
19. Hadjicostis, C.N., Verghese, G.: Structured redundancy for fault tolerance in LTI state-space models and Petri nets. Kybernetika **35** (1999) 39–55