Output Reachable Set Estimation for Switched Linear Systems and Its Application in Safety Verification

Weiming Xiang, Hoang-Dung Tran, and Taylor T. Johnson

***Abstract*—This paper addresses the output reachable set estimation problem for continuous-time switched linear systems consisting of Hurwtiz stable subsystems. Based on a common Lyapunov function approach, the output reachable set is estimated by a union of bounding ellipsoids. Then, multiple Lyapunov functions with time-scheduled structure are employed to estimate the output reachable set for switched systems under dwell time constraint. Furthermore, the safety verification problem of uncertain switched systems is investigated based on the result of output reachable set estimation. First, a sufficient condition ensuring the existence of an approximate bisimulation relation between two switched linear systems with a prescribed precision is proposed. Then, the safety verification for an uncertain switched system can be performed through an alternative safety verification for a switched system with exact parameters. Numerical examples are provided to illustrate our results.**

***Index Terms*—Reachable set estimation, safety verification, switched system, uncertain system.**

I. Introduction

Switched systems are a typical class of hybrid systems, which consist of a family of subsystems described by continuous or discrete-time dynamics, and a switching law that specifies the active subsystem at each time instant. Due to the multi-modal feature, switched systems can efficiently model practical systems that are inherently multi-modal, i.e., several dynamical subsystem models are required to describe their behaviors. So far, the research on switched systems has attracted significant attention and an extensive literature is by now available, for example in stability and stabilization [1]–[5], controllability and reachability analysis [6], $\mathcal{H}_\infty$ control and filtering [7]–[9].

Reachable set estimation aims to derive a closed bounded set that constrains all the state trajectories generated by a dynamic system with a prescribed initial state set and an input set. As its further extension, the output reachable set estimation is to derive a closed bounded set containing the set of all outputs of a system. Reachable set estimation problem is not only of theoretical interest in robust control theory [10], but also closely related to practical engineering for the safety verification problems [11]. In some early work, the reachable set bounding was considered in the context of state estimation and it has later received a lot of attention in parameter estimation, see [12] and references therein. Recently, many researchers have been interested in employing ellipsoidal techniques based on Lyapunov function approaches to estimate the reachable sets for different classes of systems. In the framework of bounding ellipsoid, the quadratic Lyapunov function has played a fundamental role in the reachable set estimation problem, and it has been further developed to time-delay systems [13]–[16], singular systems [17], discrete-time switched systems under arbitrary switching [18] and periodic switching [19]. However, according to the best of the authors' knowledge, the reachable set estimation for continuous-time switched systems with dwell-time restriction has not been fully investigated, and it therefore motivates our study.

In this paper, the contributions are two folds. First, we study the output reachable set estimation problem for continuous-time switched linear systems consisting of Hurwitz stable subsystems. In the arbitrary switching case, an over approximation of output reachable set is obtained as a union of a collection of bounding ellipsoids centered around origin and moreover, a linear matrix inequality (LMI) based optimization problem is formulated to obtain the smallest estimated reachable set. These results are all derived in the framework of a common Lyapunov function shared across modes, however, it may yield overly conservative results, especially when some information of switching laws is available. Thus, with regard to a class of time-dependent switching signal under dwell time constraint, a time-scheduled multiple Lyapunov function approach is further employed and preciser estimation results can be achieved. In particular, it is worth mentioning that this time-scheduled multiple Lyapunov function approach covers the common Lyapunov function approach. In some papers, e.g., [20], [21], the finite-time boundedness is used for bounding state trajectories of a system, but it focuses on a finite-time interval other than all time along the system operation. Furthermore, the estimation from initial time to infinity is necessary for some problems such as the bisimulation and safety verification in the second contribution in this paper.

Based on the results for output reachable set estimation and inspired by approximate bisimulation relations in [22]–[24], a sufficient condition is derived to establish the existence of approximate bisimulation of two switched linear systems. Then, since the safety verification for uncertain systems is

The material presented in this paper is based upon work supported by the National Science Foundation (NSF) under grant numbers CNS 1464311, EPCN 1509804, and SHF 1527398, the Air Force Research Laboratory (AFRL) through contract number FA8750-15-1-0105, and the Air Force Office of Scientific Research (AFOSR) under contract numbers FA9550-15-1-0258 and FA9550-16-1-0246.

Authors are with the Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, Tennessee 37212, USA. Emails: xiangwming@gmail.com; trhoangdung@gmail.com; taylor.johnson@gmail.com

difficult due to the uncertain time-varying coefficients in the system matrices, one would ask: *Can we find a bisimilar system with exact parameters for an uncertain system and perform a safety verification for the bisimilar system to ensure the safety of the uncertain system?* In this paper, an LMI-based method is proposed to convert the uncertain switched system into a switched system with exact parameters along with a precision between two systems, so that the safety verification for uncertain systems can be performed by verifying the safety of the transformed systems, avoiding the difficulties in handling the uncertainties.

The rest of this paper is organized as follows. Some preliminaries and problem formulation are given in Section II. The main results on output reachable set estimation is proposed in Section III. In Section IV, the application to safety verification for uncertain switched systems is presented. Conclusions are given in Section V.

Notation: $\mathbb{N}$ represents the set of natural numbers. $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ denote the fields of real numbers and nonnegative real numbers, respectively. $\mathbb{R}^n$ is the vector space of all n-tuples of real numbers, $\mathbb{R}^{n\times n}$ is the space of $n\times n$ matrices with real entries. $\mathbb{S}_+^{n\times n}$ is the set of real symmetric positive definite $n\times n$ matrices. The notation $P\succ 0$ ($P\prec 0$) means P is real symmetric and positive definite (negative definite). $A^\top$ denotes the transpose of A, and we let $\mathrm{Sym}(A)=A^\top+A$. In symmetric block matrices, we use * as an ellipsis for the terms that are introduced by symmetry. $\mathrm{diag}\{\cdots\}$ denotes a block-diagonal matrix. $\|\cdot\|$ stands for the Euclidean norm. The bounding ellipsoid is expressed by $\mathcal{E}(R)\triangleq\{x\in\mathbb{R}^n \mid x^\top Rx\leq 1, R\in\mathbb{S}_+^{n\times n}\}$, and ball $\mathcal{B}(x_0,\delta)\triangleq\{x\in\mathbb{R}^n \mid \|x-x_0\|\leq\delta, x_0\in\mathbb{R}^n,\delta>0\}$. The right derivative of a matrix function $F(x)$ is defined by $\dot F(x)\triangleq\lim_{h\to 0^+}\frac{F(x+h)-F(x)}{h}$. For the sake of simplicity, we denote $\mathscr{L}(A,B,P,R,\alpha)\triangleq\begin{bmatrix} A^\top P+PA+\alpha P & * \\ B^\top P & -\alpha R\end{bmatrix}$.

II. Switched Systems and Output Reachable Set

In this paper, we consider a continuous-time switched linear system in the form of

$$\Sigma:\ \dot x(t)=A_{\sigma(t)}x(t)+B_{\sigma(t)}u(t) \quad (1)$$
$$y(t)=C_{\sigma(t)}x(t) \quad (2)$$

where $x(t)\in\mathbb{R}^{n_x}$ are the state of the system, and the initial condition x_0 belongs to a bounded ellipsoid:

$$x_0\in\mathcal{X}_0\triangleq\mathcal{E}(R_0) \quad (3)$$

and $u(t)\in\mathbb{R}^{n_u}$ is the input vector which is assumed to satisfy the following ellipsoidal constraint:

$$u(t)\in\mathcal{U}\triangleq\mathcal{E}(R_u),\ \forall t\in\mathbb{R}_{\geq 0} \quad (4)$$

and $y(t)\in\mathbb{R}^{n_y}$ is the output. Define index set $\mathcal{M}\triangleq\{1,2,\ldots,N\}$, where N is the number of modes and, $\sigma:\mathbb{R}_{\geq 0}\to\mathcal{M}$ denotes the switching function, which is assumed to be a piecewise constant function continuous from right and only non-Zeno swtichings (i.e., the switch at most a finite number of times in any finite time interval) are considered in this paper. The switching instants are expressed by a sequence $\mathcal{S}\triangleq\{t_k\}_{k\in\mathbb{N}}$, where t_0 is the initial time and t_k is the kth switching instant. Then, we define $\mathcal{I}_i\triangleq\{t\in\mathbb{R}_{\geq 0}\mid\sigma(t)=i, i\in\mathcal{M}\}$ to denote the activation time interval for ith mode. Obviously, we can see that $\bigcup_{i\in\mathcal{M}}\mathcal{I}_i=\mathbb{R}_{\geq 0}$ and $\mathcal{I}_i\cap\mathcal{I}_j=\emptyset$, for $i\neq j$, $\forall i,j\in\mathcal{M}$.

The output reachable set of system (1)–(2) is defined as

$$\mathcal{R}_y\triangleq\{y(t)\in\mathbb{R}^{n_y}\mid x(t),y(t),x_0,u(t)\text{ satisfy } (1),(2),(3),(4),t\in\mathbb{R}_{\geq 0}\} \quad (5)$$

The following lemma introduces the main idea to determine the over-approximate set $\tilde{\mathcal{R}}_y$ for switched system (1)–(2).

Lemma 1: Consider system (1)–(2) under initial state condition (3) and input condition (4). If there exist a family of Lyapunov functions $V_i:\mathbb{R}^{n_x}\to\mathbb{R}_{\geq 0}$, $i\in\mathcal{M}$, satisfying $V_i(0)=0$ and $V_i(x)>0$, $\forall x\neq 0$, $\forall i\in\mathcal{M}$, matrices $R_{i,y}\in\mathbb{S}_+^{n\times n}$, $i\in\mathcal{M}$, and scalars $\alpha>0$, $0<\beta\leq 1$ such that

$$F_i(t)\leq 0,\ \forall t\in\mathcal{I}_i,\forall i\in\mathcal{M} \quad (6)$$
$$G_{i,j}(t_k)\leq 0,\ \forall t_k\in\mathcal{S}, i\neq j,\forall i,j\in\mathcal{M} \quad (7)$$
$$V_i(x_0)\leq x_0^\top R_0x_0,\ \forall i\in\mathcal{M} \quad (8)$$
$$x^\top(t)C_i^\top R_{i,y}C_ix(t)\leq V_i(x(t)),\ \forall t\in\mathcal{I}_i,\forall i\in\mathcal{M} \quad (9)$$

where $F_i(t)=\dot V_i(x(t))+\alpha V_i(x(t))-\alpha u^\top(t)R_uu(t)$ and $G_{i,j}(t_k)=V_i(x(t_k^+))-\beta V_j(x(t_k^-))+\beta-1$. Then, the output reachable set $\mathcal{R}_y$ satisfies $\mathcal{R}_y\subseteq\tilde{\mathcal{R}}_y\triangleq\bigcup_{i\in\mathcal{M}}\mathcal{E}(R_{i,y})$.

Proof: See the Appendix. ■

Remark 1: Conditions (6) and (7) actually characterize an invariant set $\Omega=\bigcup_{i\in\mathcal{M}}\Omega_i$, where $\Omega_i=\{x(t)\in\mathbb{R}^{n_x}\mid V_i(x(t))\leq 1\}$, $i\in\mathcal{M}$. By (6), it leads to $\dot V_i(x(t))<0$, $\forall x(t)\in\bar\Omega_i\triangleq\{x(t)\in\mathbb{R}^{n_x}\mid V_i(x(t))>1\}$, this guarantees that once the state $x(t)$ enters Ω_i, it remains in it during the activation time of the ith subsystem. However, (6) is not enough to ensure $x(t)$ staying in Ω forever, in presence of abrupt changes from $V_i(x(t_k^+))$ to $V_j(x(t_k^-))$, where $i\neq j$ at switching instant $t_k\in\mathcal{S}$. Thus, (7) is necessary to define the invariant Ω. It ensures that $V_i(x(t_k^+))\leq 1$ when $V_i(x(t_k^-))\leq 1$, that means the switching actions will not cause $x(t)$ escaping from Ω. In addition, (8) implies that the initial state $x_0\in\mathcal{X}_0\subseteq\bigcap_{i\in\mathcal{M}}\Omega_i$, and (9) estimates the output reachable set based on the invariant set Ω.

III. Output Reachable Set Estimation

Although Lemma 1 provides a general framework to handle the output reachable set estimation problem, it is impractical for actual use, since it does not provide any available computational techniques for the construction of Lyapunov functions $V_i(x(t))$, $i\in\mathcal{M}$. Moreover, the proposed condition (7) requires us to check the values of Lyapunov functions at all the switching instant $t_k\in\mathcal{S}$. However, the switching instant sequence $\mathcal{S}$ usually cannot be specified in advance, and it is impossible to check Lemma 1 for all the switching instants t_k in the case of $k\to\infty$. In the following, numerically tractable methods are presented to solve the output reachable set estimation problem in the framework of Lemma 1.

A. Common Lyapunov Function

One natural idea to analyze switched system (1)–(2) is to use common quadratic Lyapunov function $V_i(x(t)) = V(x(t)) = x^\top(t)Px(t)$, $i \in \mathcal{M}$, to avoid checking (7) for every $t_k \in \mathcal{S}$.

Theorem 1: Consider system (1)–(2) under initial state condition (3) and input condition (4). If there exist matrices $P \in \mathbb{S}_+^{n_x \times n_x}$, $R_{i,y} \in \mathbb{S}_+^{n \times n}$, $i \in \mathcal{M}$, and a scalar $\alpha > 0$ such that

$$\mathscr{L}(A_i, B_i, P, R_u, \alpha) \prec 0,\ \forall i \in \mathcal{M} \tag{10}$$

$$C_i^\top R_{i,y} C_i \prec P \prec R_0,\ \forall i \in \mathcal{M} \tag{11}$$

then, the output reachable set $\mathcal{R}_y \subseteq \tilde{\mathcal{R}}_y \triangleq \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y})$.

Proof: Construct a Lyapunov function in the form of $V(x(t)) = x^\top(t)Px(t)$, $P \in \mathbb{S}_+^{n\times n}$. Let us consider $F(t) = \dot{V}(x(t)) + \alpha V(x(t)) - \alpha u^\top(t)R_u u(t)$, and along with the trajectory of system (1)–(2), we have $F(t) = \chi^\top(t)\mathscr{L}(A_i, B_i, P, R_u, \alpha)\chi(t)$, where $\chi^\top(t) = [x^\top(t)\ \ u^\top(t)]$, and from (10), it yields $F(t) < 0$, $\forall t \in \mathbb{R}_{\geq 0}$, so that (6) holds.

Then, since the common Lyapunov function is chosen, (7) automatically holds with $\beta = 1$. By (11), $P \prec R_0$ ensures $V(x_0) < x_0^\top R_0 x_0$, and $C_i^\top R_{i,y} C_i \prec P$, $i \in \mathcal{M}$, guarantees $x^\top(t)C_i^\top R_{i,y} C_i x(t) < V(x(t))$, $\forall t \in \mathbb{R}_{\geq 0}$, $\forall i \in \mathcal{M}$, that is (8) and (9) hold. Thus, by Lemma 1, we have the output reachable set $\mathcal{R}_y \subseteq \tilde{\mathcal{R}}_y \triangleq \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y})$. ■

Remark 2: The set $\tilde{\mathcal{R}}_y$ is usually expected to be as small as possible to achieve a precise estimate of reachable set $\mathcal{R}_y$. Based on Theorem 1, one may add an additional constraint that

$$R_{i,y} \succeq \epsilon I,\ \epsilon > 0,\ \forall i \in \mathcal{M} \tag{12}$$

which implies that $\epsilon y^\top(t)y(t) \leq y^\top(t)R_{i,y}y(t) \leq 1$, namely $y(t) \in \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y}) \subseteq \mathcal{B}(0, 1/\sqrt{\epsilon})$, $\forall t \in \mathbb{R}_{\geq 0}$, so we have to maximize ϵ to obtain the smallest ball $\mathcal{B}(0, 1/\sqrt{\epsilon})$ by

$$\max\ \epsilon\ \text{ s.t. } (10),\ (11) \text{ and } (12) \tag{13}$$

Moreover, due to the existence of the tuning parameter α, the result in Theorem 1 and corresponding optimization problem (13) are not standard LMI problems, they are bilinear matrix inequality (BMI) problems and known to be NP-hard. Fortunately, several algorithms are available to solve BMI problems such as the iterative linear matrix inequality (ILMI) approach in [25], [26], or using numerical optimization algorithms, such as `fminsearch` [13] or genetic algorithm (GA) [18] in the optimization toolbox of Matlab.

B. Multiple Lyapunov Functions

Switching actions are able to significantly affect the evolution of switched systems, for example the instability arises as a result of a rapid switching between stable subsystems. Similarly, the switching rate has a great impact on the reachable set as well. Thus, given a switching rate, how to estimate the set $\mathcal{R}_y$ is one of the basic problems for reachable set estimation. In this work, the concept of minimum dwell time is given to constrain the switching rate.

Definition 1: [27] Given a switching signal function $\sigma(t)$ with a generated switching sequence $\mathcal{S}$, $\tau_{\min} = \inf_{k\in\mathbb{N}}\{t_{k+1} - t_k\}$ is called the dwell time of $\sigma(t)$, and $\mathcal{D}_{\tau_{\min}} \triangleq \{\sigma(t) \mid \sigma : \mathbb{R}_{\geq 0} \to \mathcal{M}, t_{k+1} - t_k \geq \tau_{\min}, \forall k \in \mathbb{N}\}$ denotes the set of all switching policies with dwell time greater than $\tau_{\min}$.

We consider a class of time-scheduled multiple Lyapunov functions inspired by [28]–[31] as follows:

$$V_i(x(t)) = x^\top(t)P_i(t)x(t),\ t \in \mathbb{R}_{\geq 0},\ i \in \mathcal{M} \tag{14}$$

where $P_i(t) \in \mathbb{S}_+^{n\times n}$, $i \in \mathcal{M}$ have the following structure:

Consider the interval $[t_k, t_k + \tau_{\min})$, we partition it into L segments described as $\mathcal{L}_{k,q} \triangleq [t_k + \theta_q, t_k + \theta_{q+1})$, $q = 0, 1, \ldots, L-1$ of equal lengths $h = \tau_{\min}/L$, and then $\theta_0 = 0$ and $\theta_q = qh = q\tau_{\min}/L$. We consider a class of continuous matrix function $P_i(t)$, $t \in [t_k, t_k + \tau_{\min})$ chosen to be linear within each segment $\mathcal{L}_{k,q}$, $q = 0, 1, \ldots, L-1$. Explicitly, we can see that $\bigcup_{n=0}^{L-1} \mathcal{L}_{k,n} = [t_k, t_k + \tau_{\min})$ and $\mathcal{L}_{k,n} \cap \mathcal{L}_{k,m} = \emptyset$, $n \neq m$. Letting $P_{i,q} = P_i(t_k + \theta_q)$, then since the matrix function $P_i(t)$ is piecewise linear in $[t_k, t_k + \tau_{\min})$, it can be expressed in terms of the values at dividing points using a linear interpolation formula, that is, for $0 \leq \mu \leq 1$, $q = 0, 1, \ldots, L-1$,

$$P_i(t) = P_i(\mu) = (1-\mu)P_{i,q} + \mu P_{i,q+1},\ t \in \mathcal{L}_{k,q},\ i \in \mathcal{M} \tag{15}$$

where $\mu = L(t - t_k - \theta_q)/\tau_{\min}$.

As a result, the continuous matrix function $P_i(t) \in \mathbb{S}_+^{n\times n}$, $i \in \mathcal{M}$ can be completely determined by $P_{i,q} \in \mathbb{S}_+^{n\times n}$, $q = 0, 1, \ldots, L$, $i \in \mathcal{M}$, in interval $[t_k, t_k + \tau_{\min})$. Then, due to $[t_k, t_k + \tau_{\min}) \subseteq [t_k, t_{k+1})$, for the remaining time in $[t_k, t_{k+1})$ denoted by $\mathcal{L}_{k,L} \triangleq [t_{k,\min}, t_{k+1})$, $P_i(t)$, $i \in \mathcal{M}$ is set to be

$$P_i(t) = P_{i,L},\ t \in \mathcal{L}_{k,L},\ i \in \mathcal{M} \tag{16}$$

In summary, $P_i(t)$, $i \in \mathcal{M}$ is defined as

$$P_i(t) = \begin{cases} P_i(\mu), & t \in \mathcal{L}_{k,q},\ q = 0, 1, \ldots, L-1 \\ P_{i,L}, & t \in \mathcal{L}_{k,L} \end{cases} \tag{17}$$

where μ is defined in (15).

Theorem 2: Given a dwell time $\tau_{\min} > 0$ and consider switched system (1)–(2) with $\sigma(t) \in \mathcal{D}_{\tau_{\min}}$ under initial state condition (3) and input condition (4). If there exist matrices $P_{i,q} \in \mathbb{S}_+^{n_x\times n_x}$, $q = 0, 1, \ldots, L$, $i \in \mathcal{M}$, $R_{i,y} \in \mathbb{S}_+^{n\times n}$, $i \in \mathcal{M}$, and a scalar $\alpha > 0$ such that for $\forall i, j \in \mathcal{M}$

$$\mathscr{L}(A_i, B_i, P_{i,q}, R_u, \alpha) + \Psi_{i,q} \prec 0,\ q = 0, \ldots, L-1 \tag{18}$$

$$\mathscr{L}(A_i, B_i, P_{i,q+1}, R_u, \alpha) + \Psi_{i,q} \prec 0,\ q = 0, \ldots, L-1 \tag{19}$$

$$\mathscr{L}(A_i, B_i, P_{i,L}, R_u, \alpha) \prec 0 \tag{20}$$

$$P_{i,0} - P_{j,L} \prec 0,\ i \neq j \tag{21}$$

$$P_{i,0} - R_0 \prec 0 \tag{22}$$

$$C_i^\top R_{i,y} C_i - P_{i,q} \prec 0,\ q = 0, \ldots, L \tag{23}$$

where $\Psi_{i,q} = \operatorname{diag}\{L(P_{i,q+1} - P_{i,q})/\tau_{\min}, 0\}$. Then, the output reachable set $\mathcal{R}_y \subseteq \tilde{\mathcal{R}}_y \triangleq \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y})$.

Proof: Construct a Lyapunov function as $V(t) = \sum_{i\in\mathcal{M}} \xi_i(t)x^\top(t)P_i(t)x(t)$, where $P_i(t)$, $i \in \mathcal{M}$, is defined by (17) and $\xi_i : \mathbb{R}_{\geq 0} \to \{0, 1\}$ and $\sum_{i\in\mathcal{M}} \xi_i(t) = 1$ is the indicator function representing the active modes at time t.

TABLE I
COMPUTATIONAL COMPLEXITIES OF THEOREM 2 WITH A FIXED α

Number of Decision Variables	LMI Constraints Size
$nN(L+1)(n+1)/2$	$n(N^2+2N+3L)$

First, let us consider $F_i(t) = \dot{V}(t)+\alpha V(t)-\alpha u^\top(t)R_u u(t)$, which can be rewritten to

$$F_i(t) = \chi^\top(t)(\mathscr{L}(A_i, B_i, P_i(t), R_u, \alpha) + \Psi_i(t))\chi(t) \quad (24)$$

where $\chi^\top(t) = [x^\top(t) \;\; u^\top(t)]$ and $\Psi_i(t) = \mathrm{diag}\{\dot{P}_i(t), 0\}$.

Suppose $\sigma(t) = i$, $t \in \mathcal{L}_{k,q}$, $q = 0, \dots, L-1$, one has

$$\mathscr{L}(A_i, B_i, P_i(t), R_u, \alpha) = (1-\mu)\Xi_{i,1} + \mu\Xi_{i,2} \quad (25)$$

where $\Xi_{i,1} = \mathscr{L}(A_i, B_i, P_{i,q}, R_u, \alpha)$ and $\Xi_{i,2} = \mathscr{L}(A_i, B_i, P_{i,q+1}, R_u, \alpha)$. Furthermore, we can see that $\dot{P}_i(t) = (P_{i,q+1} - P_{i,q})\dot{\mu}$, $t \in \mathcal{L}_{k,q}$, $q = 0, \dots, L-1$, and because of $\mu = L(t-t_k-\theta_q)/\tau_{\min}$, it implies that $\dot{\mu} = L/\tau_{\min}$, leading to $\dot{P}_i(t) = \Psi_{i,q}$, $t \in \mathcal{L}_{k,q}$, $q = 0, \dots, L-1$. Thus, by (18), (19), it leads to

$$F_i(t) < 0, \;\forall t \in \bigcup_{n=0}^{L-1} \mathcal{L}_{k,n} = [t_k, t_k + \tau_{\min}) \quad (26)$$

Then, we consider $t \in \mathcal{L}_{k,L}$. Since $P_i(t) = P_{i,L}$, $t \in \mathcal{L}_{k,L}$, we have $P_i(t) = 0$, $\forall t \in \mathcal{L}_{k,L}$, thus (20) guarantees that

$$F_i(t) < 0, \;\forall t \in \mathcal{L}_{k,L} \quad (27)$$

Thus, from (26) and (27), we can conclude that $F_i(t) < 0$, $\forall t \in \mathcal{I}_i$, $\forall i \in \mathcal{M}$, which means (6) in Lemma 1 holds. Next, (21) ensures (7) holds with $\beta = 1$ and (22) guarantees (8) holds Finally, we consider

$$\begin{aligned} &C_i^\top R_{i,y} C_i - P_i(t) \\ =&(1-\mu)(C_i^\top R_{i,y} C_i - P_{i,q}) + \mu(C_i^\top R_{i,y} C_i - P_{i,q+1}) \end{aligned}$$

and (23) ensures that $C_i^\top R_{i,y} C_i - P_i(t) < 0$, $\forall t \in \mathbb{R}_{\geq 0}$, $\forall i \in \mathcal{M}$, which implies (9) holds. Therefore, we have the output reachable set $\mathcal{R}_y \subseteq \tilde{\mathcal{R}}_y \triangleq \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y})$ by Lemma 1. ■

Remark 3: Some remarks on parameter L are given.

(1) Parameter L implies the number of segments consisting of the dwell time interval $[t_k, t_k + \tau_{\min})$. A larger L yields a finer division of $[t_k, t_k + \tau_{\min})$, and a less conservative result can be consequently obtained, which will be demonstrated by a numerical example later. However, the computational cost increases as L grows, since a larger L inevitably introduces more decision variables and LMI constraints, see TABLE I for the computational complexity analysis for Theorem 2 for an n-dimensional switched system consisting of N modes.

(2) Similar as the methods adopted in [20], a piecewise matrix function $P_i(\mu)$ in (15) with a sufficiently large L is able to approximate a generic continuously differentiable $P_i(t)$ with adequate accuracy over the finite-time interval $[t_k, t_k + \tau_{\min})$. In other words, if $L \to \infty$, conditions (18)–(23) in Theorem 2 can be expressed as follows with $i, j \in \mathcal{M}$ and $t \in [0, \tau_{\min})$

$$P_i(t) \succ 0 \quad (28)$$
$$\mathscr{L}(A_i, B_i, P_i(t), R_u, \alpha) + \Psi_i(t) \prec 0 \quad (29)$$
$$\mathscr{L}(A_i, B_i, P_i(\tau_{\min}), R_u, \alpha) \prec 0 \quad (30)$$
$$P_i(0) - P_j(\tau_{\min}) \prec 0, \; i \neq j \quad (31)$$
$$P_i(0) - R_0 \prec 0 \quad (32)$$
$$C_i^\top R_{i,y} C_i - P_i(t) \prec 0 \quad (33)$$

where $\Psi_i(t) = \mathrm{diag}\{\dot{P}_i(t), 0\}$. It should be noted that the above differential linear matrix inequality (DLMI) (28)–(33) can achieve the result with least conservativeness in our framework, but it is not numerically tractable due to the presence of continuous matrix functions $P_i(t)$.

(3) In another extreme case with $L = 0$, $P_{i,q}$, shrinks to P_i, moreover, due to (21), we have to choose $P_i = P_j$, $i \neq j$. Thus, Theorem 2 is reduced to Theorem 1, namely the common Lyapunov function result.

Given an L, the smallest ball $\mathcal{B}(0, 1/\sqrt{\epsilon})$ containing the trajectories of output $y(t)$ in the framework of our approach can be obtained. Based on Theorem 2, an optimization problem can be formulated by adding (12) with (18)–(23) as follows:

$$\max \; \epsilon \;\; \text{s.t. (12) and (18)} - \text{(23)} \quad (34)$$

C. Example

Consider a switched system with two subsystems as

$$\begin{bmatrix} A_1 \\ \hdashline B_1^\top \\ \hdashline C_1 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ 0 & -0.9 \\ \hdashline 3 & 1 \\ \hdashline 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} A_2 \\ \hdashline B_2^\top \\ \hdashline C_2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ -1 & -1 \\ \hdashline 2 & 3 \\ \hdashline 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The initial state is assumed to satisfy $x_0 \in \{x_0 \in \mathbb{R}^2 \mid \|x_0\| \leq 1\}$ and the input is assumed to satisfy $u(t) \in \{u(t) \in \mathbb{R} \mid -1 \leq u(t) \leq 1, \; \forall t \in \mathbb{R}_{\geq 0}\}$, which implies that $R_0 = \mathrm{diag}\{1, 1\}$ and $R_u = 1$.

First, we use Theorem 1 to estimate the reachable set $\tilde{\mathcal{R}}_y$ contained in the ball $\mathcal{B}(0, \delta)$ with the minimal δ, where $\delta = 1/\sqrt{\epsilon}$. The minimal δ is 2.9033 obtained by solving optimization (13) with the aid of `fminsearch`. It should be noted that this result is applicable for the arbitrary switching, since the common Lyapunov function approach is employed.

Next, if the dwell-time constraint is further considered in the switching signal, we can apply Theorem 2. Suppose dwell time $\tau_{\min} = 1$, we solve optimization problem (34) to obtain the minimal δ with $L = 1, 2, \dots, 10$, which are depicted in Fig. 1. The following two points can be observed in Fig. 1, which are consistent with Remark 3.

1) The value of δ monotonically decreases as L increases. This means that a less conservative result, namely a smaller δ, can be obtained, if a greater L is chosen.
2) The $L = 0$ is equivalent to the result of common Lyapunov function approach, but it is more restrictive than the result obtained by the multiple Lyapunov function approach with $L \geq 1$.

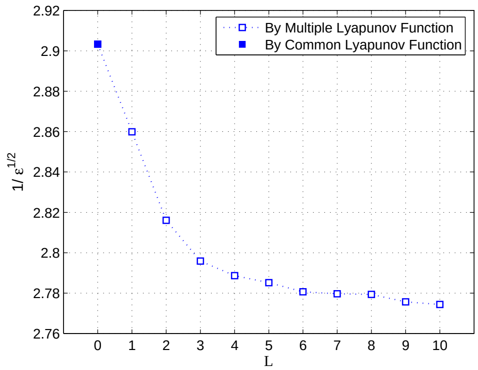

Fig. 1. Minimized $\delta = 1/\sqrt{\epsilon}$ by the common Lyapunov function approach (Theorem 1) and the multiple Lyapunov function approach (Theorem 2) with respect to $L = 0, 1, 2, \ldots, 10$.

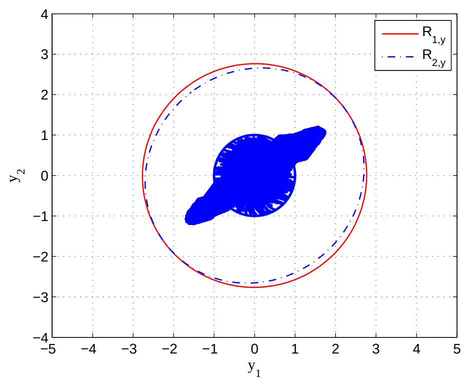

Fig. 2. 1000 randomly generated state trajectories are bounded in the estimated output reachable set $\tilde{\mathcal{R}}_y = \mathcal{R}_{1,y} \cup \mathcal{R}_{2,y}$.

Finally, the bounding ellipsoids $\mathcal{R}_{1,y}$ and $\mathcal{R}_{2,y}$ obtained with $L = 10$ are shown in Fig. 2. The switching signal has $t_{k+1} - t_k = 1 + \mathrm{rand}$, $k \in \mathbb{N}$, where rand is a random number within $[0, 1]$, thus the switching signal $\sigma(t) \in D_{\tau_{\min}}$ with $\tau_{\min} = 1$. With an input $u(t) = \sin(t)$, 1000 state trajectories generated from 1000 random initial states from a unit circle are illustrated in Fig. 2. As Fig. 2 shows, all the state trajectories are bounded in the estimated reachable set $\tilde{\mathcal{R}}_y = \mathcal{R}_{1,y} \cup \mathcal{R}_{2,y}$, showing the effectiveness of our approach.

IV. Safety Verification for Uncertain Switched System

For the sake of being concise, we focus on the application of Theorem 2 in the rest of this paper, since Theorem 1 is just a special case of Theorem 2 with parameter $L = 0$, see point (3) in Remark 3.

A. *Approximate Bisimulation*

For a continuous-time switched linear system Σ described by (1)–(2), an approximately bisimilar continuous-time switched linear system $\tilde{\Sigma}$ is considered in the following form

$$\tilde{\Sigma}: \ \dot{\tilde{x}}(t) = \tilde{A}_{\sigma(t)}\tilde{x}(t) + \tilde{B}_{\sigma(t)}u(t) \tag{35}$$

$$\tilde{y}(t) = \tilde{C}_{\sigma(t)}\tilde{x}(t) \tag{36}$$

where $\tilde{x}(t) \in \mathbb{R}^{\tilde{n}_x}$ is the state of the bisimilar system, the initial state $\tilde{x}_0$ is assumed to be in

$$\tilde{x}_0 \in \tilde{\mathcal{X}}_0 \triangleq \mathcal{E}(\tilde{R}_0) \tag{37}$$

and $\tilde{y}(t) \in \mathbb{R}^{n_y}$ is the output of the bisimilar system. In the rest of the work, the input $u(t)$ and switching signal $\sigma(t)$ of $\tilde{\Sigma}$ is considered to be same as those for system Σ.

Definition 2: [22] A relation $\mathscr{R}_\delta \subseteq \mathbb{R}^{n_x} \times \mathbb{R}^{\tilde{n}_x}$ is called a δ-approximate bisimulation relation between systems Σ and $\tilde{\Sigma}$, of precision δ, if for all $(x(t), \tilde{x}(t)) \in \mathscr{R}_\delta$

1) $\|y(t) - \tilde{y}(t)\| \le \delta$, $\forall t \in \mathbb{R}_{\ge 0}$,
2) $\forall u(t) \in \mathcal{U}$, $\forall x(t)$ satisfies Σ, $\exists \tilde{x}(t)$ satisfies $\tilde{\Sigma}$ such that $(x(t), \tilde{x}(t)) \in \mathscr{R}_\delta$, $\forall t \in \mathbb{R}_{\ge 0}$,
3) $\forall u(t) \in \mathcal{U}$, $\forall \tilde{x}(t)$ satisfies $\tilde{\Sigma}$, $\exists x(t)$ satisfies Σ such that $(x(t), \tilde{x}(t)) \in \mathscr{R}_\delta$, $\forall t \in \mathbb{R}_{\ge 0}$.

and we say systems Σ and $\tilde{\Sigma}$ are approximately bisimilar with precision δ, denoted by $\Sigma \sim_\delta \tilde{\Sigma}$.

Define the following notations $\hat{x}(t) = [x^\top(t) \ \tilde{x}^\top(t)]^\top$, $\hat{y}(t) = y(t) - \tilde{y}(t)$ and

$$\left[\begin{array}{c:c:c} \hat{A}_i & \hat{B}_i & \hat{C}_i^\top \end{array}\right] = \left[\begin{array}{cc:c:c} A_i & 0 & B_i & C_i^\top \\ 0 & \tilde{A}_i & \tilde{B}_i & -\tilde{C}_i^\top \end{array}\right]$$

and let $0 \le \gamma \le 1$, we define $\hat{R}_0(\gamma) = \mathrm{diag}\{\gamma R_0, (1-\gamma)\tilde{R}_0\}$.

Since Σ and $\tilde{\Sigma}$ share same switching signal $\sigma(t)$ and input $u(t)$, an augmented system $\hat{\Sigma}$ can be derived from Σ and $\tilde{\Sigma}$ as below

$$\hat{\Sigma}: \ \dot{\hat{x}}(t) = \hat{A}_{\sigma(t)}\hat{x}(t) + \hat{B}_{\sigma(t)}u(t) \tag{38}$$

$$\hat{y}(t) = \hat{C}_{\sigma(t)}\hat{x}(t) \tag{39}$$

with initial state $\hat{x}_0 \in \hat{\mathcal{X}}_0 \triangleq \mathcal{E}(\hat{R}_0(\gamma))$ and input $u(t) \in \mathcal{U} \triangleq \mathcal{E}(R_u)$.

Because $\|y(t) - \tilde{y}(t)\| \le \delta$, $\forall t \in \mathbb{R}_{\ge 0}$ holds if and only if $\hat{y}(t) \in \mathcal{B}(0, \delta)$, $\forall t \in \mathbb{R}_{\ge 0}$, the problem of computing the distance δ between Σ and $\tilde{\Sigma}$ can be converted to the problem of output reachable set estimation for augmented system $\hat{\Sigma}$.

Theorem 3: Given a dwell time $\tau_{\min} > 0$ and consider switched systems Σ by (1)–(2) and $\tilde{\Sigma}$ by (35)–(36) with $\sigma(t) \in \mathcal{D}_{\tau_{\min}}$ under initial state condition (3), (37) and input condition (4). If there exist a set of matrices $P_{i,q} \in \mathbb{S}_+^{(n_x+\tilde{n}_x)\times(n_x+\tilde{n}_x)}$, $q = 0, 1, \ldots, L$, $i \in \mathcal{M}$ and scalars $\alpha > 0$, $0 \le \gamma \le 1$, $\epsilon \ge 0$ such that for $\forall i, j \in \mathcal{M}$

$$\mathscr{L}(\hat{A}_i, \hat{B}_i, P_{i,q}, R_u, \alpha) + \Psi_{i,q} \prec 0, \ q = 0, \ldots, L-1 \tag{40}$$

$$\mathscr{L}(\hat{A}_i, \hat{B}_i, P_{i,q+1}, R_u, \alpha) + \Psi_{i,q} \prec 0, \ q = 0, \ldots, L-1 \tag{41}$$

$$\mathscr{L}(\hat{A}_i, \hat{B}_i, P_{i,L}, R_u, \alpha) \prec 0 \tag{42}$$

$$P_{i,0} - P_{j,L} \prec 0, \ i \neq j \tag{43}$$

$$P_{i,0} - \hat{R}_0(\gamma) \prec 0 \tag{44}$$

$$\epsilon \hat{C}_i^\top \hat{C}_i - P_{i,q} \prec 0, \ q = 0, \ldots, L \tag{45}$$

where $\Psi_{i,q} = \mathrm{diag}\{L(P_{i,q+1} - P_{i,q})/\tau_{\min}, 0\}$. Then, we have an approximation bisimulation relation $\mathscr{R}_\delta$, $\delta = 1/\sqrt{\epsilon}$ such that $\Sigma \sim_\delta \tilde{\Sigma}$.

Proof: Since the initial states $x_0 \in \mathcal{E}(R_0)$ and $\tilde{x}_0 \in \mathcal{E}(\tilde{R}_0)$, the initial state $\hat{x}_0$ satisfies

$$\hat{x}_0^\top \hat{R}_0(\gamma)\hat{x}_0 = \gamma x_0^\top R_0 x_0 + (1-\gamma)\tilde{x}_0^\top \tilde{R}_0 \tilde{x}_0 \le 1, \ 0 \le \gamma \le 1 \tag{46}$$

Thus, it means that $\hat{x}_0 \in \mathcal{E}(\hat{R}_0(\gamma))$, $0 \le \gamma \le 1$.

From Theorem 2, it implies that the output reachable set of $\hat{\Sigma}$ can be estimated by $\bigcup_{i\in\mathcal{M}} \mathcal{E}(\epsilon I) = \mathcal{B}(0,\delta)$, where $\delta = 1/\sqrt{\epsilon}$, so the output $\hat{y}(t) \in \mathcal{B}(0,\delta)$, $\forall t \in \mathbb{R}_{\ge 0}$. Furthermore, due to $\hat{y}(t) = y(t) - \tilde{y}(t)$, we have $\|y(t) - \tilde{y}(t)\| \le \delta$, $\forall t \in \mathbb{R}_{\ge 0}$, along with the trajectories $x(t)$, $\tilde{x}(t)$ generated by Σ and $\tilde{\Sigma}$. The approximation bisimulation relation $\mathscr{R}_\delta$ such that $\Sigma \sim_\delta \tilde{\Sigma}$ can be established. ■

The choice of a larger L in Theorem 3 will lead to a less conservative analysis result, the result with the least conservativeness can be deduced by letting $L \to \infty$, which is however numerically intractable. For the particular case with $L = 0$, Theorem 3 is reduced to a result by the common Lyapunov function approach, but it can be used for the arbitrary switching case.

B. Safety Verification

We consider the system matrices of switched system Σ are uncertain and satisfy that $[A_i \;\; B_i \;\; C_i^\top] \in \mathfrak{R}_i$, where

$$\mathfrak{R}_i \triangleq \mathbf{co}\left\{[A_i^{(1)} \; B_i^{(1)} \; (C_i^{(1)})^\top], \ldots, [A_i^{(S)} \; B_i^{(S)} \; (C_i^{(S)})^\top]\right\} \tag{47}$$

where $\mathbf{co}\{\cdot\}$ is the convex-hull operator.

Definition 3: Consider system Σ described by (1)–(2) and (47) with $C_i^{(s)} = I$, $\forall s = 1, \ldots, S, \forall i \in \mathcal{M}$. System Σ is said to be safe with respect to the unsafe region Ω_u, if $\mathcal{R}_y \cap \Omega_u = \emptyset$.

Let $\tilde{\Sigma}$ be an approximately bisimilar system such that $\Sigma \sim_\delta \tilde{\Sigma}$. Denote $\mathcal{R}_y$, $\mathcal{R}_{\tilde{y}}$ the output reachable sets of Σ and $\tilde{\Sigma}$ respectively, then it can be seen that $\mathcal{R}_y \subseteq \mathcal{N}(\mathcal{R}_{\tilde{y}}, \delta)$, where $\mathcal{N}(\cdot, \delta)$ denotes the δ-neighborhood of a set. Consequently, to prove that Σ is safe, it is sufficient to verify that $\mathcal{R}_{\tilde{y}} \cap \mathcal{N}(\Omega_u, \delta) = \emptyset$.

Proposition 1: If $\Sigma \sim_\delta \tilde{\Sigma}$, then $\mathcal{R}_{\tilde{y}} \cap \mathcal{N}(\Omega_u, \delta) = \emptyset \Rightarrow \mathcal{R}_y \cap \Omega_u = \emptyset$. Namely, $\tilde{\Sigma}$ is safe with respect to $\mathcal{N}(\Omega_u, \delta) \Rightarrow \Sigma$ is safe with respect to Ω_u.

In the following, a theorem is presented to compute the system matrices for a bisimilar system for uncertain switched system Σ.

Theorem 4: Given a dwell time $\tau_{\min} > 0$ and consider uncertain switched systems Σ by (1)–(2), (47) and $\tilde{\Sigma}$ by (35)–(36) with $\sigma(t) \in \mathcal{D}_{\tau_{\min}}$ under initial state condition (3), (37) and input condition (4). If there exist a set of matrices $M_i \in \mathbb{R}^{n_x \times n_x}$, $N_i \in \mathbb{R}^{n_x \times n_u}$, $X_i \in \mathbb{R}^{n_x \times n_x}$, $Y_i \in \mathbb{R}^{n_x \times n_x}$, $Z_i \in \mathbb{R}^{n_x \times n_x}$, $S_i \in \mathbb{R}^{n_y \times n_x}$, $P_{i,q} \in \mathbb{S}_+^{2n_x \times 2n_x}$, $q = 0, 1, \ldots, L$, $i \in \mathcal{M}$ and scalars $\alpha > 0$, $0 \le \gamma \le 1$, $\delta \ge 0$ such that for $\forall i, j \in \mathcal{M}$ and $\forall s = 1, 2, \ldots, S$,

$$\Xi_{i,q,1}^{(s)} \prec 0, \; q = 0, \ldots, L-1 \tag{48}$$

$$\Xi_{i,q,2}^{(s)} \prec 0, \; q = 0, \ldots, L-1 \tag{49}$$

$$\Xi_{i,L}^{(s)} \prec 0 \tag{50}$$

$$P_{i,0} - P_{j,L} \prec 0, \; i \ne j \tag{51}$$

$$P_{i,0} - \hat{R}_0(\gamma) \prec 0 \tag{52}$$

$$\begin{bmatrix} -P_{i,q} & * \\ W_i^{(s)} & -\delta^2 I \end{bmatrix} \prec 0, \; q = 0, \ldots, L \tag{53}$$

where $\hat{R}_0(\gamma) = \mathrm{diag}\{\gamma R_0, (1-\gamma) R_0\}$, and

$$\Xi_{i,q,1}^{(s)} = \begin{bmatrix} -\mathrm{Sym}(U_i^{(s)}) + \alpha P_{i,q} + \Psi_{i,q} & * & * \\ -(V_i^{(s)})^\top & -\alpha R_u & * \\ P_{i,q} + Q_i - (U_i^{(s)})^\top & -V_i^{(s)} & \mathrm{Sym}(Q_i) \end{bmatrix}$$

$$\Xi_{i,q,2}^{(s)} = \begin{bmatrix} -\mathrm{Sym}(U_i^{(s)}) + \alpha P_{i,q+1} + \Psi_{i,q} & * & * \\ -(V_i^{(s)})^\top & -\alpha R_u & * \\ P_{i,q+1} + Q_i - (U_i^{(s)})^\top & -V_i^{(s)} & \mathrm{Sym}(Q_i) \end{bmatrix}$$

$$\Psi_{i,q} = L(P_{i,q+1} - P_{i,q})/\tau_{\min}$$

$$\Xi_{i,L}^{(s)} = \begin{bmatrix} -\mathrm{Sym}(U_i^{(s)}) + \alpha P_{i,L} & * & * \\ -(V_i^{(s)})^\top & -\alpha R_u & * \\ P_{i,L} + Q_i - (U_i^{(s)})^\top & -V_i^{(s)} & \mathrm{Sym}(Q_i) \end{bmatrix}$$

$$U_i^{(s)} = \begin{bmatrix} X_i A_i^{(s)} & M_i \\ Z_i A_i^{(s)} & M_i \end{bmatrix}, \; V_i^{(s)} = \begin{bmatrix} X_i B_i^{(s)} + N_i \\ Z_i B_i^{(s)} + N_i \end{bmatrix}$$

$$W_i^{(s)} = \begin{bmatrix} C_i^{(s)} & -S_i^\top \end{bmatrix}, \; Q_i = \begin{bmatrix} X_i & Y_i \\ Z_i & Y_i \end{bmatrix}$$

Then, we can obtain an approximately bisimilar system $\tilde{\Sigma}$ in the form of (35)–(36) and an approximation bisimulation relation $\mathscr{R}_\delta$ such that $\Sigma \sim_\delta \tilde{\Sigma}$, where the corresponding system matrices are

$$\begin{bmatrix} \tilde{A}_i \;\vdots\; \tilde{B}_i \;\vdots\; \tilde{C}_i^\top \end{bmatrix} = \begin{bmatrix} Y_i^{-1} M_i \;\vdots\; Y_i^{-1} N_i \;\vdots\; S_i^\top \end{bmatrix} \tag{54}$$

Proof: First, $Q_i + Q_i^\top \prec 0$ implies $Y_i + Y_i^\top \prec 0$, thus Y_i is nonsingular. Then, substituting $M_i = \tilde{A}_i Y_i$, $N_i = \tilde{B}_i Y_i$ and $S_i = \tilde{C}_i$ into (48), it becomes

$$\begin{bmatrix} -\mathrm{Sym}(Q_i \hat{A}_i^{(s)}) + \alpha P_{i,q} + \Psi_{i,q} & * & * \\ -(\hat{B}_i^{(s)})^\top Q_i^\top & -\alpha R_u & * \\ P_{i,q} + Q_i - (\hat{A}_i^{(s)})^\top Q_i^\top & -Q_i \hat{B}_i^{(s)} & Q_i + Q_i^\top \end{bmatrix} \prec 0$$

By left-multiplying the third row of above inequality by $(\hat{A}_i^{(s)})^\top$ or $(\hat{B}_i^{(s)})^\top$ and adding it to the first or second row, and right-multiplying the third column by $\hat{A}_i^{(s)}$ or $\hat{B}_i^{(s)}$ and adding it to the first or second column, it yields

$$\begin{bmatrix} \mathrm{Sym}(P_{i,q} \hat{A}_i^{(s)}) + \alpha P_{i,q} + \Psi_{i,q} & * & * \\ (\hat{B}_i^{(s)})^\top P_{i,q} & -\alpha R_u & * \\ P_{i,q} + Q_i^\top - Q_i \hat{A}_i^{(s)} & -Q_i \hat{B}_i^{(s)} & Q_i + Q_i^\top \end{bmatrix} \prec 0$$

Due to (47) and simple convexity arguments, the above inequality ensures (40) holds. Through a similar proof, it can be found that (49) $\Rightarrow$ (41) and (50) $\Rightarrow$ (42). Moreover, (51) and (52) are equivalent to (43) and (44).

Finally, letting $\epsilon = 1/\delta^2$ and by Schur complement, (53) ensures that (45) holds. Therefore, the approximation bisimulation $\Sigma \sim_\delta \tilde{\Sigma}$ can be established by Theorem 3. ■

Given an L, the optimized approximately bisimilar system $\tilde{\Sigma}_{\mathrm{opt}}$ can be obtained by minimizing the precision δ by

$$\min \;\; \delta^2 \;\; \text{s.t.} \; (48) - (53) \tag{55}$$

So far, according to Proposition 1, we can perform the safety verification for uncertain system Σ with respect to Ω_u via verifying the safety specification of the bisimilar system $\tilde{\Sigma}$ with respect to the set $\mathcal{N}(\Omega_u, \delta)$, the δ-neighborhood of Ω_u.

TABLE II
PRECISION δ WITH $L = 1, 2, 3, 4, 5$ AND COMPUTATION TIME (C.T.) WITH A FIXED α

	$L = 1$	$L = 2$	$L = 3$	$L = 4$	$L = 5$
δ	0.459	0.434	0.425	0.414	0.409
C. T.	0.573 s	0.862 s	1.221 s	4.762 s	15.263 s

C. Example

In this subsection, the safety verification for an uncertain switched affine system $\dot{x}(t) = A_i(t)x + b_i$, $i \in \{1, 2\}$, is considered. The system matrices are given as blow:

$$\begin{bmatrix} A_1 \\ \hdashline b_1^\top \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ \gamma(t) & -0.9 \\ \hdashline 3 & 1 \end{bmatrix}, \quad \begin{bmatrix} A_2 \\ \hdashline b_2^\top \end{bmatrix} = \begin{bmatrix} -1 & \gamma(t) \\ -1 & -1 \\ \hdashline 2 & 3 \end{bmatrix}$$

where $\gamma(t) \in [0, 0.1]$ is an uncertain time-varying parameter. The initial state is assumed to be $x_0 \in \{x_0 \in \mathbb{R}^2 \mid \|x_0\| \leq 0.1\}$, which implies that $R_0 = \mathrm{diag}\{100, 100\}$. The switching signal is a periodic switching law as $t_{k+1} - t_k = 1$, $\forall k \in \mathbb{N}$.

Using Theorem 4, a switched system with exact parameters can be obtained, with a corresponding precision δ. One point needs to be clarified here is that (50) can be removed for this particular periodic switching case, since (50) exactly corresponds to the interval $[t_k + \tau_{\min}, \infty)$ which does not appear at all. Similar to the experimental results for reachable set estimation (Section III, C), the precision δ tends to a smaller value as a larger L is chosen to apply Theorem 4, see TABLE II for $L = 1, 2, 3, 4, 5$.

Then, in order to validate our approach, we first let $L = 1$ and obtain the corresponding system matrices as follows:

$$\begin{bmatrix} A_1 \\ \hdashline b_1^\top \\ \hdashline C_1 \end{bmatrix} = \begin{bmatrix} -1.520 & 0.383 \\ 0.152 & -1.115 \\ \hdashline -2.895 & -1.087 \\ \hdashline -0.969 & -0.036 \\ -0.0355 & -0.9413 \end{bmatrix}, \begin{bmatrix} A_2 \\ \hdashline b_2^\top \\ \hdashline C_2 \end{bmatrix} = \begin{bmatrix} -0.858 & -0.091 \\ -0.508 & -1.560 \\ \hdashline -2.043 & -3.112 \\ \hdashline -0.969 & -0.036 \\ -0.036 & -0.941 \end{bmatrix}$$

With the above switched system with exact parameters, we can conduct the verification for the uncertain switched system. Given three unsafe regions $\Omega_{u,1} \triangleq \mathcal{B}([0.7\ 1.7], 0.6)$, $\Omega_{u,2} \triangleq \mathcal{B}([2\ \ -0.2], 0.5)$ and $\Omega_{u,3} \triangleq \mathcal{B}([3.5\ 1.5], 0.9)$, the new unsafe regions are described by their neighborhoods $\tilde{\Omega}_{u,1} \triangleq \mathcal{N}(\Omega_{u,1}, 0.459)$, $\tilde{\Omega}_{u,2} \triangleq \mathcal{N}(\Omega_{u,2}, 0.459)$ and $\tilde{\Omega}_{u,3} \triangleq \mathcal{N}(\Omega_{u,3}, 0.459)$. Thus, the verification for uncertain switched system can be done via verifying if the new system is safe with respect to the new unsafe regions. We can use SpaceEx [32] to perform the verification for the certain system.

The verification result is illustrated in Fig. 3. However, the safety of the original system cannot be guaranteed since the computed reach set intersects with $\tilde{\Omega}_{u,3}$. Then, we let $L = 5$ which produces a smaller precision δ, and the system matrices are

$$\begin{bmatrix} A_1 \\ \hdashline b_1^\top \\ \hdashline C_1 \end{bmatrix} = \begin{bmatrix} -1.611 & 0.427 \\ 0.170 & -1.106 \\ \hdashline -2.981 & -1.030 \\ \hdashline -0.970 & -0.032 \\ -0.032 & -0.948 \end{bmatrix}, \begin{bmatrix} A_2 \\ \hdashline b_2^\top \\ \hdashline C_2 \end{bmatrix} = \begin{bmatrix} -0.909 & -0.023 \\ -0.359 & -1.685 \\ \hdashline -1.980 & -3.139 \\ \hdashline -0.970 & -0.032 \\ -0.032 & -0.949 \end{bmatrix}$$

In comparison with Fig. 3, this smaller δ yields smaller unsafe regions as $\tilde{\Omega}_{u,1} \triangleq \mathcal{N}(\Omega_{u,1}, 0.409)$, $\tilde{\Omega}_{u,2} \triangleq \mathcal{N}(\Omega_{u,2}, 0.409)$ and $\tilde{\Omega}_{u,3} \triangleq \mathcal{N}(\Omega_{u,3}, 0.409)$. By the results in Fig. 4, we can conclude the safety of the uncertain switched system.

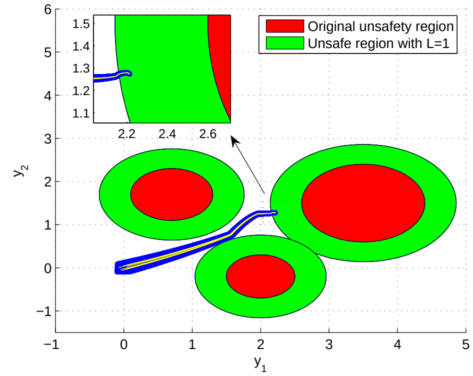

Fig. 3. The safety verification via SpaceEX for the certain system derived with ($L = 1$). The blue area is the reach set computed by SpaceEX, and the yellow lines are the random state trajectories. The safe or unsafe property of the original uncertain system cannot be concluded since the reach set of the certain system intersects with the new unsafe region.

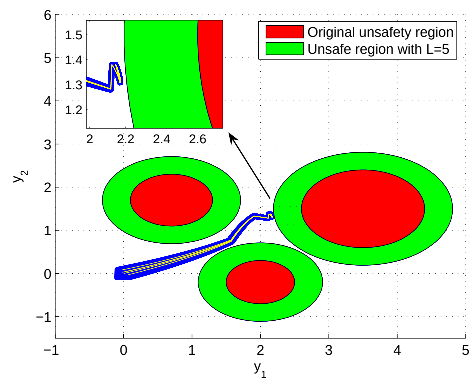

Fig. 4. The safety verification via SpaceEX for the certain system derived with ($L = 5$). The safety of the original uncertain system can be concluded since the reach set of certain system has no intersection with the new unsafe regions.

V. CONCLUSIONS

In this paper, the output reachable set estimation problem for switched linear systems has been investigated. With the aid of the common Lyapunov function and multiple Lyapunov function approaches, the output reachable set can be over-approximated by a set of bounding ellipsoids. Moreover, a sufficient condition for the existence of an approximate bisimulation of two switched linear systems is proposed, which can be viewed as an output reachable set estimation for the system combining the two bisimilar systems. Finally, by the result of approximate bisimulation, the safety verification problem for uncertain switched systems can be dealt with by verifying the safety of its bisimilar system with exact parameters. In this paper, A_i are required to be Hurwitz stable. By the techniques used in [33], the result in this paper can be readily extended to the case with some A_i are unstable. In addition, according to Table I, the computational cost significantly increases as the system order and number of modes grows, how to reduce the computational complexity and make it applicable for high dimensional systems with large amounts of subsystems will be our future study.

References

[1] R. DeCarlo, M. S. Branicky, S. Pettersson, and B. Lennartson, "Perspectives and results on the stability and stabilizability of hybrid systems," *Proceedings of the IEEE*, vol. 88, no. 7, pp. 1069–1082, 2000.

[2] H. Lin and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: a survey of recent results," *IEEE Trans. Autom. Control*, vol. 54, no. 2, pp. 308–322, 2009.

[3] D. Liberzon, *Switching in Systems and Control*. Springer Science & Business Media, 2012.

[4] H. Yang, B. Jiang, and V. Cocquempot, *Stabilization of Switched Nonlinear Systems with Unstable Modes*. Switzerland: Springer, 2014.

[5] J. C. Geromel and P. Colaneri, "Stability and stabilization of continuous-time switched linear systems," *SIAM J. Control Optimiz.*, vol. 45, no. 5, pp. 1915–1930, 2006.

[6] Z. Sun, S. S. Ge, and T. H. Lee, "Controllability and reachability criteria for switched linear systems," *Automatica*, vol. 38, no. 5, pp. 775–786, 2002.

[7] L. Zhang and P. Shi, "Stability, ℓ_2-gain and asynchronous control of discrete-time switched systems with average dwell time," *IEEE Trans. Autom. Control*, vol. 54, no. 9, pp. 2192–2199, 2009.

[8] L. Zhang, S. Zhuang, and P. Shi, "Non-weighted quasi-time-dependent $\mathcal{H}_\infty$ filtering for switched linear systems with persistent dwell-time," *Automatica*, vol. 54, pp. 201–209, 2015.

[9] G. Zhai, B. Hu, K. Yasuda, and A. N. Michel, "Disturbance attenuation properties of time-controlled switched systems," *J. Franklin Inst.*, vol. 338, no. 7, pp. 765–779, 2001.

[10] E. Fridman, A. Pila, and U. Shaked, "Regional stabilization and $\mathcal{H}_\infty$ control of time-delay systems with saturating actuators," *Int. J. Robust Nonlin. Control*, vol. 13, no. 9, pp. 885–907, 2003.

[11] J. Lygeros, C. Tomlin, and S. Sastry, "Controllers for reachability specifications for hybrid systems," *Automatica*, vol. 35, no. 3, pp. 349–370, 1999.

[12] C. Durieu, E. Walter, and B. Polyak, "Multi-input multi-output ellipsoidal state bounding," *J. Optim. Theory Appl.*, vol. 111, no. 2, pp. 273–303, 2001.

[13] E. Fridman and U. Shaked, "On reachable sets for linear systems with delay and bounded peak inputs," *Automatica*, vol. 39, no. 11, pp. 2005–2010, 2003.

[14] J.-H. Kim, "Improved ellipsoidal bound of reachable sets for time-delayed linear systems with disturbances," *Automatica*, vol. 44, no. 11, pp. 2940–2943, 2008.

[15] Z. Feng and J. Lam, "An improved result on reachable set estimation and synthesis of time-delay systems," *Applied Mathematics and Computation*, vol. 249, pp. 89–97, 2014.

[16] P. T. Nam and P. N. Pathirana, "Further result on reachable set bounding for linear uncertain polytopic systems with interval time-varying delays," *Automatica*, vol. 47, no. 8, pp. 1838–1841, 2011.

[17] Z. Feng and J. Lam, "On reachable set estimation of singular systems," *Automatica*, vol. 52, pp. 146–153, 2015.

[18] Y. Chen, J. Lam, and B. Zhang, "Estimation and synthesis of reachable set for switched linear systems," *Automatica*, vol. 63, pp. 122–132, 2016.

[19] Y. Chen and J. Lam, "Estimation and synthesis of reachable set for discrete-time periodic systems," *Optim. Control Appl. Methods*, 2015.

[20] F. Amato, R. Ambrosino, C. Cosentino, and G. De Tommasi, "Input–output finite time stabilization of linear systems," *Automatica*, vol. 46, no. 9, pp. 1558–1562, 2010.

[21] F. Amato, M. Ariola, and C. Cosentino, "Finite-time stability of linear time-varying systems: analysis and controller design," *IEEE Trans. Autom. Control*, vol. 55, no. 4, pp. 1003–1008, 2010.

[22] A. Girard and G. J. Pappas, "Approximate bisimulation: A bridge between computer science and control theory," *European Journal of Control*, vol. 17, no. 5, pp. 568–578, 2011.

[23] G. Pola, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," *Automatica*, vol. 44, no. 10, pp. 2508–2516, 2008.

[24] A. Girard, "Controller synthesis for safety and reachability via approximate bisimulation," *Automatica*, vol. 48, no. 5, pp. 947–953, 2012.

[25] Y.-Y. Cao, J. Lam, and Y.-X. Sun, "Static output feedback stabilization: an ILMI approach," *Automatica*, vol. 34, no. 12, pp. 1641–1645, 1998.

[26] Z. Shu and J. Lam, "An augmented system approach to static output-feedback stabilization with $\mathcal{H}_\infty$ performance for continuous-time plants," *Int. J. Robust Nonlin. Control*, vol. 19, no. 7, pp. 768–785, 2009.

[27] A. S. Morse, "Supervisory control of families of linear set-point controllers part I. exact matching," *IEEE Trans. Autom. Control*, vol. 41, no. 10, pp. 1413–1431, 1996.

[28] L. Allerhand and U. Shaked, "Robust stability and stabilization of linear switched systems with dwell time," *IEEE Trans. Autom. Control*, vol. 56, no. 2, pp. 381–386, 2011.

[29] C. Briat and A. Seuret, "A looped-functional approach for robust stability analysis of linear impulsive systems," *Syst. Control Lett.*, vol. 61, no. 10, pp. 980–988, 2012.

[30] W. Xiang and J. Xiao, "Stabilization of switched continuous-time systems with all modes unstable via dwell time switching," *Automatica*, vol. 50, no. 3, pp. 940–945, 2014.

[31] W. Xiang, "Necessary and sufficient condition for stability of switched uncertain linear systems under dwell-time constraint," *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp. 3619–3624, 2016.

[32] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, "Spaceex: Scalable verification of hybrid systems," in *Computer Aided Verification*, pp. 379–395, Springer, 2011.

[33] W. Xiang, G. Zhai, and C. Briat, "Stability analysis for LTI control systems with controller failures and its application in failure tolerant control," *IEEE Trans. Autom. Control*, vol. 61, no. 3, pp. 811–816, 2016.

Appendix

Proof of Lemma 1: Define the following Lyapunov function as $V(t) = \sum_{i\in\mathcal{M}} \xi_i(t)V_i(x(t))$, where $\xi_i(t)$, $i \in \mathcal{M}$, is same as in Theorem 2. First, we consider any $t \in [t_k, t_{k+1}) \subset \mathcal{I}_i$, $\forall i \in \mathcal{M}$. (6) implies

$$\dot{V}(t) \leq -\alpha V(t) + \alpha u^\top(t) R_u u(t),\ t \in [t_k, t_{k+1}) \tag{56}$$

Then, multiplying both sides of (56) with $e^{\alpha(t-t_k)}$ and then integrating it over $[t_k, t)$, we have $V(t) \leq e^{-\alpha(t-t_k)}V(t_k^+) + \int_{t_k}^t e^{-\alpha(t-s)}u^\top(s)R_u u(s)\mathrm{d}s$. Due to $u(t) \in \mathcal{E}(R_u)$, $\forall t \in \mathbb{R}_{\geq 0}$, that is $u^\top(t)R_u u(t) \leq 1$, $\forall t \in \mathbb{R}_{\geq 0}$, we have the following result

$$\begin{aligned} V(t) &\leq e^{-\alpha(t-t_k)}V(t_k^+) + \int_{t_k}^t e^{-\alpha(t-s)}\mathrm{d}s \\ &= e^{-\alpha(t-t_k)}V(t_k^+) + 1 - e^{-\alpha(t-t_k)} \end{aligned} \tag{57}$$

and it can be rewritten to

$$V(t) - 1 \leq e^{-\alpha(t-t_k)}(V(t_k^+) - 1),\ t \in [t_k, t_{k+1}) \tag{58}$$

Next, we consider $t_k \in \mathcal{S}$. From (7), we can obtain that $V(t_k^+) \leq \beta V(t_k^-) + 1 - \beta$, $t_k \in \mathcal{S}$, which can be equivalently rewritten to

$$V(t_k^+) - 1 \leq \beta(V(t_k^-) - 1),\ t_k \in \mathcal{S} \tag{59}$$

Combining (58) and (59), the following derivation can be obtained for $\forall t \in \mathbb{R}_{\geq 0}$

$$\begin{aligned} V(t) - 1 &\leq e^{-\alpha(t-t_k)}(V(t_k^+) - 1) \leq \beta e^{-\alpha(t-t_k)}(V(t_k^-) - 1) \\ &\leq \cdots \leq \beta^{\mathrm{Num}(t-t_0)}e^{-\alpha(t-t_0)}(V(t_0) - 1) \end{aligned}$$

where $\mathrm{Num}(t-t_0)$ denotes the number of switchings during $[t_0, t)$. Due to $\alpha > 0$ and $0 < \beta \leq 1$, it means that

$$V(t) - 1 \leq V(t_0) - 1,\ \forall t \in \mathbb{R}_{\geq 0} \tag{60}$$

Furthermore, (8) implies that $V(t_0) \leq x_0^\top R_0 x_0 \leq 1$, and (9) together with (60) yield that $y^\top(t)R_{i,y}y(t) \leq V(t) \leq 1$ holds when $\sigma(t) = i \in \mathcal{M}$, $t \in \mathbb{R}_{\geq 0}$. For all possible $i \in \mathcal{M}$, $y(t)$ thus satisfies $y(t) \in \bigcup_{i\in\mathcal{M}} \mathcal{E}(R_{i,y})$, $\forall t \in \mathbb{R}_{\geq 0}$ and therefore, $\mathcal{R}_y \subseteq \tilde{\mathcal{R}}_y$ by the definition of $\tilde{\mathcal{R}}_y$ given in (1).