






# A Relative Operation-Based Separation Model for Safe Distances of Virtually Coupled Trains

Ming Chai , Member, IEEE, Haifeng Wang , Member, IEEE, Tao Tang , Senior Member, IEEE, Jinchuan Chai , Member, IEEE, and Hongjie Liu , Member, IEEE

**Abstract**—Virtual coupling is a novel railway transport concept that allows trains to split and join on-the-fly by switching from mechanical to virtual couplers. One of the main challenges in applying virtual coupling in metro railways is to reduce the tracking distance between trains without compromising safety. This article proposes a relative operation-based train separation model to reduce the safe distance between trains. This model applies a fault tolerance principle. The principle is that the preceding train normally operates for a time interval from its last-known state before initiating an emergency brake to stop the train. A difficulty in applying the proposed model is to predict the boundary of all possible time-position trajectories of the preceding train, which is the reachability problem of a hybrid system. To solve this problem, we formalise the operation of the preceding train by a parameterized hybrid automaton. A polytope-based algorithm is then developed for computing an over-approximated reachable set of the automaton. We compare our approach with a state-of-the-art relative braking distance-based train separation model for virtual coupling on a concrete metro line in Chengdu, China, and evaluate the method with several benchmarks. The results demonstrate that the relative operation-based model substantially reduces the safe distances between trains. Compared to conventional approaches, the proposed model provides a considerable 90.7% decrease in unnecessary waiting time at railway stations for virtually coupled trains and a 4.9% increase in the capacity of the given railway lines.

**Index Terms**—Virtual coupling, Safe distance, Train separation model, Train control system, Hybrid automata.

## I. INTRODUCTION

THE ever-increasing need for service improvements led the railway industry to explore the next generation of train

Manuscript received 7 June 2023; revised 3 July 2023 and 21 July 2023; accepted 27 July 2023. Date of publication 2 August 2023; date of current version 23 February 2024. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2022JBZY003, in part by Beijing Municipal Natural Science Foundation under Grant L201004, in part by the science and technology research plan of China Railway Corporation under Grant L2021G009, and in part by the Frontiers Science Center for Smart High-speed Railway System and the Beijing Laboratory of Urban Rail Transit. (Corresponding author: Hongjie Liu.)

Ming Chai, Haifeng Wang, and Hongjie Liu are with the National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing 100044, China (e-mail: chaiming@bjtu.edu.cn; hfwang@bjtu.edu.cn; hjliu2@bjtu.edu.cn).

Tao Tang is with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China (e-mail: ttang@bjtu.edu.cn).

Jinchuan Chai is with the National Railway Track Test Center, China Academy of Railway Sciences Corporation Ltd., Beijing 100015, China (e-mail: chajinchuan@rails.cn).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TIV.2023.3301009>.

Digital Object Identifier 10.1109/TIV.2023.3301009

control concepts, such as virtual coupling [1]. This concept entails tracked trains virtually coupled via distributed controls and vehicle-to-vehicle communication. The distance between two virtually coupled trains is much shorter than conventional railway systems. On the one hand, virtual coupling expands the railway transportation capacity of existing networks. On the other hand, trains can split and join on-the-fly according to transport demand. Virtual coupling is a promising technique for achieving the *zero capacity waste* target proposed by the European Rail Research Advisory Council (ERRAC).

One of the main challenges in applying virtual coupling in metro railway transportation is reducing the distance between the tracked trains without compromising safety. A long tracked distance can make it difficult for trains to arrive simultaneously at stations, resulting in unnecessary additional waiting time at the station. This shortcoming significantly reduces the transportation capacity and service quality of metro railways.

A typical train control system in metro railways adopts an ATP-ATO control scheme, which consists of an automatic train operation (ATO) controller supervised by an automatic train protection (ATP) controller [2]. The ATO is similar to an adaptive cruise controller used in road vehicles. It performs nominal train driving actions like speed regulations, tractions and service brakes. In contrast, the ATP protects a train by computing a safe distance to prevent collisions and initiating an emergency brake whenever a safe distance cannot be guaranteed. A similar control scheme has also been proposed for autonomous vehicles to guarantee safety [3].

In railways, the ATP is safety-critical, following the *fail-safe principle*, i.e., the safe distance must prevent collisions even with the worst-case credible latent system failure modes. An example of the worst-case is that the following train loses partial braking capacity by equipment failures while its preceding train decelerates with an emergency brake. Existing ATP controllers of train control systems use pneumatic brake systems to perform emergency brakes. Compared to the electric braking systems used by autonomous road vehicles, a pneumatic brake system leads to extra difficulties in reducing the safe distance for the following reasons. On the one hand, a pneumatic brake is an open-loop mechanical controller with significant controlling error. The worst-case of the braking performance must always be considered to ensure collision-free. On the other hand, once a train initiates an emergency brake, it is impossible to reduce the braking force or release the brake until it has fully stopped. When the preceding train initiates an emergency brake, it cannot

adjust the braking force even if the following train runs too close.

Reducing the safe distance between trains is a central problem in virtual coupling because the safe distance decides the smallest possible tracking distance between the trains under the *ATP-ATO* control scheme. The safe distance is computed in railways by a so-called *train separation model*. Conventional train control systems use the *absolute brake distance-based train separation* (ABS) model (also known as “moving block”), where the safety distance equals the emergency braking distance of the following train plus a safety margin. Adopting that a train is physically impossible to stop instantly, a *relative brake distance-based train separation* (RBS) model is proposed. In the RBS model, the preceding train is assumed to apply an emergency brake from its last-known state. The safe distance between two tracked trains is decided by ensuring that both trains do not collide under the worst-case stopping scenario [4]. By assuming that the trains always have the same braking performance, the safe distance is simplified to be the difference of the emergency braking distances of the trains plus a safety margin [5]. Unfortunately, the safe distance computed by the RBS model is still too big for virtual coupling in metro railways. For example, considering the worst-case control errors and failures of real-world pneumatic brake systems, the safe distance between two trains is greater than 100 meters at 80 *km/h* even if the trains have the same braking performance. With such a considerable safe distance, it is difficult for trains to arrive simultaneously at stations. Consequently, gaining actual capacity from the concept of virtual coupling is impacted.

This article addresses the needs to further reduce the safe distance by defining a novel train separation model and solving the model to find the required safe distance without compromising safety. The model mainly builds on the assertion that the ATP only applies an emergency brake in the occurrence of failures and fault propagation takes time. Therefore, it is unrealistic that an ATP applies an emergency brake instantly if there are no faults in the last-known state of the train. In this model, the preceding train is assumed to operate by the ATO for a short time and then applies an emergency brake by the ATP. Because the model uses the relations between the operation processes of the tracked trains to compute the safe distance, we name it by *relative operation-based train separation model* (ROS).

The RBS model requires the tracked trains to have the same emergency brake performance. The safe distance between the trains in an RBS model equals the difference in the braking distances of the trains. However, this safe distance cannot guarantee collision-free if the trains have different deceleration rates. To solve the problem, in the proposed ROS model, the safe distance is decided by ensuring that all possible time-position trajectories of the trains never join until both have fully stopped. Therefore, the boundaries of all possible time-position trajectories of the trains must be predicted. When a train is controlled with a constant strategy of braking, such as an emergency brake or a more complicated deceleration profile, the boundaries of possible time-position trajectories can be computed by simply using the boundary values of the deceleration [6]. Unfortunately, predicting the preceding train is complicated when applying the

fault tolerance principle. In the normal operation phase, the control input is multi-variant with discrete changes that follow ATO control rules. The maximal/minimal accelerations for each point in time are difficult to obtain, and the boundaries of the possible time-position trajectories of the train cannot be predicted with global boundary values of control inputs (Theorem 2).

In the ROS model, the operation of the preceding train is a hybrid system, where evolutions of train positions depend on interactions of continuous (train dynamic) and discrete (changes of control inputs) components. The analysis of the behaviour boundary of a hybrid system is inherently complex. In this article, we develop a *reachable set*-based approach to predicate the boundary of all possible time-position trajectories of the preceding train. This approach first formalises the train operation with a parameterized hybrid automaton with uncertain nonlinear switch conditions. Because the dynamic of the automaton is linear, we choose to use a polytope-based algorithm to compute the over-approximation of the reachable set of the automaton.

We further illustrate the practicality of the proposed approach with numerical experiments. The safe distance is translated into the emergency brake intervention (EBI) speed of the following train. With an EBI speed, the target speed of the ATO controller of the following train can be obtained. We compare the method of the paper with the state-of-the-art RBS model. As demonstrated through the simulation results, the tracked distances between the trains can be reduced, and the train capacity can be improved by applying the proposed ROS model.

The main contribution of the paper is the development of the ROS model that reduces the safe distance between virtually coupled trains without compromising safety. In metro railways, a shorter safe distance is conducive to the simultaneous arrival of virtually coupled trains at stations. Consequently, the model reduces the unnecessary waiting time of trains at stations and improves the capacity of railway lines.

The remainder of this article is organised as follows. Section II provides a brief overview of related work. Section III introduces the preliminaries of automatic train control systems and the conventional relative brake distance-based train separation model. Section IV proposes a relative operation-based train separation model for virtual coupling. Section V develops a reachable set-based method for predicting the boundary of time-position trajectories of the preceding train. Section VI demonstrates the proposed approach using concrete data from Chengdu Metro Line No. 8 in China. Section VII presents the conclusions and directions for future work.

## II. RELATED WORK

### A. Control Approaches for Virtual Coupling

The problem of optimising train operations has a long tradition in the railway community, including optimising operation trajectories [7], control strategies [8], [9], [10] and timetables [11], [12]. The concept of virtual coupling in railways was first proposed by Bock et al. to improve the capacity of existing railway lines [13]. In this concept, trains are no longer physically coupled; each has individual propulsion and brake systems. An advantage of virtual coupling is that trains can split and join

on-the-fly to fulfil transportation needs. Chai et al. considered the time-dependent passenger demand and train loading capacities in virtual coupling. They proposed a linear programming-based approach for virtual coupling to improve line capacity and reduce congestion in metro railway networks [14]. The distance between virtually coupled trains must be small enough for simultaneous arrival to make the concept practicable in metro railway transportation. In railways, a train control system adopts the ATP-ATO scheme. Both the controllers of the ATO and ATP have been investigated for reducing tracked distances between trains.

Using model predictive control (MPC) and its extensions to design the ATO for virtual coupling is one of the most popular research directions in recent years. Su et al. proposed a centralized MPC for virtual coupling with nonlinear safety equilibrium spacing policy [15]. Decentralised model predictive control methods for virtually coupled trains have been investigated, where the trajectories of the preceding trains are assumed to be predictable over a short time horizon [16], [17]. Di Meo et al. defined a coupling algorithm by considering time-varying delays in vehicle-to-vehicle communications of trains [18]. Park et al. proposed a robust gap controller based on sliding mode control [19]. Liu et al. designed a gap reference generation algorithm to allow the trains to merge into the same convoy, maintain the convoy and then separate [20]. Luo et al. proposed a robust MPC approach to reduce the tracking distance between virtually coupled trains while satisfying the safety constraints of trains [21].

The smallest possible tracked distance between trains cannot be smaller than the safe distance used by the ATP. Therefore, reducing the safe distance without compromising safety is a fundamental problem in virtual coupling. Two train separation models have been carried out in railways to compute the safe distance between two tracking trains [5]. The first model assumes the preceding train stops instantly at its last-known position, called *absolute braking distance*-based model (also known as *moving block*). In this model, the safe distance between tracked trains equals the emergency braking distance of the following train. The second model adopts the fact that the preceding train is physically impossible to stop instantly, called *relative brake distance*-based model. In this model, the safe distance reduces to the difference in the emergency braking distances of the trains.

Ning showed that the relative brake distance-based model only prevents collisions when the preceding train has a worse braking performance than the following train [22]. A similar result was shown by Althoff et al. in the context of road vehicles [6]. Because it is impossible that two trains always have the same emergency brake performance in practice, the conventional RBS model cannot guarantee collision-free in virtual coupling. Quaglietta et al. proposed a train-following model with a dynamic safety margin that considers differences in braking performances of the tracked trains [23]. A specific braking performance manoeuvre is designed for the RBS model to avoid collisions [24]. Zhao et al. proposed a more general train separation method by considering the whole braking process of the trains [4]. Their model can guarantee collision-free with arbitrary emergency braking performances of the tracked trains.

Su et al. proposed an approach to predict the braking process of the preceding for computing the safe distance [25]. The above models are extensions of the RBS model, assuming that the preceding train applies an emergency brake. The safe distance computed by these models is still too big for virtual coupling in metro railways. To the best of our knowledge, no train separation model has been proposed yet that considers the fault tolerance time before initiating an emergency brake of the preceding train.

## B. Predictions of Train Operations

A central problem in applying a train separation model is predicting all possible tracked train operations.

Machine learning-based methods that apply data-driven models have been investigated for predicting trajectories of autonomous vehicles [26]. However, as machine learning has an inherent unexplainable problem, a machine learning-based method cannot guarantee to predict the boundaries of train operations. Therefore, it cannot be used to compute the safe distance between trains.

Proving the correctness of a train control system with formal methods is an important research direction [27]. *Runtime verification* is a lightweight formal method that can predict undesired behaviours while the system is running [28]. In the following, we mainly focus on previous work on reachable set-based prediction approaches since this work can guarantee obtaining boundaries of system behaviours. Hybrid automata have been proposed to formalise systems with discrete-continuous state spaces [29]. This formalism is expressive but has considerable difficulties in solving its reachability problem. Girard et al. proposed a zonotope-based approach for overestimating the reachable set of hybrid automata with linear dynamics and guards [30]. Based on those works, Kochdumper et al. proposed an algorithm for computing intersections between nonlinear guards and reachable sets with Taylor models or polynomial zonotopes [31]. Ramdani et al. presented an interval Taylor method-based approach of computing reachable sets of hybrid systems with uncertain nonlinear monotone dynamics [32].

Various reachable set-based collision avoidance approaches have been developed by predicting the complete operations of a system. Based on the computation of reachable sets, a collision detection method for autonomous driving has been proposed for predicting possible crashes during specific trajectories [33]. Malone et al. proposed an accurate potential field generation approach for autonomous robotics based on stochastic reachable sets considering the effects of uncertain and dynamic environments [34]. Lin et al. presented a real-time path planning algorithm for unmanned aerial vehicles (UAV) by predicting possible collisions in the region reachable set of an obstacle aircraft [35]. Zhou et al. proposed an onboard collision avoidance method that guaranteed the safety of UAVs by computing the trajectories within the reachable tube [36]. Söntges et al. presented an approach for determining the optimal intervention time to mitigate and prevent collisions of intelligent vehicles by computing the over-approximation of the possible trajectories in the reachable sets [37]. Loos et al. combined hybrid system verification techniques with a wireless communication model



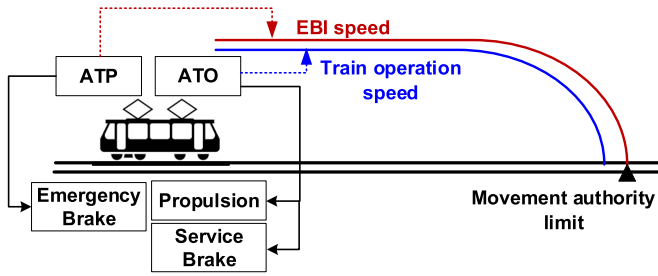


Fig. 1. Typical automatic train control system.

to analyse the effectiveness of timeout values to a provably safe cruise adaptive control system [38]. Stursberg et al. used a counterexample-guided verification approach to prove the correctness of a cruise control system, which is modelled as a hybrid automaton [39]. Xu et al. proposed a collision prediction approach for satellites with zonotope-based reachable sets, in which the satellites are simplified as cuboids to compute reachable domains and dangerous domains with uncertain motions [40]. These works focus on proving the correctness of a system. How to compute the safe distance between trains when considering normal operations of the preceding train in virtual coupling is still an ongoing research topic.

### III. PRELIMINARIES

#### A. Automatic Train Control System

Due to unpredictable driving actions and the reaction time of human drivers, virtually coupled trains must be operated by automatic train control (ATC) systems to maintain a safe small tracked distance. An ATC system adopts an automatic train protection-automatic train operation (ATP-ATO) control scheme, as shown in Fig. 1. The ATP provides fail-safe protections with the emergency brake to ensure the tracked trains keep a safe distance. In contrast, the ATO performs automatic driving functions by applying propulsions and service brakes. A safe distance between tracked trains is transferred to a *movement authority* of the following train, which is the authority for the train to enter and travel through a specific section of track. An EBI speed is the maximal speed that ensures under no circumstances will the train stop at the movement authority limit (i.e., the furthest position of the movement authority) by applying an emergency brake. It is derived from the braking curve of the train with the guaranteed emergency brake rate. The EBI speed curve is regarded as a “safe envelope” for automatic driving [41]. The ATO shall maintain the train speed below the EBI speed. If the EBI speed at the train location is exceeded, the ATP initiates an immediate emergency brake application.

#### B. Relative Brake Distance-Based Train Separation Model

In railways, the safe distance between two tracked trains is computed by a train separation model to guarantee collision-free. A relative brake distance-based separation (RBS) model has been proposed that the safe distance between two trains equals the difference in the braking distances of the trains plus a *safety*

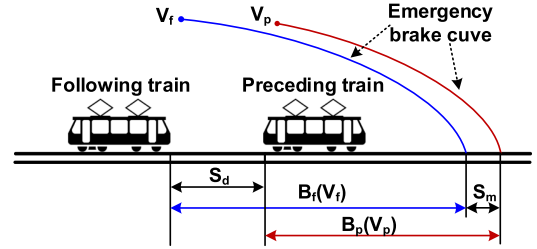


Fig. 2. Relative brake distance train separation model.

*margin* [5]. A safety margin is an extra distance to handle the impact of other unknown factors, such as the measurement error of train position and speed and communication delays. Fig. 2 illustrates an RBS model. Let  $S_d$  be the safe distance between two tracked trains;  $B_p(V_p)$  and  $B_f(V_f)$  be the emergency brake distances of the preceding train and the following train starting from their current speed  $V_p$  and  $V_f$  respectively, and  $S_m$  be a safety margin. The RBS model is defined as follows.

$$S_d = \max((B_f(V_f) - B_p(V_p)), 0) + S_m \quad (1)$$

A train separation model guarantees the collision-free property, i.e., two tracked trains are never in the same position simultaneously. The standard RBS model, as defined by (1), simplifies the train separation model indicating that the property can be satisfied if the distance between two trains is always greater than the relative emergency braking distances. Unfortunately, this simplification only holds at some ideal conditions. Ning proved that the standard RBS model could prevent collisions only if the braking performance of the preceding train is worse than or equal to the braking performance of the following train [22]. Because the ATP uses the open-looped pneumatic brake system, it is possible that the emergency brake of the following train has a smaller deceleration. This braking rate combination must be considered in real-world train control systems. Therefore, the standard RBS model is insufficient to guarantee collision-free in real-world applications. Consider the following example. Let the initial speeds of two tracked trains be  $V_p = 17$  m/sec and  $V_f = 22$  m/sec, the emergency brake accelerations be  $a_p = -0.8$  m/sec<sup>2</sup> and  $a_f = -1.2$  m/sec<sup>2</sup>. Let the safety margin be  $S_m = 5$  m. The safe distance is 26.1 m according to the RBS model. Fig. 3 shows that when the preceding train applies an emergency brake, a collision occurs even if the following train initiates an emergency brake immediately.

### IV. COMPUTATIONAL MODEL OF SAFE DISTANCE FOR VIRTUAL COUPLING

#### A. Relative Operation-Based Train Separation Model

We propose a *relative operation-based separation (ROS)* model to compute the safe distance for virtual coupling. In the ROS model, the safe distance between two tracked trains is decided by ensuring that when the following train applies an emergency brake, the smallest distance between the trains is greater than or equal to the safety margin with the predicted worst-case operation of the preceding train. According to the

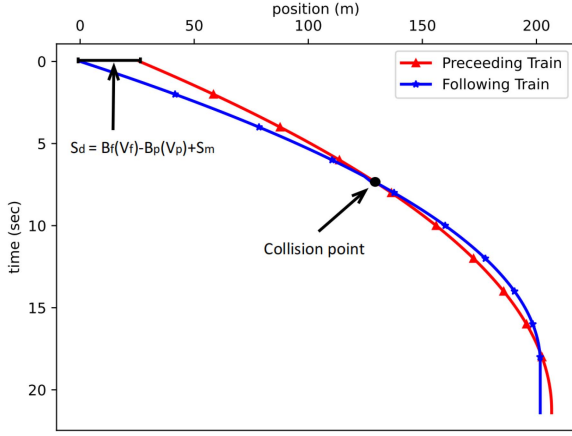


Fig. 3. Counter-example showing that the RBS model cannot guarantee collision-free.

ATP-ATO control scheme, as shown in Fig. 1, the ATP computes the EBI speed from the ROS model. After that, the ATO generates its speed constraint concerning the EBI speed.

An ATP only initiates an emergency brake with certain failures. Because fault propagation consumes time, if the last-known status of a train does not meet any pre-conditions of such a failure, it is safe to predict that the train will operate normally without triggering an emergency brake for at least a period of fault-tolerant time. According to this assertion, the ROS model applies a  $\hat{T}$  fault tolerance ( $\hat{T}$ -FT) principle with  $\hat{T}$  being an interval of a fault-tolerant time. With this principle, the operation of the preceding train is divided into two phases. In the first phase, the train operates normally for  $\hat{T}$  seconds by the ATO. In the second phase, the train applies an *emergency brake strategy* that the ATP initiates an emergency brake to stop the train. The  $\hat{T}$ -FT principle is formally defined as follows.

We use *time-position state (TPS)* to define the train position at some time point. Given the set  $\mathbb{R}$  of real numbers and a time  $t \in \mathbb{R}$ , a TPS  $D(t)$  represents the position of a train at time  $t$ . A *time-position trajectory (TPT)*  $\vec{D} \triangleq (D(T_0), D(T_1), \dots, D(T_N))$  is a finite sequence of TPSs, where  $N$  is an index. A TPT represents an operational process of a train. A TPT is called *complete* if it indicates that the train eventually stops, i.e., a TPT  $\vec{D}$  is complete if and only if

$$\exists i \in [0, N] \text{ s.t. } \forall j \in [i, N] : D(T_j) = D(T_i) \quad (2)$$

By “.” we denote the concatenation of sequences, e.g., the concatenation of sequences  $\vec{A}$  and  $\vec{B}$  yields a sequence  $\vec{A} \cdot \vec{B}$ . The  $\hat{T}$ -FT principle is defined as follows.

**Definition 1** ( $\hat{T}$  fault tolerance principle ( $\hat{T}$ -FT principle)): Let  $\vec{D}$  be a complete TPT of the preceding train in virtual coupling with  $\vec{D} \triangleq \vec{D}_1 \cdot \vec{D}_2$ . If the train applies the  $\hat{T}$ -FT principle, then  $\vec{D}_1 \triangleq (D(T_0), \dots, D(T_N))$  is a normal operational (control by ATO) TPT with  $T_N - T_0 = \hat{T}$ , and  $\vec{D}_2$  is an emergency brake (control by ATP) TPT.

We illustrate the  $\hat{T}$ -FT principle with the *communication failure*, one of the pre-conditions of triggering an emergency brake. An ATC system exchange messages periodically with wayside and central systems while operating a train. When the

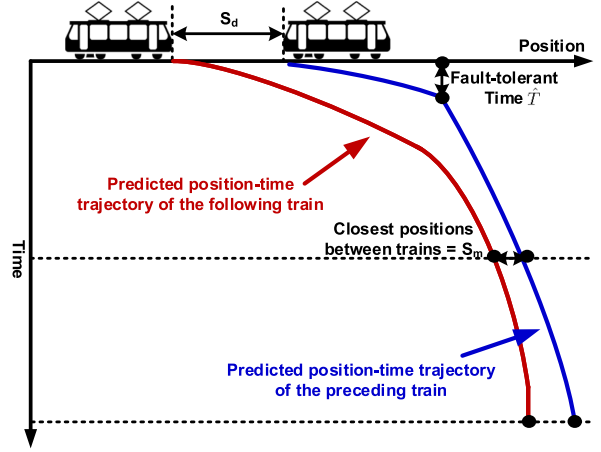


Fig. 4. Illustration of the relative operation-based separation model.

ATC fails to receive a periodic message, it starts a timer and attempts to reconnect. No message is received by the ATC continuously for a time interval, e.g.,  $\hat{T}$  seconds. The ATP system can confirm the occurrence of a communication failure and initiates an emergency brake application. In this case, if a message is received in the last-known state of the ATC, one can predict that an emergency brake will not occur within  $\hat{T}$  seconds caused by communication failure.

A *time-position space*  $\mathcal{D}$  is the set of all possible complete time-position trajectories of a train under an automatic train control system.

**Definition 2** (ROS model): Let  $\mathcal{D}_p$  and  $\mathcal{D}_f$  be the time-position space of the preceding train and the following train, respectively. Given a safety margin  $S_m$ , the safe distance  $S_d$  between the trains in the ROS model can be computed by solving the following problem:

$$\begin{aligned} \min S_d, \text{ s.t.} \\ S_d &= D_p(T_0) - D_f(T_0) \\ \forall (D_p(T_0), D_p(T_1), \dots, D_p(T_N)) &\in \mathcal{D}_p \\ \forall (D_f(T_0), D_f(T_1), \dots, D_f(T_N)) &\in \mathcal{D}_f \\ \forall i \in [0, N] : D_p(T_i) - D_f(T_i) &\geq S_m \end{aligned} \quad (3)$$

An illustration of the ROS model is shown in Fig. 4. In the ROS model, the safe distance is computed by ensuring that the smallest distance between the time-position trajectories of the tracked trains is greater than or equal to the safety margin.

We prove that if the safe distance between two virtually coupled trains is computed by the ROS model, collision-free can be guaranteed with an arbitrary configuration of emergency brake rates of the trains.

**Proposition 1:** Given two tracked trains with an arbitrary configuration of emergency brake rates, if  $S_d$  is computed by the ROS model as defined in (3), then  $(S_p(t) - S_f(t)) \geq S_m$  for all  $t > 0$ .

**Proof:** According to the definitions,  $\mathcal{D}_p$  and  $\mathcal{D}_f$  are time-position spaces that contain all possible complete time-positions of the preceding train and the following train, respectively. The

smallest distance between the trains equals or exceeds the safety margin  $S_m$  until both trains have fully stopped.  $\square$

One of the main challenges in the ROS model is predicting the time-position spaces (i.e., all possible TPTs) of the tracked trains.

### B. The Time-Position Space of Preceding Train

With the  $\hat{T}$ -FT principle, the ATO behaviour of the preceding train must be considered when predicting the time-position space of the train. An ATO system can choose different control strategies by considering operation efficiency, energy savings, passenger comfort, etc. This article considers a typical strategy in which a train operation process between two stations is divided into three phases: departure, cruising and arrival. The ATO target speed in the first two phases is according to the EBI speed, whereas in the third phase, it is computed according to the intended stopping position. During the departure phase, the train accelerates with its maximum propulsion until it reaches the target speed. During cruising, the ATO system ensures that the train operates at the target speed. During the arrival phase, the ATO applies a programmed stopping process. An ATO system applies the following *adjustment inhibition strategy* (AIS) to avoid frequent control adjustments. Once the ATO system is in either the propulsion or brake status, the system stays in that status for a time interval before switching to the other status.

Let a control  $u \in \mathbb{R}$  be the acceleration of a train. A *control trace*  $\mathbf{u}$  is defined as a sequence of controls, i.e.,  $\mathbf{u} \triangleq (u_0, \dots, u_N)$ . Given an integer  $K$ , the set  $\mathbb{R}^K$  contains all control traces with length  $K$  over  $\mathbb{R}$ . Given integers  $K_1$  and  $K_2$ , we denote by  $T_\Delta$  and  $[T_\Delta K_1, T_\Delta K_2]$  the control cycle and the time interval of the AIS, respectively. An *ATO control space* contains all possible control traces concerning the ATC operation logic.

*Definition 3 (ATO control space):* Let  $V_{\text{Tar}}^i$  be the ATO target speed at the  $i$ th position in a control trace, and  $\mathcal{A}_P$  and  $\mathcal{A}_B$  be the range of accelerations of propulsion and service brake, respectively. The ATO control space  $\mathcal{U}_O$  is the set of all possible ATO control traces as follows.

$$\mathcal{U}_O \triangleq \{\mathbf{u} \mid \mathbf{u} = \mathbf{u}_A \cdot \mathbf{u}_B\}, \text{ where :}$$

$\mathbf{u}_A = (u_1, \dots, u_n)$  represents the departure phase:

$$\forall i \in [1, n] : u_i = \max \mathcal{A}_P$$

$\mathbf{u}_B = (\mathbf{u}_1 \cdot \dots \cdot \mathbf{u}_n)$  is the cruising and arrival phases:

$$\forall i \in [1, n] : \left( v_i < V_{\text{Tar}}^i \Rightarrow \mathbf{u}_i \in \bigcup_{k \in [K_1, K_2]} \mathcal{A}_P^k \right) \wedge \left( v_i \geq V_{\text{Tar}}^i \Rightarrow \mathbf{u}_i \in \bigcup_{k \in [K_1, K_2]} \mathcal{A}_B^k \right)$$

If we define the solution of the model  $f(D(T), u)$  as the TPS at time  $T + T_\Delta$  from  $D(T)$  under a control  $u$ , then  $\vec{f}(D(T_0), \mathbf{u})$  is a TPT (i.e., a sequence of time-position states) starting from

$D(T_0)$  under a control trace  $\mathbf{u}$  such that

$$\vec{f}(D(T_0), \mathbf{u}) \triangleq (D(T_0), D(T_1), \dots, D(T_n)) \quad (4)$$

where  $\forall i \in [1, n] : D(T_i) = f(D(T_{i-1}), u_{i-1})$ .

*Definition 4 ( $\hat{T}$ -time-position space):* Let  $\mathcal{U}_O^K$  be the subset of the ATO control space  $\mathcal{U}_O$  containing all control traces, i.e.,  $\mathcal{U}_O^K \subset \mathcal{U}_O$ , each of which has a length  $K$  with  $K = \frac{\hat{T}}{T_\Delta}$ . The  $\hat{T}$ -time-position space  $\mathcal{D}^{\hat{T}}(D(T_0))$  is the set of all possible TPTs starting from  $D(T_0)$  within  $\hat{T}$  seconds such that

$$\mathcal{D}^{\hat{T}}(D(T_0)) \triangleq \{\vec{f}(D(T_0), \mathbf{u}) \mid \mathbf{u} \in \mathcal{U}_O^K\} \quad (5)$$

We denote by  $\langle \vec{D} \rangle$  the last TPS of  $\vec{D} \triangleq (D(T_0), \dots, D(T_n))$ , i.e.,  $\langle \vec{D} \rangle \triangleq D(T_n)$ . Given a control trace  $\mathbf{u} \triangleq (a_{PT}, \dots, a_{PT})$  with  $a_{PT}$  being the emergency brake acceleration of the preceding train and the last-known TPS  $D(T_0)$  of the preceding train, the time-position space  $\mathcal{D}_p$  of the preceding train in the ROS model with the  $\hat{T}$ -FT principle is as follows.

$$\mathcal{D}_p \triangleq \{(\vec{D}_1 \cdot \vec{D}_2) \mid \vec{D}_1 \in \mathcal{D}^{\hat{T}}(D(T_0)), \vec{D}_2 = \vec{f}(\langle \vec{D}_1 \rangle, \mathbf{u})\} \quad (6)$$

Intuitively, the subsequence  $\vec{D}_1$  specifies the normal operation phase, controlled by ATO, with the  $\hat{T}$ -FT principle, whereas  $\vec{D}_2$  represents the emergency brake phase.

Due to unmodelled dynamics and mismatched parameters, the ROS model contains uncertainties in parameters and control traces. When the time value  $\hat{T}$  of the  $\hat{T}$ -FT principle is greater than 0 sec, the boundaries of the time-position space cannot be computed with boundary values of accelerations. Because the ATC operations follow specific logical rules, the possible accelerations at each time point are multi-variant. They are challenging to obtain. We prove that using the global acceleration boundaries of an ATO cannot cover all possible TPTs of a train.

*Proposition 2:* Let  $\vec{D}_1, \dots, \vec{D}_N$  be the complete TPTs of the preceding train in the ROS model obtained by simulations with the boundary values of accelerations. If  $\hat{T} > 0$ , then there exists a complete TPT  $\vec{D}_o \in \mathcal{D}_p$  and a point of time  $T$ , it holds that  $D(T)_o < \min(D(T)_1, \dots, D(T)_N)$ , where  $D(T)_o \in \vec{D}_o$  and  $D(T)_i \in \vec{D}_i$  with  $i \in [1, N]$ .

*Proof:* According to the  $\hat{T}$ -FT principle, the train operation trajectory is as follows. The ATO system controls the train for  $\hat{T}$  seconds. After  $\hat{T}$  seconds, the ATP system immediately initiates the emergency brake, and then the train moves with its maximum emergency brake acceleration until it fully stops. Without loss of generality, we use the following parameters in the proof: The ATO target speed is 20 m/sec. The upper and lower boundaries of the propulsion acceleration are 1.0 m/sec<sup>2</sup> and 0.4 m/sec<sup>2</sup>, respectively. The upper and lower boundaries of the service brake acceleration are  $-0.3$  m/sec<sup>2</sup> and  $-0.6$  m/sec<sup>2</sup>, respectively. The time duration of the adjustment inhibition strategy is set to be between 5 and 12 control cycles; The control period is 0.2 sec. The acceleration of the emergency brake is  $-1.2$  m/sec<sup>2</sup>. The time duration of the  $\hat{T}$ -FT principle is 6 seconds.

Let the initial train speed be 18.5 m/s. Simulations according to the boundaries of the parameters (PCS-BA) suggest that the complete time-position trajectories are shown as the grey area

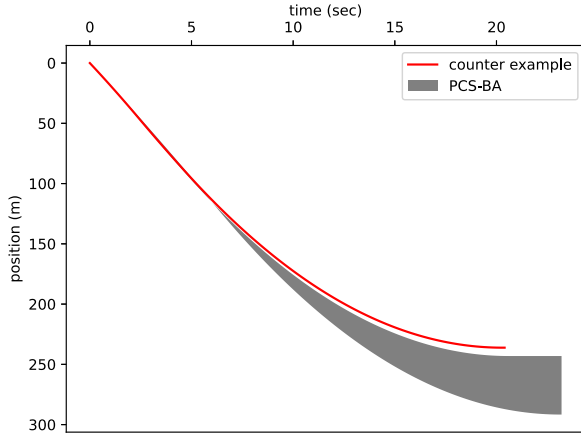


Fig. 5. Proof of Proposition 2.

in Fig. 5. However, there are possible operations where the train stops faster than the simulation results. For example, one counterexample is that the propulsion acceleration is  $0.75 \text{ m/sec}^2$ , the service brake acceleration is  $-0.5 \text{ m/sec}^2$ , and the time duration of the adjustment inhibition strategy is 7 control cycles. The TPT  $\vec{D}_o$  is indicated by the red line in Fig. 5. There exists  $T > 0$  such that  $\vec{D}(T)_o$  is smaller than any TPS in the grey area at the same time. If  $\hat{T} = 0$ , the counterexample  $\vec{D}_o$  does not exist. That is because the train has a constant deceleration in this case.  $\square$

### C. The Time-Position Space of the Following Train

The following train in the ROS model implements an emergency brake. Therefore, the time-position space of the following train can be predicted by using the boundary acceleration of the emergency brake. The worst case of establishing an emergency brake is the *safe braking model* [42], in which the braking process is divided into four components of (A) propulsion disabled, (B) coasting, (C) emergency brake building-up and (D) emergency brake at the guaranteed emergency brake rate (GEBR). The acceleration  $a_{fc}(t)$  of the following train at time  $t$  in the ROS model is

$$a_{fc}(t) \triangleq \begin{cases} a_f(0) + \int_0^t j_{dp}(\tau) d\tau & 0 \leq t < T_A \\ 0 & T_A \leq t < T_B \\ \int_0^t j_{eeb}(\tau) d\tau & T_B \leq t < T_C \\ a_{FT} & T_C \leq t < T_D \end{cases} \quad (7)$$

where  $a_f(0)$  ( $\text{m/sec}^2$ ) is the possible greatest acceleration at the last-known state of the following train;  $j_{dp}(\tau)$  ( $\text{m/sec}^3$ ) and  $j_{eeb}(\tau)$  ( $\text{m/sec}^3$ ) are the derivatives of the decelerations at time  $\tau$  while the propulsion is disabled and the emergency brake is activated, respectively;  $a_{FT}$  ( $\text{m/sec}^2$ ) is the GEBR of the following train; and  $T_A, T_B, T_C$  and  $T_D$  are the time points at the end of the four components, respectively. Note that the emergency brake acceleration  $a_{FT}$  of the following train is allowed to be different from the emergency brake acceleration  $a_{PT}$  of

the preceding train used in (6). Compared to the conventional RBS model, the ROS model as defined in (1) can guarantee collision-free with an arbitrary combination of emergency brake performances, e.g., the counter-example as shown in Fig. 3.

Let  $a_d(t)$  ( $\text{m/sec}^2$ ) be the additional acceleration at time  $t$  by unmodelled dynamics, such as the resistances of the aerodynamics, the grad and curve of the railway line and the rolling and bearing. The acceleration  $a_f(t)$  of the following train at time  $t$  is

$$a_f(t) \triangleq \begin{cases} a_{fc}(t) + a_d(t) & 0 \leq t < T_D \\ 0 & t \geq T_D \end{cases} \quad (8)$$

Let  $D(T_0)$  and  $\underline{a}_{FT}$  be the last-known TPS and the possible biggest emergency brake deceleration of the following train, respectively. The time-position space of the following train  $\mathcal{D}_f$  contains all complete TPT such as

$$\mathcal{D}_f \triangleq \{(D(T_0), \dots, D(T_N)) \mid \forall i \in [1, N] : D(T_i) \in [\vec{f}(D(T_{i-1}), \underline{a}_{FT}), \vec{f}(D(T_{i-1}), a_f(T_{i-1}))]\} \quad (9)$$

## V. PREDICTING THE TIME-POSITION SPACE OF THE PRECEDING TRAIN

As shown in proposition 2, the time-position space of the preceding train cannot be predicted with boundary values of the accelerations of the preceding train. To overcome this problem, we propose a *reachable set*-based approach, i.e., computing all reachable (possible) TPSs of the preceding train from its last-known state.

In our approach, the operation process of the preceding train is first formalised with a *parameterized hybrid automaton* (PHA). The automaton is then instantiated by evaluating the parameters according to the last-known TPS of the train and the related railway line data. We design a polytope-based algorithm to compute an over-approximation of the reachable set of the instantiated automaton. The reachable set of the automaton covers the time-position space of the train. Therefore, it can be used in the ROS model to guarantee collision-free.

### A. Parameterized Hybrid Automata

We briefly present basic notions regarding *parameterized hybrid automata* (PHA). A *dimension* of a system is the number of state variables. Given real numbers  $\mathbb{R}$ , the state of a dynamic system can be modelled by a vector in  $\mathbb{R}^n$ , where  $n$  is the dimension of the system. A *hybrid automaton* is a directed graph that specifies a system with discrete and continuous components. The edges of the graph denote discrete control switches, whereas the flows (ordinary differential equations, ODEs) associated with the vertices specify the continuous changes of states of the system. The parameterized hybrid automata is an extension of hybrid automata that introduces *parameters*, which are specific variables with constant values as the automaton operates.

*Definition 5 (Parameterized Hybrid Automata (PHA)):* A parameterized hybrid automaton consists of the following components:



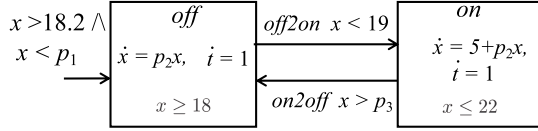


Fig. 6. Exmample of PHA modelling a thermostat.

- **Variables:** A finite set  $X \triangleq \{x_1, \dots, x_n\}$  of real-number variables. By  $\dot{X} \triangleq \{\dot{x}_1, \dots, \dot{x}_n\}$  we denote the set of first derivatives of the variables during a continuous change, and by  $X' \triangleq \{x'_1, \dots, x'_n\}$  we denote the set of values at the conclusion of a discrete change.
- **Parameters:** A finite set  $P \triangleq \{p_1, \dots, p_n\}$  of real-number parameters, where  $\forall p_i \in P : \dot{p}_i = 0$ .
- **Constraints:** A finite set  $\Phi \triangleq \{\varphi_1, \dots, \varphi_n\}$  of parametric linear constraints. A parametric constraint  $\varphi$  is constructed as follows, with  $x \in X$  and  $p \in P$ :  
 $\varphi ::= x < p \mid x = p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi$ .
- **Valuations:** A finite set  $\Omega \triangleq 2^{X \rightarrow \mathbb{R}}$  of variable valuations, each of which maps a variable to a real-number value.
- **Flows:** A finite set  $\mathcal{F}$  of flows. Each flow  $f(x)$  is an ODE containing variables in  $(X \cup \dot{X})$  and parameters in  $P$ .
- **Locations:** A finite set  $Q \triangleq \mathcal{N} \times 2^{\mathcal{F}} \times \Phi$  of locations. A location is labelled by a nominal in the set  $\mathcal{N}$ . The set contains the flows of continuous changes of variables in  $\mathcal{F}$  and an invariant from  $\Phi$ . An invariant constrains the legal values of a variable when the hybrid system is at a given location.
- **Initial:** An initial  $(\varphi_0, q_0) \in (\Phi \times Q)$  is a pair with the initial values of the variables and the initial location of the automaton.
- **Edges:** A finite set  $\Delta \triangleq Q \times \Phi \times 2^{\Omega(X)} \times Q$  of edges that represent the control switches of the system. The switch condition is a proposition expressed by a parametric constraint from  $\Phi$ . The possible discrete updates to a variable during control switches are subsets of the variable valuations in  $\Omega$ .

Fig. 6 illustrates a PHA of a thermostat. The variable  $x$  represents the temperature, and  $p_1$ ,  $p_2$  and  $p_3$  are parameters in the system. The system has two control modes *on* and *off*. The initial temperature is  $x \in (18.2, p_1)$ , and the temperature changes are specified by the derivatives of  $x$  within the respective locations. The constraints  $x < 19$  and  $x > p_3$  describe the translation conditions between control modes.

### B. Train Operation Model With PHA

The train operation is formalised with a PHA  $\mathcal{S}_H$  as shown in Fig. 7. The main notations of the automaton are listed in Table I.

The Locations of the automaton formalised the train control status as follows. Location *Tra* represents the train operating with propulsion. The flow at this location presents the dynamics governing the train position, speed, local time and global time. The constraint specifies that a train can remain at location *Tra* for at most  $\bar{k}_{TC}$  seconds according to the adjustment inhibition strategy (AIS). Furthermore, the global time of the system must be less than  $k_{\hat{T}}$  seconds according to the  $\hat{T}$ -FT principle, and the

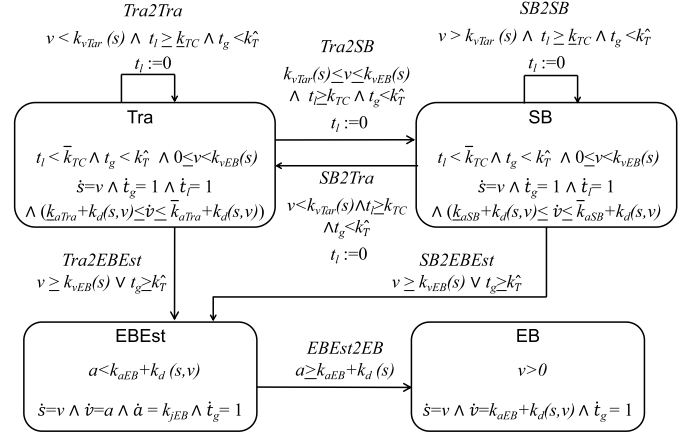


Fig. 7. Parameterized hybrid automaton of the train operation model.

TABLE I  
MAIN NOTATIONS

Notation	Explanation
<b>Location</b>	
Tra	Accelerating with a propulsion
SB	Decelerating with a service brake (SB)
EBEst	Emergency brake (EB) force being established
EB	Decelerating with an EB
<b>Variable</b>	
$s$	Train moving distance
$v$	Train speed
$a$	Train acceleration
$t_l$	Local time
$t_g$	Global time
<b>Parameter</b>	
$k_{\hat{T}}$	Time of the $\hat{T}$ -FT principle
$\bar{k}_{TC}$	Upper boundary of the time in the AIS
$\underline{k}_{TC}$	Lower boundary of the time in the AIS
$k_{vTar}(s)$	ATO target speed at position $s$
$k_{vEB}(s)$	EBI speed at position $s$
$\bar{k}_{aSB}$	Upper boundary of the acceleration of the SB
$\underline{k}_{aSB}$	Lower boundary of the acceleration of the SB
$\bar{k}_{aTra}$	Upper boundary of the acceleration of the propulsion
$\underline{k}_{aTra}$	Lower boundary of the acceleration of the propulsion
$k_{aEB}$	Acceleration of the EB
$k_{jEB}$	Derivative of the deceleration when establishing the EB
$k_d(s, v)$	Additional acceleration at position $s$ with speed $v$

train speed must be less than the EBI speed. Similarly, location *SB* represents the train control status of the service brake. The location *EBEst* models the behaviour when the emergency brake is established, where the derivative of the acceleration (jerk) is  $k_{jEB}$  (m/sec<sup>3</sup>). The train remains at that location until the acceleration reaches the maximal emergency brake rate  $k_{aEB}$  plus the additional acceleration. The location *EB* models the control status that the train operates with its maximal emergency braking rate.

The edges represent the discrete transitions between train controls. The edge between locations *Tra* and *SB* is crossed if the speed of the train is between the ATO target speed and the EBI speed, the local time is greater than or equal to  $\underline{k}_{TC}$  seconds, or the global time is less than  $k_{\hat{T}}$  seconds. The discrete variable update  $t_l := 0$  specifies that the local clock is reset



after the transition. If the local time is greater than or equal to  $k_{TC}$  seconds but the train speed is still less than the ATO target speed, a self-transition is triggered at location  $Tra$  to maintain the propulsion. If the speed of the train is greater than or equal to the EBI speed or the global time is greater than  $k_{\hat{T}}$  seconds, the emergency brake is initiated by transitioning to location  $EBEst$ . The edge between locations  $EBEst$  and  $EB$  specifies that the emergency brake has been established. There is the transition out of location  $EB$  because once the emergency brake has been activated, it cannot be released until the train fully stops. Uncertainties of flows and switch conditions in the automaton represent unmodelled dynamics and parameters mismatched in train operations.

The PHA  $S_H$  models the behaviour of the preceding train within a two-train convoy. The operation of the train is only affected by the movement authority and line speed restrictions. When a convoy has more than two trains, the operations of the preceding trains are more complicated because they are additionally affected by their preceding trains.

### C. Reachable Set Computation of the Train Operation Model

The train operation model has 5 dimensions. A *train operation state* (TOS) is defined as a vector  $\sigma \triangleq (s, v, a, t_l, t_g)$  from the set  $\mathbb{R}^5$ , where  $s, v, a, t_l$  and  $t_g$  represent the train position, train speed, train acceleration, local time and global time, respectively. A TOS represents a TPS of a train and changes according to the following rules for the PHA  $H$  as shown in Fig. 7.

- 1) Discrete change: an edge instantaneously changes the control mode and variable values.
- 2) Continuous change: the variable values change continuously according to the flow of a location.

A path of the hybrid automaton  $H$  represents a TPT of a train modelled by  $H$ ; this path is a possible evolution of the TOS over time. By  $\mathfrak{w}$  we denote a finite path of TOSs, i.e.,  $\mathfrak{w} \triangleq \sigma_0 \sigma_1 \dots \sigma_n$ . With any  $i \geq 0$  the relation between  $\sigma_{i+1}$  and  $\sigma_i$  follows one of the above two rules. We define  $\mathbf{State}(\mathfrak{w})$  as *all* TOSs appearing in  $\mathfrak{w}$ . A path  $\mathfrak{w}$  *reaches* a TOS  $\sigma$  if and only if  $\sigma \in \mathbf{State}(\mathfrak{w})$ . Let  $\mathbf{Path}(H)$  be *all* possible paths of the hybrid automaton  $H$ . The reachable set of  $H$  is defined as follows.

**Definition 6 (Reachable Set):** Given a hybrid automaton that represents train operations, the reachable set  $\mathcal{R}(H)$  of TOSs is the set such that:

$$\mathcal{R}(H) \triangleq \left\{ \sigma \mid \sigma \in \bigcup_{\mathfrak{w} \in \mathbf{Path}(H)} \mathbf{State}(\mathfrak{w}) \right\}$$

Although the reachability problem of hybrid automata is undecidable in general [43], various convex models have been proposed to represent a segment of the reachable set of a hybrid automaton [44] [32] [45]. Due to the dynamic part of train operations being linear, we use polytopes to represent TOSs of  $H$ . An algorithm to compute an over-approximation of the reachable set of  $H$  is as follows.

**Definition 7 (Generator):** Given a TOS  $\mathbf{c} \in \mathbb{R}^5$ , a generator  $\mathbf{g}(\mathbf{c}, \mathbf{f}, \Delta T) \in \mathbb{R}^5$  yields a new the TOS  $\mathbf{c}'$  according to a flow condition  $\mathbf{f}$  within a time interval  $\Delta T$ .

A generator  $\mathbf{g}(\mathbf{c}, \mathbf{f}, \Delta T) \in \mathbb{R}^5$  changes  $\mathbf{c}$  by solving the ODE  $\dot{\mathbf{c}} = \mathbf{f}$ . Let flows  $\underline{\mathbf{f}}$  and  $\overline{\mathbf{f}}$  be the slowest and fastest changes of the TOSs within a location, respectively. As a result, generators  $\underline{\mathbf{g}} \triangleq \mathbf{g}(\mathbf{c}, \underline{\mathbf{f}}, \Delta T)$  and  $\overline{\mathbf{g}} \triangleq \mathbf{g}(\mathbf{c}, \overline{\mathbf{f}}, \Delta T)$  can be obtained. Given a vector  $\mathcal{C} \triangleq [\underline{\mathbf{c}}, \overline{\mathbf{c}}]$  of a TOS and generators  $\mathcal{G} \triangleq [\underline{\mathbf{g}}, \overline{\mathbf{g}}]$ , we define a *vector evolution function*  $\mathcal{B}(\mathcal{C}, \mathcal{G}) = \{\mathcal{C}_1, \mathcal{C}_2\}$  with  $\mathcal{C}_1 = [\underline{\mathbf{c}}_1, \overline{\mathbf{c}}_1]$  and  $\mathcal{C}_2 = [\underline{\mathbf{c}}_2, \overline{\mathbf{c}}_2]$  as follows, where additions are made with the regular vector addition manner.

- Case 1:  $\underline{v} \leq \overline{v}$  and  $\underline{s} < \overline{s}$ :

$$\overline{\mathbf{c}}_1 = \overline{\mathbf{c}} + \overline{\mathbf{g}} \quad (10a)$$

$$\underline{\mathbf{c}}_1 = \underline{\mathbf{c}}_2 = \overline{\mathbf{c}} + \underline{\mathbf{g}} \quad (10b)$$

$$\underline{\mathbf{c}}_2 = \underline{\mathbf{c}} + \underline{\mathbf{g}} \quad (10c)$$

- Case 2:  $\underline{v} > \overline{v}$  and  $\underline{s} \leq \overline{s}$ :

$$\overline{\mathbf{c}}_1 = \overline{\mathbf{c}} + \overline{\mathbf{g}} \quad (11a)$$

$$\underline{\mathbf{c}}_1 = \overline{\mathbf{c}}_2 = \underline{\mathbf{c}} + \overline{\mathbf{g}} \quad (11b)$$

$$\underline{\mathbf{c}}_2 = \underline{\mathbf{c}} + \underline{\mathbf{g}} \quad (11c)$$

- Case 3:  $\underline{v} = \overline{v}$  and  $\underline{s} = \overline{s}$ :

$$\overline{\mathbf{c}}_1 = \overline{\mathbf{c}}_2 = \overline{\mathbf{c}} + \overline{\mathbf{g}} \quad (12a)$$

$$\underline{\mathbf{c}}_1 = \underline{\mathbf{c}}_2 = \underline{\mathbf{c}} + \underline{\mathbf{g}} \quad (12b)$$

By  $\llbracket \mathbf{x}, \mathbf{x}' \rrbracket$  we denote the set of all points in vector  $[\mathbf{x}, \mathbf{x}']$ . The polytope representing an over-approximation of the reachable set of TOSs is defined as follows.

**Definition 8 (Polytope of TOSs):** Given a vector  $\mathcal{C} = [\underline{\mathbf{c}}, \overline{\mathbf{c}}]$ , generators  $\mathcal{G} = [\underline{\mathbf{g}}, \overline{\mathbf{g}}]$ , and  $\mathcal{C}_1$  and  $\mathcal{C}_2$  obtained by solving  $\mathcal{B}(\mathcal{C}, \mathcal{G}) = \{\mathcal{C}_1, \mathcal{C}_2\}$ , a polytope of TOSs  $\mathcal{P}(\mathcal{C}, \mathcal{G})$  is a set such that:

$$\mathcal{P}(\mathcal{C}, \mathcal{G}) \triangleq \{ \mathbf{x} \in \mathbb{R}^5 \mid \mathbf{x} = \mathbf{c} + \alpha \mathbf{c}', \mathbf{c} \in \llbracket \mathcal{C} \rrbracket, \alpha \in [0, 1], \mathbf{c}' \in \llbracket \mathcal{C}_1 \rrbracket \cup \llbracket \mathcal{C}_2 \rrbracket \} \quad (13)$$

Based on the initial TOS  $\mathbf{c}_0$  and a location  $q$  representing the initial train control status, the reachable set of TOSs can be computed with Algorithm 1. This algorithm can terminate because  $H$  inevitably translates into location  $EB$  after  $\hat{T}$  seconds and the variable  $v$  eventually decreases to 0.

According to the definitions, if the parameters of the PHA  $H$  cover possible concrete data of train dynamics and railway lines, then the reachable set of  $H$  represents a superset of the time-position space of the train. Therefore, the automaton is *reachset conformance* to the real train control system, i.e., a possible TPT from an arbitrary TPS of the train is in the reachable set of  $H$  [46].

### D. Computing the Following Train EBI by the Reachable Sets

In virtual coupling, the ATP of the following train uses the ROS model to compute the EBI speed, which is further used as the speed constraint by the ATO.

Let  $\mathcal{R}_p$  be the reachable set of the TOSs of the preceding train within the ROS model. The EBI speed of the following train is computed according to the worst-case of the TOSs  $\Sigma_{pw}$  of the

**Algorithm 1:** Reachable Set Computation for TOSs.

---

**Input:** initial TOS  $\mathbf{c}_0 = (s_0, v_0, a_0, t_{l0}, t_{g0})$ ; initial location  $q$  with flow  $\bar{f}$  and guard  $\varphi$ ; and time interval  $\Delta T$

**Output:** Reachable Set of TOSs  $\mathcal{R}$

```

1 foreach  $(\mathcal{C}, q) \in \mathcal{D} : \exists \mathbf{c} \in \llbracket \mathcal{C} \rrbracket : v > 0$  do
2    $\mathcal{G} \leftarrow (\mathbf{g}(\mathbf{c}, \bar{f}, \Delta T), \mathbf{g}(\mathbf{c}, \bar{f}, \Delta T))$ ;
3    $\mathcal{C} \leftarrow (\mathbf{c}, \mathbf{c})$ ;
4    $\mathcal{R} \leftarrow \mathcal{R} \cup (\mathcal{P}(\mathcal{C}, \mathcal{G}) \cap \mathcal{R}(\varphi))$ ; //  $\mathcal{R}(\varphi)$  is the
      set of all TOS satisfying guard
       $\varphi$  of location  $q$ 
5    $\mathcal{D} \leftarrow \mathcal{D} \cup ((\mathcal{B}(\mathcal{C}, \mathcal{G}) \cap \mathcal{R}(\varphi)) \times \{q\})$ ; //  $\mathcal{D}$  is a
      set of pairs of a vector
      satisfying  $\varphi$  and the location
      belongs to  $\varphi$ 
6   if  $\mathcal{P}(\mathcal{C}, \mathcal{G}) \not\subset \mathcal{R}(\varphi)$  // if evolutions of
      TOSs trigger a transition
7     then
8        $\mathcal{C}' \leftarrow [\mathbf{p}_1, \mathbf{p}_2]$ ; //  $\mathbf{p}_1$  and  $\mathbf{p}_2$  are
          crosspoints of  $\mathcal{P}(\mathcal{C}, \mathcal{G})$  and
           $\mathcal{R}(\varphi)$ , which can be obtained
          by, e.g., a standard
          traversal algorithm.
9        $\mathcal{D} \leftarrow \mathcal{D} \cup \{(\mathcal{C}', q')\}$ ; //  $q'$  is the target
          location
10    end
11 end
12 return  $\mathcal{R}$ 

```

---

preceding train as follows:

$$\Sigma_{pw} \triangleq \{(s_i, t_i) \in \mathcal{R} \mid \forall (s, t_i) \in \mathcal{R} \text{ s.t. } s_i \leq s\} \quad (14)$$

Let  $\mathcal{R}_f(v)$  be the reachable set of the following train with the initial train speed  $v$ . The EBI speed  $v_f$  of the following train is the maximal speed such that there is no TOSs in the  $\mathcal{R}_p$  and  $\mathcal{R}_f(v)$  indicating the trains collide, i.e.,

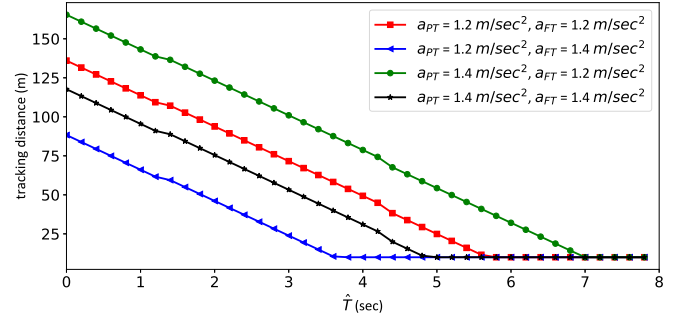
$$\begin{aligned} v_f &= \max V \text{ s.t.} \\ V &= \{v \mid \forall (s_p, t_{i_p}) \in \Sigma_{pw} \text{ and } (s_f, t_{i_f}) \in \mathcal{R}_f(v) \\ &\quad \text{s.t. } (t_{i_p} = t_{i_f}) \Rightarrow (s_f \leq s_p)\} \end{aligned} \quad (15)$$

A switch in the ROS model is treated as a special ‘‘preceding train’’ whose speed is always 0. If the nearest obstacle of the following train is a switch, e.g., during joint manoeuvres, the worst-case TOSs  $\Sigma_{pw}$  of the ‘‘preceding train’’ equals  $\{(S_{swi}, t_i)\}$  with  $S_{swi}$  being a constant value of switch position. A speed margin between the ATO target and EBI speeds must be considered to avoid emergency brakes triggered by control overshoots.

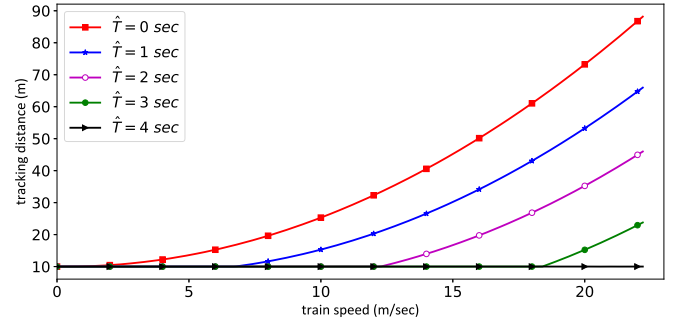
## VI. NUMERICAL EXPERIMENTS WITH CASE STUDIES

### A. Performance of the ROS Model

We first evaluate several fundamental aspects of the proposed approach with a basic scenario. In this scenario, the virtually



(a) Safe Distances at a speed of 22.22 m/sec.



(b) Safe distances with  $a_{PT} = 1.2 \text{ m/sec}^2$  and  $a_{FT} = 1.4 \text{ m/sec}^2$

Fig. 8. Safe Distances concerning parameters of the ROS model.

coupled trains operate on a straight track with a slope of 0 and a speed limitation of 23 m/sec; the safety margin is  $S_m = 10 \text{ m}$ .

1) *Influence of the Value of  $\hat{T}$* : Several simulations are run to analyse the minimal safety operation distances between two trains following the  $\hat{T}$ -FT principle. Since it is more challenging to have a long fault tolerance time in train controls, we consider the *optimal value* of  $\hat{T}$ , which is the time when the safe tracking distance is equal to the safety margin.

The safe tracking distances for different values of  $\hat{T}$  with various emergency brake configurations are shown in Fig. 8(a). The figure shows that  $\hat{T}$  has a smaller optimal value if the following train has a better brake performance. In contrast,  $\hat{T}$  has a bigger optimal value if the preceding train has a better brake performance. If the two trains have the same brake performance, the optimal value of  $\hat{T}$  is between these two situations.

2) *Safe Distances Concerning Train Speed*: We analyse the safe tracking distances between virtually coupled trains at different speeds. The  $\hat{T}$  values are 0 to 4 seconds in these simulations.

When  $\hat{T}$  is 4 seconds, the tracking distance is a constant value of 10 m according to the predefined safety margin, the minimal possible safe tracking distance in our simulation model. When  $\hat{T}$  is less than 4 seconds, the tracking distances progressively increase with increasing train speed. When  $\hat{T}$  is greater than 4 seconds, the safe tracking distance equals the safety margin of the trains with the greater speed. These results are shown in Fig. 8(b).

3) *Efficiency of the Reachable Set Computation*: We analyse the efficiency of the reachable set computation algorithm with

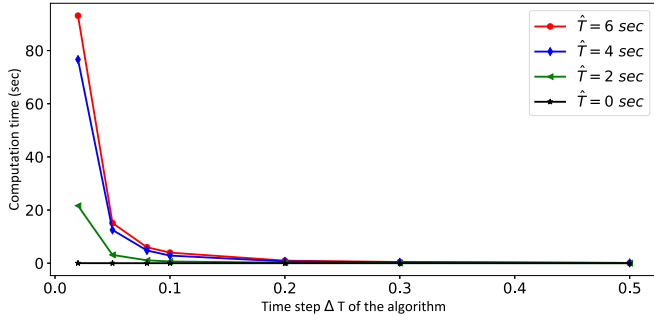
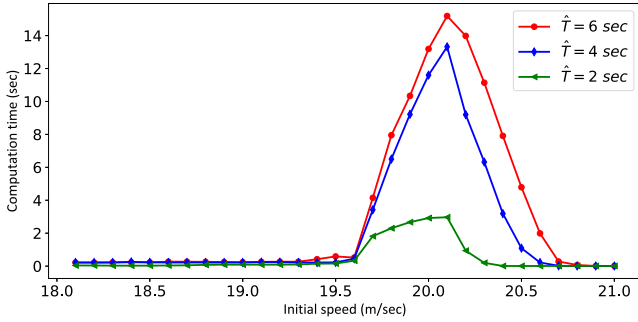

 (a) Efficiency of the algorithm with with respect to  $\Delta t$  with  $v_0 = 20$  m/s.

 (b) Efficiency of the algorithm with respect to  $v_0$  with  $\Delta t = 0.05$ .

Fig. 9. Efficiency of the reachable set computation algorithm.

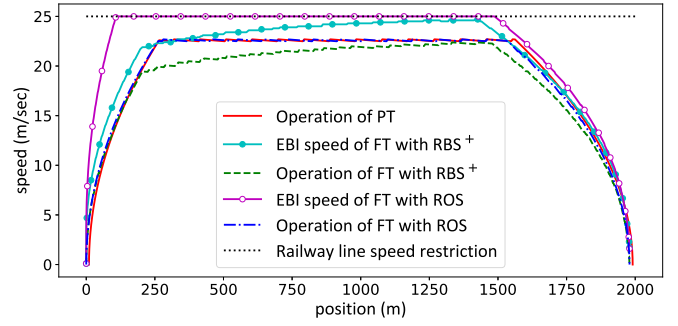
different values of  $\hat{T}$ ,  $\Delta T$  and initial train speed. In these simulations, the ATO target speed is 20 m/sec.

The computation of the reachable set requires more time with a shorter time step  $\Delta T$  or a larger value of  $\hat{T}$ . With a smaller value of  $\Delta t$ , a more accurate reachable set can be obtained; with a larger value of  $\hat{T}$ , a shorter tracking distance can be achieved. Furthermore, the computation of the algorithm requires more time when the initial train speed is between 19.5 m/sec and 20.5 m/sec. This result occurs because the control system has more control switches at these initial train speeds. These results are shown in Fig. 9. We choose  $\Delta T = 0.1$  because this value balances reasonable computational efficiency and accuracy.

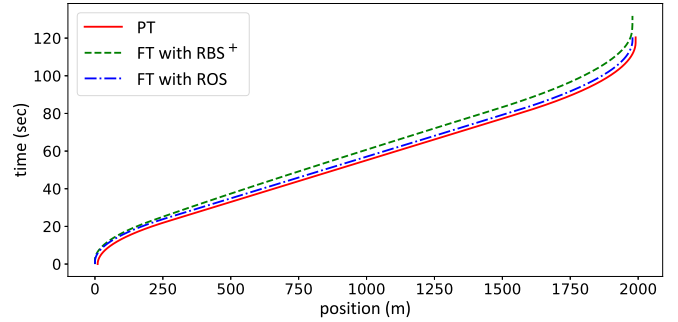
### B. Typical Metro Line Simulation Environment

The ROS model is to reduce the safe distance between trains without compromising safety. The state-of-the-art train separation method in railways is the relative brake distance model. To guarantee collision-free, a standard RBS model restricts that the tracked trains either have the same emergency braking performance [5] or follow a specific braking performance manoeuvre [24]. Zhao et al. proposed a general version of the RBS model that allows tracked trains to have an arbitrary combination of emergency braking performance [4]. Instead of considering the braking distances of the trains, their model uses the whole time-position trajectories of the trains to compute safe distances. By RBS<sup>+</sup> we denote Zhao's model for comparisons in the rest of the paper.

We analyse two distinct segments of a metro railway line. In Segment I (SI), the speed limit between two adjacent stations



(a) Speed-position trajectories



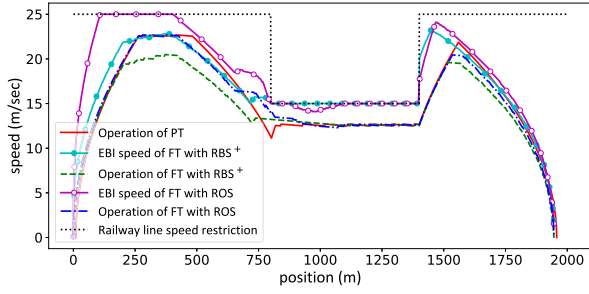
(b) Comparison of time-position trajectories

Fig. 10. Operations of virtually coupled trains on SI.

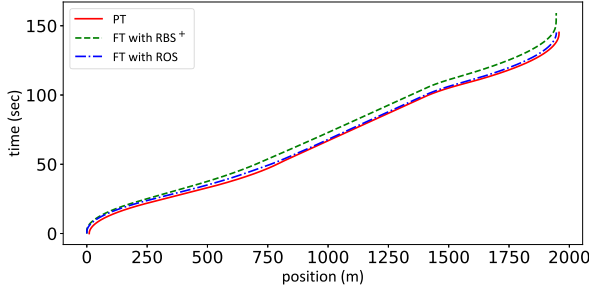
is a constant value of 25 m/sec, and the slope of the line is 16%. Segment II (SII) has a railway section between positions 800 m and 1400 m with a lower speed limitation of 15 m/sec. The speed limitation of the rest of the segment is 25 m/sec. The two segments have the same length.

1) *Performance of Train Operations:* The initial distance between the trains is the safety margin  $S_m$  in the simulations. Figs. 10 and 11 show SI and SII simulation results, respectively. In Figs. 10(a) and 11(a), one can see how the tracked trains can have a more consistent speed with the ROS model in test conditions. If the following train uses the RBS<sup>+</sup> model in its ATP, the EBI speed is affected by the speed of the preceding train. The EBI speed of the following train increases slowly with the speed of the preceding train. As the ATO target speed must be lower than the EBI speed, the speed of the following train is difficult to consistent with the preceding train. With the ROS model, the EBI speed of the following train is not restricted by the speed of the preceding train. It can quickly reach the highest permitted speed of the railway line. The ATO controller of the following train has a greater speed adjustment window. As a result, the speed of the following train is more consistent with the preceding train. The distances between the trains with the two models are shown in Figs. 10(b) and 11(b). The ROS model allows the virtually coupled trains to maintain a stable formation and arrive simultaneously at the next railway station. The comparisons of speed differences and the distances between the tracked trains are shown in Fig. 12.

2) *String Stability:* String stability is an important problem in virtual coupling. By  $(s_R(t), v_R(t))$  we denote a constant



(a) Speed-position trajectories



(b) Time-position trajectories

Fig. 11. Operations of virtually coupled trains on SII.

reference trajectory tracked by the preceding train. Let  $(s_L(t), v_L(t))$  and  $(s_F(t), v_F(t))$  be the trajectories of the preceding train and the following train, respectively. According to [24] and [47], string stability can be defined as follows. For a step change in the speed  $v_L$  of the leading train at time  $t = 0$ , a train platoon can be said lead-follower string stable if there exists a constant  $\alpha \in (0, 1)$  such that

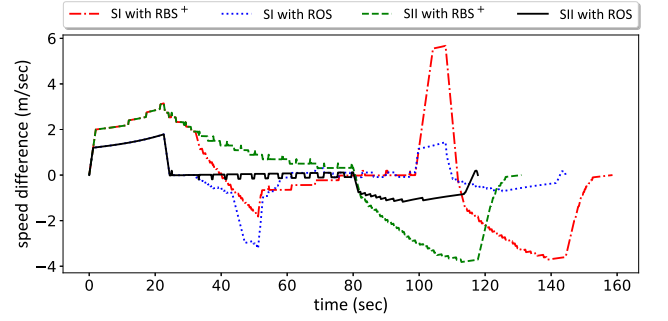
$$\max_{t \geq 0} |s_F(t) - s_R(t) + S_{sep}| \leq \alpha \max_{t \geq 0} |s_L(t) - s_R(t)| \quad (16)$$

where  $S_{sep}$  is the desired separation distance between trains.

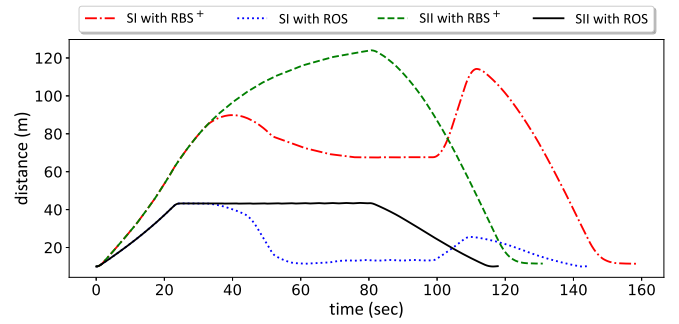
Given  $\Delta S(t) = \frac{|s_F(t) - s_R(t) + S_{sep}|}{|s_L(t) - s_R(t)|}$ , if  $\Delta S(t) < 1$  for all  $t > 0$ , then an  $\alpha \in (0, 1)$  in (16) exists and the train platoon is string stable. A desired separation distance  $S_{sep}$  between trains must be greater than the safe distance to guarantee collision-free. Due to the proposed ROS model providing a smaller safe distance than the RBS<sup>+</sup> model, the string stable can be held with a smaller desired separation distance. As illustrated in Fig. 13, a platoon with the ROS model is string stable with desired separation distance  $S_{sep} = 20$  m. However, the string stable does not hold for this desired separation distance with the RBS<sup>+</sup> model because there exists some  $t$  such that  $\Delta S(t) > 1$ . The platoon is string stable with the RBS<sup>+</sup> model when  $S_{sep} \geq 93$  m.

### C. Real Metro Line Simulation Environment

We validate the proposed ROS model on a simulation platform developed using the digital twin techniques. This platform models a real-world physical asset of the Chengdu No. 8 metro line in China. The operation of the preceding train uses actual



(a) Speed difference



(b) Distances

Fig. 12. Speed differences and distances of two virtually coupled trains.

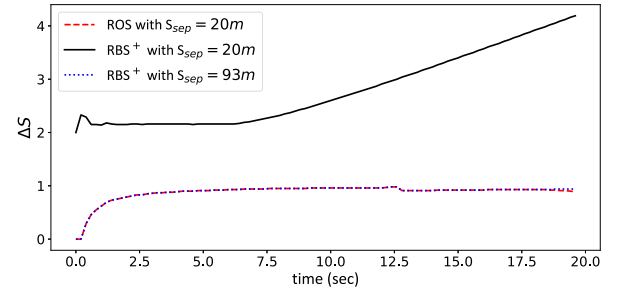


Fig. 13. String stability of a train platoon, where the initial speed of the platoon is 22 m/sec.

data of the trains running on the railway line. The following train in the platform is modelled digitally. The ATP of the following train applies the ROS model and its comparisons to compute the EBI speed. The ATO regulates and controls the train speed accordingly.

In the simulations, the initial speed of both trains is 0 m/sec, and the initial distance between the trains is a safety margin  $S_m = 10$  metres. The dwell time of the virtual coupling in every station is 30 seconds. The first-stopped train can only depart after the second-stopped train has stopped 30 seconds in a station.

Fig. 14(a) and (b) show the differences in train movements between the two train separation models. It appears to have



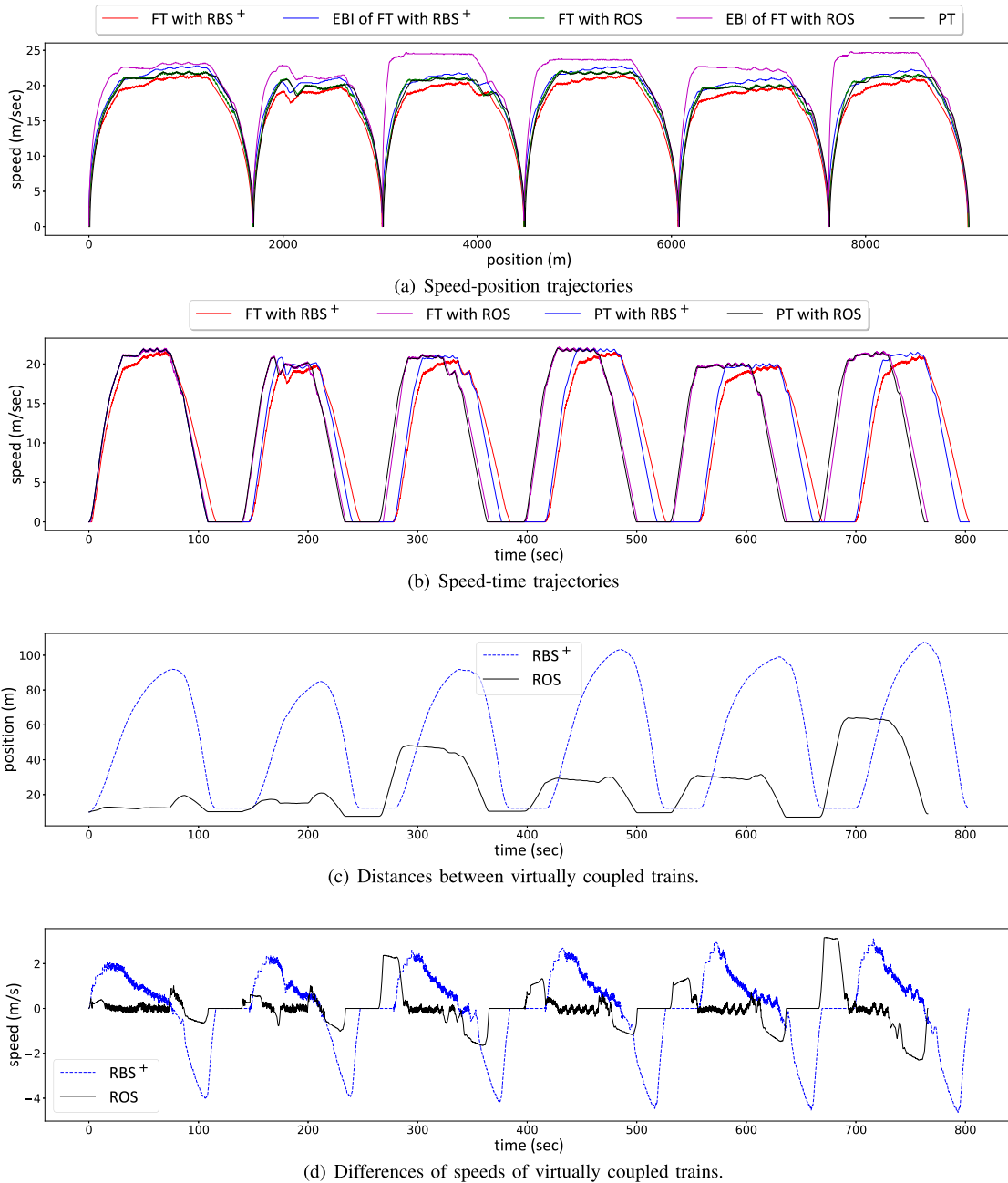


Fig. 14. Comparisons of the different train separation models.

distinctive train operation trajectories with the ROS and conventional RBS<sup>+</sup> models. Fig. 14(a) demonstrates that ROS provides a higher EBI speed for the following train. Therefore, the model maintains a much more consistent speed between trains. Fig. 14(b) shows that due to having a lower EBI speed and a bigger speed difference using the RBS<sup>+</sup> model, the following train arrives significantly later at the stations than the preceding train. This disadvantage does not appear in the ROS model, where the following train has a high enough EBI speed. Consequently, the following train has a consistent speed with the preceding train. The trains arrive almost simultaneously at the stations.

Fig. 14(c) shows the distances between the trains with ROS and RBS<sup>+</sup>, whereas Fig. 14(d) presents the speed differences

between the trains. The results show that when using the ROS model in the following train, the tracked trains have more consistent speeds and closer distances during virtual coupling operations without compromising safety. The ROS model could be beneficial for increasing the capacity of the railway line. The total operation time within the six tested railway sections is 803.4 seconds with the RBS<sup>+</sup> model. In contrast, the ROS model reduces the operation time to 765.6 seconds. The operation time of a non-virtual coupling train (i.e., a conventional CBTC train) within these sections is 761.6 seconds. A train platoon with the RBS<sup>+</sup> model gives an extra operation time of 41.8 seconds due to the speed inconsistency of the trains. This time significantly drops to 3.9 seconds by using the ROS model. The ROS model

brings us a considerable 90.7% decrease in unnecessary extra waiting time and a 4.9% increase in the line capacity.<sup>1</sup>

## VII. CONCLUSION

This article presented a relative operation-based train separation (ROS) model for virtual coupling. The model applied a  $\hat{T}$ -FT principle, according to which the preceding train normally operated for  $\hat{T}$  seconds before initiating an emergency brake. The reachable set-based method was applied to predict the boundary of time-position trajectories of the preceding train in the ROS model. The train operation was formalized with a parameterized hybrid automaton, with the train accelerations and control switching conditions specified by parameters. A polytope-based algorithm was developed for computing the reachable set of the parameterized hybrid train operation model. Various simulations were designed, and the results of different train separation models were compared. The results showed that larger values of  $\hat{T}$  allowed higher EBI speeds and significantly shorter distances between trains. This result validated that the ROS model significantly reduced unnecessary waiting time when virtually coupled trains arrived at a station and improved the capacity of railway lines.

Several interesting topics can be investigated in future work. First, a bigger value of fault-tolerant time increases the risk of train operations. As the value of  $\hat{T}$  is significant for improving the virtual coupling performance, reducing risks with a long prediction time without activating the emergency brake is an important issue. Secondly, when considering a convoy with more than two trains, the normal operation phases of the preceding trains are more complicated. It is worth investigating how to model their behaviours and compute the boundaries of time-position trajectories. Finally, local and string stabilities of virtual coupling with advanced control methods, such as MPC and its extensions, using the ROS model is still an ongoing research topic.

## REFERENCES

- [1] E. Quaglietta, M. Wang, and R. M. Goverde, "A multi-state train-following model for the analysis of virtual coupling railway operations," *J. Rail Transp. Plan. Manage.*, vol. 15, 2020, Art. no. 100195.
- [2] J. Yin, T. Tang, L. Yang, J. Xun, Y. Huang, and Z. Gao, "Research and development of automatic train operation for railway transportation systems: A survey," *Transp. Res. Part C: Emerg. Technol.*, vol. 85, pp. 548–572, 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0968090X17302498>
- [3] J. Ligthart, E. Semsar-Kazerooni, J. Ploeg, M. Alirezaei, and H. Nijmeijer, "Controller design for cooperative driving with guaranteed safe behavior," in *Proc. IEEE Conf. Control Technol. Appl.*, 2018, pp. 1460–1465.
- [4] Y. Zhao and P. Ioannou, "Positive train control with dynamic headway based on an active communication system," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 3095–3103, Dec. 2015.
- [5] J. Pachel, *Railway signalling principles*. Braunschweig, Germany, 2020.
- [6] M. Althoff, S. Maierhofer, and C. Pek, "Provably-correct and comfortable adaptive cruise control," *IEEE Trans. Intell. Veh.*, vol. 6, no. 1, pp. 159–174, Mar. 2021.
- [7] Y. Cao, Z. Zhang, F. Cheng, and S. Su, "Trajectory optimization for high-speed trains via a mixed integer linear programming approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 17666–17676, Oct. 2022.
- [8] S. Su, Q. Zhu, J. Liu, T. Tang, Q. Wei, and Y. Cao, "A data-driven iterative learning approach for optimizing the train control strategy," *IEEE Trans. Ind. Inform.*, vol. 19, no. 7, pp. 7885–7893, Jul. 2023.
- [9] Q. Zhu, S. Su, T. Tang, W. Liu, Z. Zhang, and Q. Tian, "An eco-driving algorithm for trains through distributing energy: A Q-learning approach," *ISA Trans.*, vol. 122, pp. 24–37, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0019057821002330>
- [10] Y. Liu, Y. Zhou, S. Su, J. Xun, and T. Tang, "Control strategy for stable formation of high-speed virtually coupled trains with disturbances and delays," *Comput.-Aided Civil Infrastructure Eng.*, vol. 38, no. 5, pp. 621–639, 2023. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/mice.12873>
- [11] J. Yin, L. Yang, A. D'Ariano, T. Tang, and Z. Gao, "Integrated backup rolling stock allocation and timetable rescheduling with uncertain time-variant passenger demand under disruptive events," *INFORMS J. Comput.*, vol. 34, no. 6, pp. 3234–3258, 2022.
- [12] J. Yin, X. Ren, S. Su, F. Yan, and T. Tao, "Resilience-oriented train rescheduling optimization in railway networks: A mixed integer programming approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 4948–4961, May 2023.
- [13] U. Bock and G. Blikker, "Design and Development of a Future Freight Train Concept - 'Virtually coupled train formations,'" in *IFAC Proc. Volumes*, vol. 33, no. 9, pp. 395–400, 2000.
- [14] S. Chai, J. Yin, A. D'Ariano, M. Samà, and T. Tang, "Scheduling of coupled train platoons for metro networks: A passenger demand-oriented approach," *Transp. Res. Rec.*, vol. 2677, no. 2, pp. 1671–1689, 2023. [Online]. Available: <https://doi.org/10.1177/03611981221109175>
- [15] S. Su, J. She, K. Li, X. Wang, and Y. Zhou, "A nonlinear safety equilibrium spacing-based model predictive control for virtually coupled train set over gradient terrains," *IEEE Trans. Transp. Electrification*, vol. 8, no. 2, pp. 2810–2824, Jun. 2022.
- [16] J. Felez, Y. Kim, and F. Borrelli, "A model predictive control approach for virtual coupling in railways," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 7, pp. 2728–2739, Jul. 2019.
- [17] M. A. Vaquero-Serrano and J. Felez, "A decentralized robust control approach for virtually coupled train sets," *Comput.-Aided Civil Infrastructure Eng.*, 2023. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/mice.12985>
- [18] C. Di Meo, M. Di Vaio, F. Flammini, R. Nardone, S. Santini, and V. Vittorini, "ERTMS/ETCS virtual coupling: Proof of concept and numerical analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2545–2556, Jun. 2020.
- [19] J. Park, B.-H. Lee, and Y. Eun, "Virtual coupling of railway vehicles: Gap reference for merge and separation, robust control, and position measurement," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1085–1096, Feb. 2022.
- [20] Y. Liu, R. Liu, C. Wei, J. Xun, and T. Tang, "Distributed model predictive control strategy for constrained high-speed virtually coupled train set," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 171–183, Jan. 2022.
- [21] X. Luo, T. Tang, J. Yin, and H. Liu, "A robust MPC approach with controller tuning for close following operation of virtually coupled train set," *Transp. Res. Part C: Emerg. Technol.*, vol. 151, 2023, Art. no. 104116. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0968090X23001055>
- [22] B. Ning, "Absolute braking and relative distance braking-train operation control modes in moving block systems," *WIT Trans. Built Environ.*, vol. 37, pp. 991–1001, 1998.
- [23] E. Quaglietta, P. Spartalis, M. Wang, R. M. Goverde, and P. van Koningsbruggen, "Modelling and analysis of virtual coupling with dynamic safety margin considering risk factors in railway operations," *J. Rail Transport Plan. Manage.*, vol. 22, 2022, Art. no. 100313.
- [24] S. Su, J. She, D. Wang, S. Gong, and Y. Zhou, "A stabilized virtual coupling scheme for a train set with heterogeneous braking dynamics capability," *Transp. Res. Part C: Emerg. Technol.*, vol. 146, 2023, Art. no. 103947. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0968090X22003606>
- [25] S. Su, W. Liu, Q. Zhu, R. Li, T. Tang, and J. Lv, "A cooperative collision-avoidance control methodology for virtual coupling trains," *Accident Anal. Prevention*, vol. 173, 2022, Art. no. 106703. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0001457522001397>
- [26] Y. Huang, J. Du, Z. Yang, Z. Zhou, L. Zhang, and H. Chen, "A survey on trajectory-prediction methods for autonomous driving," *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 652–674, Sep. 2022.

<sup>1</sup>In this case, we consider the railway line capacity to be the cycle time [48].

- [27] Y. Zhang, H. Wang, P. James, M. Roggenbach, and D. Tian, "A train protection logic based on topological manifolds for virtual coupling," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11930–11945, Aug. 2022.
- [28] M. Chai, H. Wang, T. Tang, and H. Liu, "Runtime verification of train control systems with parameterized modal live sequence charts," *J. Syst. Softw.*, vol. 177, 2021, Art. no. 110962. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0164121221000595>
- [29] T. A. Henzinger, "The theory of hybrid automata," in *Verification of Digital and Hybrid Systems*, M. K. Inan and R. P. Kurshan, Eds. Berlin, Germany: Springer, 2000, pp. 265–292.
- [30] A. Girard and C. Le Guernic, "Zonotope/Hyperplane intersection for hybrid systems reachability analysis," in *Hybrid Systems: Computation and Control*, M. Egerstedt and B. Mishra, Eds. Berlin, Germany: Springer, 2008, pp. 215–228.
- [31] N. Kochdumper and M. Althoff, "Reachability analysis for hybrid systems with nonlinear guard sets," in *Proc. 23rd Int. Conf. Hybrid Syst.: Comput. Control*, 2020, pp. 1–10.
- [32] N. Ramdani, N. Meslem, and Y. Candau, "Computing reachable sets for uncertain nonlinear monotone systems," *Nonlinear Anal.: Hybrid Syst.*, vol. 4, no. 2, pp. 263–278, 2010. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1751570X09001198>
- [33] M. Althoff, O. Stursberg, and M. Buss, "Model-based probabilistic collision detection in autonomous driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 2, pp. 299–310, Jun. 2009.
- [34] N. Malone, H.-T. Chiang, K. Lesser, M. Oishi, and L. Tapia, "Hybrid dynamic moving obstacle avoidance using a stochastic reachable set-based potential field," *IEEE Trans. Robot.*, vol. 33, no. 5, pp. 1124–1138, Oct. 2017.
- [35] Y. Lin and S. Saripalli, "Collision avoidance for UAVs using reachable sets," in *Proc. IEEE Int. Conf. Unmanned Aircr. Syst.*, 2015, pp. 226–235.
- [36] Y. Zhou and J. S. Baras, "Reachable set approach to collision avoidance for UAVs," in *Proc. IEEE 54th Conf. Decis. Control*, 2015, pp. 5947–5952.
- [37] S. Sontges, M. Koschi, and M. Althoff, "Worst-case analysis of the time-to-react using reachable sets," in *Proc. IEEE Intell. Veh. Symp.*, 2018, pp. 1891–1897.
- [38] S. M. Loos, D. Witmer, P. Steenkiste, and A. Platzer, "Efficiency analysis of formally verified adaptive cruise controllers," in *Proc. IEEE 16th Int. Conf. Intell. Transp. Syst.*, 2013, pp. 1565–1570.
- [39] O. Stursberg, A. Fehnker, Z. Han, and B. H. Krogh, "Verification of a cruise control system using counterexample-guided search," *Control Eng. Pract.*, vol. 12, no. 10, pp. 1269–1278, 2004. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0967066104000760>
- [40] Z. Xu, X. Chen, Y. Huang, Y. Bai, and Q. Chen, "Collision prediction and avoidance for satellite ultra-close relative motion with zonotope-based reachable sets," in *Proc. Inst. Mech. Eng., Part G: J. Aerosp. Eng.*, vol. 233, no. 11, pp. 3920–3937, 2019.
- [41] F. Flammini, L. De Donato, A. Fantechi, and V. Vittorini, "A vision of intelligent train control," in *Proc. Int. Conf. Rel., Saf., Secur. Railway Syst.*, 2022, pp. 192–208.
- [42] C. Qiu, T. Chen, S. Lu, and H. Wang, "A safety-oriented dynamic moving block train control system based on train-to-train communication," *IEEE Intell. Transp. Syst. Mag.*, vol. 14, no. 3, pp. 175–187, May/June 2022.
- [43] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya, "What's decidable about hybrid automata?," *J. Comput. Syst. Sci.*, vol. 57, no. 1, pp. 94–124, 1998.
- [44] A. Girard, "Reachability of uncertain linear systems using zonotopes," in *Hybrid Systems: Computation and Control*, M. Morari and L. Thiele, Eds. Berlin, Germany: Springer, 2005, pp. 291–305.
- [45] M. Althoff, "Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets," in *Proc. 16th Int. Conf. Hybrid Syst.: Comput. Control*, 2013, pp. 173–182.
- [46] H. Roehm, J. Oehlerking, M. Woehrle, and M. Althoff, "Model conformance for cyber-physical systems: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 3, no. 3, pp. 1–26, Aug. 2019. [Online]. Available: <https://doi.org/10.1145/3306157>
- [47] J. Zhan, L. Chen, and Y. Chen, "Distributed model predictive control of heterogeneous vehicle platoons with guaranteed string stability," in *Proc. IEEE China Automat. Congr.*, 2021, pp. 2086–2091.
- [48] S. Su, T. Tang, X. Li, and Z. Gao, "Optimization of multitrain operations in a subway system," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 2, pp. 673–684, Apr. 2014.



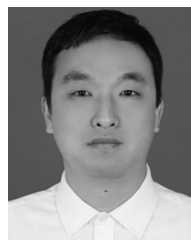
**Ming Chai** (Member, IEEE) received the Ph.D. degree from Computer Science Department, Humboldt University of Berlin, Berlin, Germany, in 2016. He is currently an Associate Professor for railway traffic information engineering and control with the National Engineering Research Center of Rail Transportation Operation and Control Systems, Beijing Jiaotong University, Beijing, China. His research interests include specification languages, runtime verification, model based testing, and their applications in the railway community.



**Haifeng Wang** (Member, IEEE) received the Ph.D. degree in system engineering from Beijing Jiaotong University, Beijing, China, in 2002. He is currently a Professor of railway traffic information engineering and control with the National Engineering Research Center of Rail Transportation Operation and Control Systems, Beijing Jiaotong University. His research interests include software safety engineering methods for railway signaling systems, new architecture of train control systems, and methods for improving railway capacity, community.



**Tao Tang** (Senior Member, IEEE) received the Ph.D. degree from Chinese Academy of Sciences, Beijing, China, in 1991. He is an Academic Pacesetter with National Key Subject Traffic Information Engineering and Control and Director of State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing. He is also a Specialist with the National Development and Reform Commission and Beijing Urban Traffic Construction Committee. His research interests include railway train control systems and intelligent control theory.



**Jinchuan Chai** (Member, IEEE) received the master's degree in communication and information system from Beijing Jiaotong University, Beijing, China, in 2015. He is currently a Senior Engineer with the National Railway Track Test Center, China Academy of Railway Sciences Corporation Limited (CARS), Beijing. His research interests include rail traffic test environment construction and comprehensive test, construction of railway science and technology innovation center, communication and information, railway signal, and Economy.



**Hongjie Liu** (Member, IEEE) received the B.S. degree in automatic control from Beijing Jiaotong University, Beijing, China in 2006 and the M.S. and Ph. D. degrees in traffic information engineering and control from Beijing Jiaotong University, in 2008 and 2019, respectively. He was with Beijing Jiaotong University in 2008. He is currently an Associate Professor. Between September 2017 and September 2018, he was with the New Jersey Institute of Technology, Newark, NJ, USA, as a Visiting Scholar. His research interests include safety design, formal modeling, verification and optimisation in railway train control systems. He has more than 80 publications including 60+ papers, 20+ patents, and one book chapter.