Letter

Attack-Resilient Distributed Cooperative Control of Virtually Coupled High-Speed Trains via Topology Reconfiguration

Shunyuan Xiao, *Member, IEEE*, Xiaohua Ge, *Senior Member, IEEE*, and Qing Wu, *Member, IEEE*

Dear Editor,

This letter addresses the resilient distributed cooperative control problem of a virtually coupled train convoy under stochastic disturbances and cyber attacks. The main purpose is to achieve distributed coordination of virtually coupled high-speed trains with the prescribed inter-train distance and same cruise velocity, while preserving driving security of the train convoy against a class of topological attacks. First, a resilient distributed cooperative control framework of the virtually coupled train convoy is established, which incorporates the longitudinal train dynamics, stochastic disturbances, and topological attacks on inter-train information flows. Building on that, a distributed cooperative control protocol and a topology reconfiguration algorithm are designed for attack-resilient train convoy tracking. Furthermore, a formal stability analysis is performed for the exponential convergence of the convoy tracking errors. Finally, a numerical case study on a 56 km-line segment of a real-world high-speed railway is carried out to validate the efficacy of our results.

In a virtually coupled train convoy, each train is equipped with onboard sensors, data processors, and transceivers, allowing for the exchange of specific train-related data (e.g., speed, position, acceleration, braking actions) with its neighboring trains in accordance with specified information flow topologies. By sharing the train information in real-time, interacted trains can make cooperative decisions and adjust their own operations accordingly to achieve a harmonized tracking objective of the train convoy [1]. This therefore testifies the significant role of the inter-train information flows in the desired train convoy tracking control. However, the implementation of virtually coupled trains is prone to malicious security threats on the wireless train information flows [2]–[4]. It is well-acknowledged that these malicious cyber attacks can impose significant adverse effects on the system and control performance [5]–[9]. Among the various cyber attacks targeting inter-train information flows, data availability attacks, such as wireless radio jamming, routing protocol falsification, and network traffic flooding [2], aim at impeding the transmission of exchanged information to the intended recipient.

When it comes to the design of a cooperative control strategy over generic information topologies, consensus-based control has been pervasively adopted [3], [4], [10]–[13]. In the context of virtual coupling control, this therefore allows flexible or varying communication topologies to be comprehensively analyzed and designed from the entire train convoy perspective. However, the majority of existing cooperative train control results rely on preconceived notions regarding the leader's global reachability or the presence of a spanning tree with the leader train acting as its root; see, e.g., [3], [4], [11]–[13]. This implies that the control strategies therein may fail to guarantee the train convoy stability once the leader's global reachability is no longer satisfied, for example, due to malicious data availability attacks. To the best of the authors' knowledge, there have been rare studies available on cooperative control of virtually coupled trains where data availability attacks are present to violate the global reachability assumption.

In this study, we delve into the resilient distributed cooperative control issue for multiple virtually coupled high-speed trains subject to topological attacks. To cope with such attacks, we propose an attack-resilient distributed cooperative control protocol together with an information flow repairing algorithm via topology reconfiguration. Summarized below are the main contributions of this study: 1) A resilient distributed cooperative control framework of a virtually coupled train convoy is established, which incorporates the longitudinal train dynamics, stochastic disturbances, and aperiodic topological attacks; 2) A numerically tractable controller design procedure and a topology reconfiguration algorithm are presented for effective and secure cooperative train tracking control; 3) A formal stability analysis is conducted to prove the exponential convergence of relative positions and velocities to the leader.

Problem formulation: Consider a train convoy comprising $N+1$ high-speed trains, where the leader train is represented as train 0 while the rest follower trains are indexed by $i \in \mathcal{V}_N = \{1,\dots,N\}$. The longitudinal dynamics of train i can be characterized by

$$m_i \dot{v}_i(t) = F_i(t) - \mathcal{F}_i(v_i(t)) - R_i(t) \tag{1}$$

where $s_i(t)$ and $v_i(t) = \dot{s}_i(t)$ denote the train i's realtime position and velocity, respectively; $F_i(t)$ denotes the driving/braking force implemented on train i; $\mathcal{F}_i(v_i(t)) = c_0 + c_1 v_i(t) + c_2 v_i^2(t)$ is the running resistance which encompasses rolling mechanical drag $c_0 + c_1 v_i(t)$ and air drag $c_2 v_i^2(t)$ with c_0, c_1, and c_2 being the corresponding coefficients; $R_i(t) = m_i f_i(s_i(t), v_i(t)) r(t)$ denotes the additional resistances composed of ramp-induced, curve-induced and tunnel-induced resistances. Note that $r(t)$ is a standard white noise; and $f_i(\cdot)$ is a nonlinear coefficient term dependent on the real-time train position and velocity, which satisfies $|f_i(m) - f_i(n)| \le \rho |m-n|$ for $\forall m,n > 0$ with a constant $\rho > 0$. For a linearization purpose, we configure the implemented driving/braking force as $F_i(t) = \mathcal{F}_i(v_i(t)) + m_i u_i(t)$, where $u_i(t)$ is the commanded control input. By defining $x_i(t) = [s_i(t), v_i(t)]^T$, for $\forall i \in \mathcal{V}_{N+1} = \mathcal{V}_N \cup \{0\}$, one can model the longitudinal train dynamics by the following Itô differential stochastic state-space equation:

$$dx_i(t) = (Ax_i(t) + Bu_i(t))dt + f_i(x_i(t))dw(t) \tag{2}$$

where $w(t)$ is a Brownian motion satisfying $w(t) = \int_0^t r(\varpi) d\varpi$ with $t \ge 0$; and $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

The inter-train information flow structure is interpreted by a directed graph $\mathcal{G} = (\mathcal{V}_N, \mathcal{E}, \mathcal{A})$, where $\mathcal{V}_N$ is the set of train indexes, $\mathcal{E} \subseteq \mathcal{V}_N \times \mathcal{V}_N$ is an information link set with (i, j) denoting the link from train j to train i, $\mathcal{A} = [a_{ij}]_{N\times N}$ is an adjacency matrix with its element $a_{ij} \ge 0$ signifying the link weight. Note that $a_{ii} = 0$ for $\forall i \in \mathcal{V}_N$. In addition, denote $a_{i0} \ge 0$ as the indication of leader association to train i, and then $a_{i0} = 1$ indicates that train i can be directly informed by train 0 while $a_{i0} = 0$ implies such information flow does not exist. Train j is deemed reachable to train i when there exists a directional path consisting of sequential information links $\{(i, l_1), (l_1, l_2), \dots, (l_q, j)\}$ with $l_p \in \mathcal{V}_{N+1}$, $p = 1, 2, \dots, q$ being train indexes. The leader train is said to be globally reachable if it is reachable to any follower train in the train convoy.

Topological attacks: We consider that adversaries intend to launch topological attacks aiming at deteriorating the global reacha-

Corresponding author: Xiaohua Ge.

Citation: S. Xiao, X. Ge, and Q. Wu, "Attack-resilient distributed cooperative control of virtually coupled high-speed trains via topology reconfiguration," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 4, pp. 1066–1068, Apr. 2024.

S. Xiao is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: xsyuan@njupt.edu.cn).

X. Ge is with the School of Science, Computing and Engineering Technologies, Swinburne University of Technology, Melbourne VIC 3122, Australia (e-mail: xge@swin.edu.au).

Q. Wu is the School of Engineering and Technology, Central Queensland University, Rockhampton QLD 4701, Australia (e-mail: q.wu@cqu.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.124011

bility of the leader train via blocking certain inter-train information flow links. In such circumstances, some existing control strategies to counter data availability attacks (e.g., those in [3], [4]) may fail to guarantee the secure and desired train operation. Denote the repairing procedure activation indication signal as $\chi(t)$. Once the topological attacks on inter-train information flow is detected, and the indication signal is then set as $\chi(t) = 1$, which indicates that a repairing procedure based on topology reconfiguration is activated. Denote by T_a and T_r the total attack duration and the repairing duration, respectively. Define $\sigma(t) : [0, +\infty) \to \Omega = \{1, 2, \ldots, m\}$, $m \in \mathbb{N}_+$ as the switching sequence of the resultant information flow topologies. As a result, m weighted digraphs $\mathcal{G}_{\sigma(t)} = (\mathcal{V}_N, \mathcal{E}_{\sigma(t)}, \mathcal{A}_{\sigma(t)})$, $\sigma(t) \in \Omega$ with $\mathcal{A}_{\sigma(t)} = [a_{ij}^{\sigma(t)}]_{N\times N}$ can be defined to describe the varying topologies during different attacking periods and repairing periods. Correspondingly, Laplacian matrices of digraphs $\mathcal{G}_{\sigma(t)}$ are defined as $\mathcal{L}_{\sigma(t)} = \mathcal{D}_{\sigma(t)} - \mathcal{A}_{\sigma(t)}$, where $\mathcal{D}_{\sigma(t)} = \mathrm{diag}_{i=1}^{N}\{d_i^{\sigma(t)}\}$ with $d_i^{\sigma(t)} = \sum_{j=1}^{N} a_{ij}^{\sigma(t)}$. Denote $\mathcal{H}_{\sigma(t)} = \mathcal{L}_{\sigma(t)} + \mathrm{diag}_{i=1}^{N}\{a_{i0}^{\sigma(t)}\}$. Further define Ω_a and Ω_r as the index set of activations of topological attacks and repairing procedures, respectively, which leads to $\Omega = \Omega_a \bigcup \Omega_r$.

Definition 1: For $\forall t_0, t$ satisfying $t > t_0 \geq 0$, denote by $N_a(t_0, t)$, $T_a(t_0, t)$ and $T_r(t_0, t)$ the attack number, attack duration and repair duration during (t_0, t), respectively. Then the attack frequency, attack length rate and average attack duration are given as $F_a(t_0, t) = \frac{N_a(t_0,t)}{t-t_0}$, $R_a = \frac{T_a(t_0,t)}{t-t_0}$ and $\bar{T}_a(t_0, t) = \frac{T_a(t_0,t)}{N_a(t_0,t)}$, respectively.

Lemma 1: If train 0 is globally reachable, there exist matrices $\Theta_{\sigma(t)} = \mathrm{diag}_{i=1}^{N}\{\theta_{\sigma(t),i}^{-1}\} > 0$ such that $\Theta_{\sigma(t)}\mathcal{H}_{\sigma(t)} + \mathcal{H}_{\sigma(t)}^{T}\Theta_{\sigma(t)} > 0$ with $\theta_{\sigma(t)} = \mathrm{col}_{i=1}^{N}\{\theta_{\sigma(t),i}\}^T = \mathcal{H}_{\sigma(t)}^{-T}\mathbf{1}$.

A resilient distributed cooperative control protocol: The attack-resilient distributed control law for each train i is designed as

$$u_i(t) = -\gamma K \sum_{j=0}^{N} a_{ij}^{\sigma(t)}(x_i(t) - x_j(t) - \bar{d}_{ij}(t)) \tag{3}$$

where γ is the coupling gain; K is the controller gain matrix; and $\bar{d}_{ij}(t) = [d_{i,j}(t), 0]^T$ with $d_{i,j}(t) = \sum_{q=j+1}^{i} d_{q,q-1}(t)$. Here, $d_{q,q-1}(t) = L_{q-1} + d_{q,q-1}^{B}(t) + d_{q,q-1}^{S}$ denotes the desired inter-train distance between two adjacent trains $q-1$ and q, which can be specified by the desired spacing policy or gap reference [14]. Here, L_{q-1} represents the train length, $d_{q,q-1}^{B}$ is the demanded braking distance, and $d_{s,s-1}^{S}$ is the extra safety distance.

Define $\delta_i^s(t) = s_i(t) - s_0(t) - d_{i,0}(t)$ and $\delta_i^v(t) = v_i(t) - v_0(t)$, as the position and velocity tracking errors. Denoting $\delta_i(t) = [\delta_i^s(t), \delta_i^v(t)]^T$, $g_i(\delta_i(t)) = f_i(x_i(t)) - f_0(x_0(t))$, $\delta(t) = \mathrm{col}_{i=1}^{N}\{\delta_i(t)\}$, $g(\delta(t)) = \mathrm{col}_{i=1}^{N}\times\{g_i(\delta_i(t))\}$, and recalling $A\bar{d}_{ij}(t) = \bar{d}_{ij}(t)$, we arrive at the following augmented tracking error system:

$$d\delta(t) = (I \otimes A - \gamma\mathcal{H}_{\sigma(t)} \otimes BK)\delta(t)dt + g(\delta(t))dw(t). \tag{4}$$

Main results: Controller design and topology reconfiguration:
Controller design and topology reconfiguration:

(Step 1) Choose positive scalars $\alpha, \beta, \gamma, \eta < \beta, \zeta < \eta$ such that

$$\varepsilon \geq \gamma|\bar{\lambda}_0|,\ \psi \leq \gamma\tilde{\lambda}_0,\ F_a(t_0, t) \leq \frac{\eta - \zeta}{2\ln(\mu)},\ R_a \leq \frac{\beta - \eta}{\alpha + \beta} \tag{5}$$

where $\mu = \frac{\bar{\theta}}{\tilde{\theta}}$ with $\bar{\theta} = \max_{s,i}\theta_{s,i}$ and $\tilde{\theta} = \min_{s,i}\theta_{s,i}$ for $\forall s \in \Omega$ and $i \in \mathcal{V}_N$; $\bar{\lambda}_0 = \min_s(\lambda_{\min}(\mathcal{H}_s + \mathcal{H}_s^T))$; and $\tilde{\lambda}_0 = \min_s(\lambda_{\min}(\Theta_s\mathcal{H}_s + \mathcal{H}_s^T\Theta_s))$ for $\forall s \in \Omega$.

(Step 2) For some positive scalars ψ, ε, ρ, solve

$$\mathrm{diag}\{\Lambda_1, \Lambda_2\} < 0 \tag{6}$$

to determine $P > 0$, where $\Lambda_1 = AP + PA^T + \varepsilon BB^T + (\rho^2 - \alpha)P$ and $\Lambda_2 = AP + PA^T - \psi\tilde{\theta}BB^T + (\rho^2 + \beta)P$. **If** feasible, compute $K = B^T P^{-1}$, then continue; **otherwise**, goto Step 1.

(Step 3) Determine the allowable average attack duration

$$\bar{T}_a(t_0, t) \leq \frac{\beta - \eta}{(\alpha + \beta)F_a(t_0, t)} \tag{7}$$

and implement Algorithm 1 when $\chi(t) = 1$.

Algorithm 1 Topology Reconfiguration

Require: Repairing procedure activation signal $\chi(t)$
1: **while** $\chi(t) = 1$ **do**
2: Identify a remaining spanning tree $F_{\sigma(t)} = (\mathcal{V}_{\sigma(t)}^F, \mathcal{E}_{\sigma(t)}^F)$ with the maximum number n_s of trains, where $\mathcal{V}_{\sigma(t)}^F \subseteq \mathcal{V}_N$ and $\mathcal{E}_{\sigma(t)}^F \subseteq \mathcal{E}_{\sigma(t)}$ are the train index set and information link set of $F_{\sigma(t)}$
3: **if** the root of $F_{\sigma(t)}$ is train 0 **then**
4: Renumber the trains in $F_{\sigma(t)}$ as $0, 1, \ldots, n_s - 1$ such that each train's parent node is lower numbered than itself
5: Set $\bar{n}_s = n_s - 1$
6: **else**
7: Renumber the trains in $F_{\sigma(t)}$ as $1, \ldots, n_s$ such that each train's parent node is lower numbered than itself
8: Build an information link from train 0 to the renumbered train 1
9: Set $\bar{n}_s = n_s$
10: **end if**
11: Define $\Upsilon = \emptyset$
12: **for** $i = \bar{n}_s : N - 1$ **do**
13: **for** $j = 1 : N$ **do**
14: **if** $j \notin \mathcal{V}_{\sigma(t)}^F \cup \Upsilon$ **then**
15: Identify train i's nearest available neighbor j
16: **if** $(j, i) \notin \mathcal{E}_{\sigma(t)}$ & Train j is not informed by train 0 **then**
17: Build an information link (j, i) from renumbered train i to its nearest neighbor train j, $j \notin \mathcal{V}_{\sigma(t)}^F$
18: Update $\mathcal{V}_{\sigma(t)}^F = \mathcal{V}_{\sigma(t)}^F \cup \{j\}$
19: Update $\mathcal{E}_{\sigma(t)}^F = \mathcal{E}_{\sigma(t)}^F \cup (j, i)$
20: Renumber train j as $i + 1$ in $F_{\sigma(t)}$ **break**
21: **else**
22: Update $\Upsilon = \Upsilon \cup \{j\}$
23: **end if**
24: **end if**
25: **end for**
26: **end for**
27: **end while**

Stability analysis: The exponential stability analysis criterion for the train tracking error dynamics (4) is presented as below.

Theorem 1: For a virtually coupled high-speed train convoy with longitudinal dynamics (2) and compromised inter-train information flows, under the distributed cooperative control protocol (3) and repairing Algorithm 1, the tracking errors $\delta_i(t)$, $i \in \mathcal{V}_N$ are exponentially stable in mean square if (5) and (6) hold.

Proof: Choose the Lyapunov function candidate as

$$V(\delta(t))_{\sigma(t)} = \begin{cases} \delta^T(t)(I_N \otimes Q)\delta(t),\ \sigma(t) \in \Omega_a \\ \delta^T(t)(\Theta_{\sigma(t)} \otimes Q)\delta(t),\ \sigma(t) \in \Omega_r \end{cases} \tag{8}$$

where $Q = P^{-1}$. First, we consider the case when $\sigma(t) \in \Omega_a$. One obtains that $d(V(\delta(t))_{\sigma(t)}) = \mathfrak{L}(V(\delta(t))_{\sigma(t)}) + 2\delta^T(t)(I_N \otimes Q)g(\delta(t))\times dw(t)$, where $\mathfrak{L}(V(\delta(t))_{\sigma(t)}) = \delta^T(t)\,[I_N \otimes (QA + A^TQ) - 2\gamma\mathcal{H}_{\sigma(t)} \otimes QBK]\delta(t) + g^T(\delta(t))(I_N \otimes Q)g(\delta(t))$.

Let $\xi_i(t) = Q\delta_i(t)$ and $\xi(t) = \mathrm{col}_{i=1}^{N}\{\xi_i(t)\}$, together with (6), one has that $\mathfrak{L}(V(\delta(t))_{\sigma(t)}) \leq \alpha\delta^T(t)(I_N \otimes Q)\delta(t)$, which yields

$$\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \leq \mathrm{e}^{\alpha(t-t_k)}\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\}, t \in [t_k, t_{k+1}).$$

Next, we discuss the case when $\sigma(t) \in \Omega_r$. Similarly, we have

$$d(V(\delta(t))_{\sigma(t)}) = \mathfrak{L}(V(\delta(t))_{\sigma(t)}) + 2\delta^T(t)(\Theta_{\sigma(t)} \otimes Q)g(\delta(t))dw(t)$$

where $\mathfrak{L}(V(\delta(t))_{\sigma(t)}) = \delta^T(t)[\Theta_{\sigma(t)} \otimes (QA + A^TQ) - 2\gamma\Theta_{\sigma(t)}\mathcal{H}_{\sigma(t)} \otimes QBK]\delta(t) + g^T(\delta(t))(\Theta_{\sigma(t)} \otimes Q)g(\delta(t))$. It then follows that:

$$\mathfrak{L}(V(\delta(t))_{\sigma(t)}) \leq \xi^T(t)[I_N \otimes (AP + PA^T + \rho^2 P - \psi\tilde{\theta}BB^T)]\xi(t)$$

which further yields

$$\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \leq \mathrm{e}^{-\beta(t-t_k)}\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\}, t \in [t_k, t_{k+1}).$$

Combining the above two cases, for $\forall t \in [t_k, t_{k+1})$, it arrives that

$$\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \leq \begin{cases} e^{\alpha(t-t_k)}\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\},\ \sigma(t) \in \Omega_a \\ e^{-\beta(t-t_k)}\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\},\ \sigma(t) \in \Omega_r. \end{cases}$$

Since $\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\} \le \mu\mathbb{E}\{V(\delta(t_k^-))_{\sigma(t_k^-)}\}$ and $\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \le e^{\alpha T_a(t_k,t)-\beta T_r(t_k,t)}\mathbb{E}\{V(\delta(t_k))_{\sigma(t_k)}\}$, we have $\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \le \mu^{N_s(t_0,t)} \times e^{\alpha T_a(t_0,t)-\beta T_r(t_0,t)}\mathbb{E}\{V(\delta(t_0))_{\sigma(t_0)}\}$, where $N_s(t_0,t)$ denotes the total switching times. From (5) and (7), the above inequality can be written as $\mathbb{E}\{V(\delta(t))_{\sigma(t)}\} \le e^{-\zeta(t-t_0)}\mathbb{E}\{V(\delta(t_0))_{\sigma(t_0)}\}$. We thus have $\mathbb{E}\{\|\delta_i(t)\|^2\} \le \kappa e^{-\zeta(t-t_0)}\mathbb{E}\{\|\delta_i(t_0)\|^2\}$, where $\kappa = \dfrac{\max\{\lambda_{\max}(\theta_{s,i}^{-1}Q),\lambda_{\max}(Q)\}}{\min\{\lambda_{\min}(\theta_{s,i}^{-1}Q),\lambda_{\min}(Q)\}}$, $s \in \Omega$, $i \in V_N$. ■

An illustrative example: A case study is performed on a practical 56km-line segment of the Wuhan-Guangzhou China high-speed railway, specifically the Yingde to Qingyuan route [15]. The cooperative control performance of seven high speed trains (one leader and six followers) of the EMU CHR3 type will be examined. Choose $m_i = 4.9\times10^5$ kg, $c_0 = 0.755$ N/kg, $c_1 = 0.00636$ N/(km/h · kg), $c_2 = 0.00636$ N/(km^2/h^2 · kg), $L_i = 200$ m, $i \in \mathcal{V}_{N+1}$, $d_{i,i+1}^S = 80$ m, $d_{i,i+1}^B(t) = 170$ m, $i \in \mathcal{V}_{N+1}/\{N\}$. Further choose $\alpha = 6$, $\beta = 1.95$, $\gamma = 3.9689$, $\eta = 0.5$, $\zeta = 0.1$, $\psi = 8$, $\varepsilon = 0.005$. The runtime is set as 120 s and the sampling period is set as $h = 0.05$ s.

The information flow topologies during attacking periods and repairing periods are depicted in Fig. 1. It can be seen that the information links (3, 2) and (1, 3) are reconstructed after links (1, 0), (2, 1), (3, 2) and (5, 0) being interrupted by Type I attacks. Together with the link reconstruction results facing Types II and III attacks, we observe that relatively few information links (less than the number of disrupted links) are built through Algorithm 1 to handle the topological attacks.

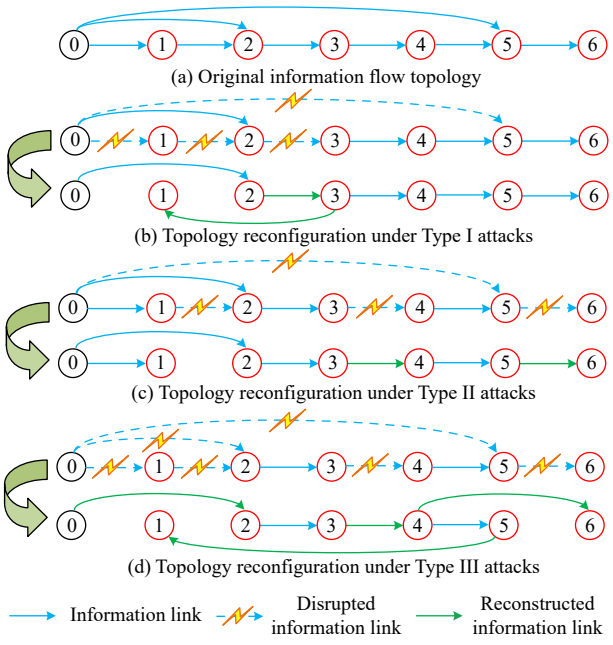

Fig. 1. Information flow topologies during attacking and repairing periods under topology reconfiguration.

Applying the proposed controller design procedure, we obtain $\bar{T}_a \le 2.4319$ s, which indicates the upper bound of average implementation time of repair procedures. Following this requirement, together with the proposed Algorithm 1, the relative positions and velocities of follower trains to the leader, are depicted in Figs. 2(a) and 2(b), respectively. It is seen that although the simulated topological attacks disrupt the global reachability of the leader train, the virtually coupled train convoy under our proposed secure distributed cooperative control scheme still achieves the desired train tracking performance in terms of prescribed inter-train distances (w.r.t. mass points) of 450 m and same velocities.

Conclusion: The resilient distributed control problem of virtually coupled high-speed trains encountering topological attacks is addressed in this paper. To cope with the generic inter-train information flow topologies with compromised global reachability of the leader train, a repairing algorithm based on topology reconfiguration is proposed, which, together with the derived distributed control protocol, achieves the desired secure train tracking performance. Finally, a case study is conducted for efficacy validation.

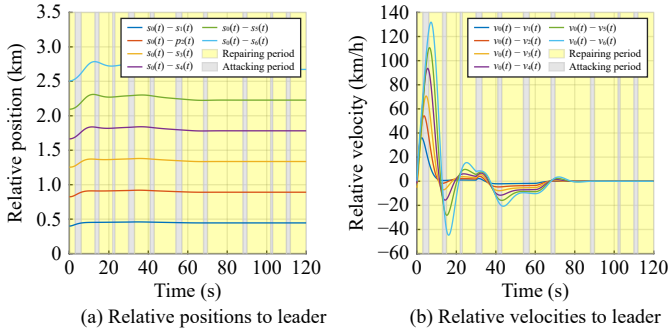

Fig. 2. Relative positions and velocities of follower trains to the leader.

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (62303240), the Natural Science Foundation of Jiangsu Province of China (BK20230356), the Natural Science Research Start-Up Foundation of Recruiting Talents of Nanjing University of Posts and Telecommunications (NY222033) and the Natural Science Foundation for Colleges and Universities in Jiangsu Province (22KJB120001).

References

[1] Q. Wu, X. Ge, Q.-L. Han, and Y. Liu, "Railway virtual coupling: A survey of emerging control techniques," *IEEE Trans. Intell. Veh*, vol. 8, no. 5, pp. 3239–3255, May 2023.

[2] S. Kim, Y. Won, I. H. Park, Y. Eun, and K.-J. Park, "Cyber-physical vulnerability analysis of communication-based train control," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6353–6362, Aug. 2019.

[3] H. Zhao, X. Dai, L. Ding, D. Cui, J. Ding, and T. Chai, "Resilient cooperative control for high-speed trains under denial-of-service attacks," *IEEE Trans. Veh. Technol.*, vol. 70, pp. 12427–12436, Dec. 2021.

[4] W. Yu, D. Huang, and N. Qin, "Resilient coordinated data-driven control of multiple high-speed trains under fading measurements and denial-of-service attacks," *IEEE Trans. Veh. Technol.*, vol. 72, pp. 5690–5701, May 2023.

[5] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure and collision-free multi-platoon control of automated vehicles under data falsification attacks," *Automatica*, vol. 145, p. 110531, Nov. 2022.

[6] X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, pp. 1234–1251, May 2023.

[7] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multi-agent systems against malicious attacks: A brief survey," *IEEE Trans. Ind. Inform.*, vol. 18, no. 6, pp. 3595–3608, Jun. 2022.

[8] X. Gong, M. Basin, Z. Feng, T. Huang, and Y. Cui, "Resilient time-varying formation-tracking of multi-UAV systems against composite attacks: A two-layered framework," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 4, pp. 969–984, Apr. 2023.

[9] H. Guo, J. Sun, and Z.-H. Pang, "Residual-based false data injection attacks against multi-sensor estimation systems," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1181–1191, May 2023.

[10] Y. Ju, D. Ding, X. He, Q.-L. Han, and G. Wei, "Consensus control of multi-agent systems using fault-estimation-in-the-loop: Dynamic event-triggered case," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 8, pp. 1440–1451, Aug. 2022.

[11] Q. Wu, X. Ge, Q.-L. Han, B. Wang, H. Wu, C. Cole, and A. Spiryagin, "Dynamics and control simulation of railway virtual coupling," *Veh. Syst. Dyn.*, vol. 61, no. 9, pp. 2292–2316, Sept. 2023.

[12] W. Bai, H. Dong, J. Lü, and Y. Li, "Event-triggering communication based distributed coordinated control of multiple high-speed trains," *IEEE Trans. Veh. Technol.*, vol. 70, pp. 8556–8566, Sept. 2021.

[13] X. Wang, L. Zhu, H. Wang, *et al.*, "Robust distributed cruise control of multiple high-speed trains based on disturbance observer," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, pp. 267–279, Jan. 2021.

[14] X. Ge, Q.-L. Han, X.-M. Zhang, and D. Ding, "Communication resource-efficient vehicle platooning control with various spacing policies," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 2, pp. 362–376, 2024.

[15] Y. Song and W. Song, "A novel dual speed-curve optimization based approach for energy-saving operation of high-speed trains," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, pp. 1564–1575, Jun. 2016.