Letter

Resilient Event-Triggered Model Predictive Control for Adaptive Cruise Control Under Sensor Attacks

Zhijian Hu, Rong Su, *Senior Member, IEEE*, Kai Zhang, Zeyuan Xu, and Renjie Ma, *Member, IEEE*

Dear Editor,

This letter addresses the resilient model predictive control (MPC) problems for adaptive cruise control (ACC) systems under sensor attacks. In the light of vulnerabilities of ACC systems to sensor attacks, an intrusion detection mechanism is proposed at the controller side to distinguish abnormal data. Then, the robust control gains are derived to design the terminal region constraint for MPC. Further, an improved event-triggered scheme is presented, which shows the ability to relieve the computation burden in the implementation of MPC, by combining the memory-based event-triggered condition and the maximum allowed time interval condition. Finally, efficacy validations are given in simulations.

ACC provides critical auxiliary techniques for autonomous vehicles, and facilitates a safe and comfortable journey for both drivers and passengers [1]–[3]. The main function of ACC system is to monitor the other vehicles' conditions by sensors and then maintain the constant velocity, acceleration and the longitudinal distance with them. In recent decades, a flood of concerns regarding to ACC have been addressed by researchers from different perspectives. Some focused on the control methods formulation [4], while others emphasized the application scenarios exploration and performance enhancement [5]–[7].

Due to the intrinsic constraints of position, velocity, and acceleration involved in ACC, the MPC methods are seen as a kind of promising solutions. In [5], road elevation information and fuel-saving factor were simultaneously considered to design MPC for ACC system. Reference [7] constructed a MPC framework for ACC system with the consideration of four objectives, including comfort, fuel-economy, safety, and car-following. However, none of the above methods considered the calculation volume when implementing MPC, let alone the countermeasures of reducing the calculation burden.

To reduce the calculation burden of implementing MPC for ACC, the event-triggered scheme has been considered as a category of efficient means. Under the event-triggered scheme, the measured output is used as the feedback signal only if well-designed event-triggered conditions hold. In existing related works, most of the event-triggered schemes were designed by comparing measured outputs at adjacent time instants, such as [8]–[11]. However, these event-triggered conditions overlooked the feature of system dynamic curves. As an improvement, memory-based event-triggered schemes have been proposed in recent years [12], in which several historic released signals were collected to formulate the event-triggered conditions.

Sensor attacks are nothing new in autonomous vehicle control systems [13]–[18]. From adversary's perspective, two different categories of malicious attacks are possible on sensors to implement their conspiracy. One category is classified as the denial-of-service (DoS) attack [16], which makes sensors cannot produce the successive measurements. The other is classified as the false data injection (FDI) attack, which plants the false information to the sensor and destroys the data's authenticity. In [17], an adaptive control framework was constructed to mitigate both sensor and actuator attacks. However, these investigations with the sensor attack considerations are not directly applicable to ACC systems.

To the authors' best knowledge, no results on resilient MPC considering computation burden releasing for ACC system under sensor attacks have been revealed till now. To fill the gap, we formulate this letter. The primary innovations are identified as the following: 1) To mitigate the impacts of sensor attacks on ACC system, a χ^2 intrusion detection mechanism is presented at the controller side under MPC framework. 2) To guarantee the stability of MPC, the robust control gains are derived to formulate the terminal region constraint. 3) To improve the memory-based event-triggered scheme [12], this letter adds the maximum allowed time interval as an auxiliary condition, which enhances the resiliency of the ACC system by guaranteeing the controller is triggered even though the memory-based event generator breaks down.

Modeling of ACC: ACC is one of the most used cruise control approaches. A general dynamic model is

$$\tau \frac{d\ddot{p}(t)}{dt} + \ddot{p}(t) = u(t) \tag{1}$$

where p is the position of the vehicle, τ is the time delay caused by the limited bandwidth of the lower controller, u is the control input of the upper controller.

In ACC system, we expect the vehicle keeps the constant longitudinal distance with the preceding one, and the same velocity and acceleration. Thus, in this letter we focus on the relative position, velocity and acceleration in ACC system, and set the dynamic model as

$$\begin{cases} \dot{x}(t) = \mathcal{A}x(t) + \mathcal{B}u(t) + \mathcal{F}w(t) \\ y(t) = Cx(t) \end{cases} \tag{2}$$

where

$$x(t) = [\Delta p(t) \quad \Delta v(t) \quad \Delta a(t)]^T,\ \mathcal{B} = [0 \quad 0 \quad 1/\tau]^T$$

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1/\tau \end{bmatrix},\ C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ \mathcal{F} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

with $\Delta p(t)$ representing the longitudinal distance between one vehicle and its preceding vehicle, $\Delta v(t)$ representing the difference of velocity, $\Delta a(t)$ representing the difference of acceleration, and $w(t)$ representing the disturbance, which indicates the acceleration of the preceding vehicle in this letter.

To facilitate the implementation of MPC with event-triggered scheme, the discrete form of (2) is given as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Fw(k) \\ y(k) = Cx(k) \end{cases} \tag{3}$$

where $A = e^{\mathcal{A}h}$, $C = C$, $B = \int_0^h e^{\mathcal{A}t}\mathcal{B}dt$, $F = \int_0^h e^{\mathcal{A}t}\mathcal{F}dt$, and h signifies the sampling time.

MPC formulation: To realize the effective control for ACC sys-

Corresponding author: Renjie Ma.

Citation: Z. J. Hu, R. Su, K. Zhang, Z. Y. Xu, and R. J. Ma, "Resilient event-triggered model predictive control for adaptive cruise control under sensor attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 3, pp. 807–809, Mar. 2023.

Z. J. Hu and R. Su are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore (e-mail: zhijian.hu@ntu.edu.sg; rsu@ntu.edu.sg).

K. Zhang is with the Key Laboratory of Ultra-Precision Intelligent Instrumentation, Ministry of Industry and Information Technology, and the Center of Ultra-Precision Optoelectronic Instrument Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: kaizhang0116@163.com).

Z. Y. Xu was with the Department of Control Science and Engineering, Harbin Institute of Technology, Harbin 150001, China. He is now with the Department of Chemical and Biomolecular Engineering, National University of Singapore, Singapore 117585, Singapore (e-mail: xzy20@nus.edu.sg).

R. J. Ma is with the State Key Laboratory of Robotics and Systems, Harbin Institute of Technology, Harbin 150001, China (e-mail: renjiema@hit.edu.cn).

Digital Object Identifier 10.1109/JAS.2023.123111

tem, this letter adopts the MPC, which has been seeing as a most promising control method in practical engineering. The cost function in MPC is related with both the system states and control input with the mathematical expression

$$\begin{aligned}\phi(&x(k+m\mid k),u(k+m\mid k))\\ &=a(\Delta p(k+m\mid k)-\Delta\bar{p})^2+b(\Delta v(k+m\mid k))^2\\ &\quad+c(\Delta a(k+m\mid k))^2+d(u(k+m\mid k))^2\end{aligned}\tag{4}$$

where a, b, c, d are the weighting coefficients, $\Delta\bar{p}$ is the desired longitudinal distance between vehicles, and $(k+m\mid k)$ denotes the predicted value at time $(k+m)$ with the real-time measurements at time k.

Throughout the prediction horizon M, the total cost function is

$$\begin{aligned}\xi(\boldsymbol{x}(k),\boldsymbol{u}(k))=&\sum_{m=0}^{M-1}\phi(x(k+m|k),u(k+m|k))\\ &+V_f(x(k+M|k))\end{aligned}\tag{5}$$

in which $\boldsymbol{u}(k)=[u(k|k)^T\cdots u(k+M-1|k)^T]^T$, $\boldsymbol{x}(k)=[x(k|k)^T\cdots x(k+M-1|k)^T]^T$, $V_f=x(k+M|k)^TPx(k+M|k)$ indicates the terminal penalty cost to be designed, and M represents the control horizon and the prediction horizon.

Considering the constraints, the following MPC framework is proposed for ACC system:

$$\min_{\boldsymbol{u}}\xi(\boldsymbol{x}(k),\boldsymbol{u}(k))\ \text{ s.t.}\begin{cases}x(k+m+1|k)=Ax(k+m|k)+Bu(k+m|k)\\ x(k|k)=x(k)\\ x(k+M|k)\in\Omega\\ \Delta p_{\min}\le\Delta p(k+m|k)\le\Delta p_{\max}\\ \Delta v_{\min}\le\Delta v(k+m|k)\le\Delta v_{\max}\\ \Delta a_{\min}\le\Delta a(k+m|k)\le\Delta a_{\max}\\ m=1,2,\dots,M-1\end{cases}\tag{6}$$

where Ω is the terminal region constraint, $\Delta p_{\min}/\Delta p_{\max}$, $\Delta v_{\min}/\Delta v_{\max}$, and $\Delta a_{\min}/\Delta a_{\max}$ respectively represent the lower and upper bounds of the predicted position, velocity, and acceleration signals.

To guarantee the stability of ACC system under MPC, the terminal penalty cost V_f should be properly designed. In this letter, a robust control gain K is derived to facilitate the design of the terminal region constraint Ω, by choosing the Lyapunov function $V(k)=x^T(k+M|k)Px(k+M|k)$ and incorporating the $\mathcal{H}_\infty$ performance index [19] and [20]. Limited by the space, interested readers can refer to Theorems 1 and 2 in [19] for the detailed deriving procedure of K. Selecting $0<\epsilon<-\max\mathrm{Re}\{\lambda(A+BKC)\}$ and calculating $\epsilon^2(A+BKC)^TP(A+BKC)-P=-(Q+K^TRK)$, a unique Lyapunov matrix P can be obtained, where Q and R can be acquired from the weighting coefficients a, b, c, d. Thus, a particular ellipsoid $\Omega=\{x\in\mathcal{R}|x^TPx\le\beta\}$ is set as the terminal region constraint with β being a positive constant, x^TPx is chosen as the terminal cost, and Ky is employed to control the terminal region.

Intrusion detection under sensor attacks: The MPC embodies the idea of rolling optimization. In each iteration, the controller needs to collect the measured outputs from sensors to rectify the prediction error. To enhance the resiliency of the MPC for ACC system, this letter considers the underlying sensor attacks. Adversaries may trick sensors to output false measurements by implanting malicious procedures, leading false control actions being executed and finally the vehicle accidents. To capture the behaviors of the sensor attacks, the actual measured output is described by

$$\tilde{y}(k)=y(k)+g(k)\tag{7}$$

where $y(k)$ denotes desired measured output, and $g(k)$ signifies the injected false information by adversaries.

To mitigate the impacts of sensor attacks, this letter proposes a χ^2 intrusion detection mechanism to detect the abnormal measurements. Once a sensor is judged as the attacked one, the backup sensor will take its place. We assume that states of the preceding vehicle are measurable and the differences of states between two adjacent vehicles are independent identically distributed. According to this basis, one can define

$$\zeta(k)=\sum_{j=k-T+1}^{k}[\tilde{y}(j)-\bar{y}(j)]^T\Phi[\tilde{y}(j)-\bar{y}(j)],\ \ k\ge T\tag{8}$$

where $\zeta(k)$ obeys the χ^2 distribution and its freedom degree is $(3\times T)$, T represents the sliding window, $\bar{y}$ denotes the state measurements for preceding vehicles, and $\Phi=\mathrm{diag}\{\omega_{\mathrm{p}},\omega_{\mathrm{v}},\omega_{\mathrm{a}}\}$ is adopted to capture the importance degree of position, velocity, acceleration.

The χ^2 intrusion detector at time k is constructed by

$$\zeta(k)\underset{H_1}{\overset{H_0}{\lessgtr}}\varrho\tag{9}$$

in which ϱ denotes false alarm probability, which can be determined based on a specific ACC system. When the initial hypothesis H_0 assuming the states of two adjacent vehicles are within the acceptable range is broken, the alarm H_1 will be instantly triggered.

Event-triggered scheme: In the design of event-triggered conditions, most of the existing literatures only focused on the difference between the current measurement and the most recently triggered signal, while ignored the significance of the historic triggered signals. The drawbacks of these results were analyzed and compared by [12] with the consideration of several historic triggered signals. This letter improves the above event-triggered scheme by incorporating the maximum allowed time interval (MATI) condition. The proposed event-triggered conditions are represented as

$$\begin{cases}\Pi(k)=\displaystyle\sum_{i=1}^{N}\eta^ie^i(k)^T\Psi e^i(k)-\delta\hat{y}(k)^T\Psi\hat{y}(k)\ge0\\ \text{or }\ \vartheta^1\ge\Gamma\end{cases}\tag{10}$$

where $e^i(k)=\tilde{y}(k)-\tilde{y}(k-\vartheta^i)$, $\hat{y}(k)=(1/N)\sum_{i=1}^{N}\tilde{y}(k-\vartheta^i)$, ϑ^i represents a positive integer satisfying $\vartheta^1<\vartheta^2<\cdots<\vartheta^i$, $\tilde{y}(k-\vartheta^i)$ signifies the recently released signal, η^i means the weighting coefficient of historic released signals with $\sum_{i=1}^{N}\eta^i=1$, N is the amount of the necessary historic released signals, matrix Ψ depicts the importance of each states, Γ is an indicator of the MATI, and δ is used to adjust the triggered frequency.

Remark: In practice, it is advised to consider zeno-like behavior when formulating the event-triggered conditions in (10), in which way the minimum interval between any two consecutive triggering instants can be strictly greater than the sampling time h. In that case, the computation efficiency will be further improved. The detailed zeno-like behavior exclusion method can refer to [11] and [21].

The advantages of the MATI condition are twofolds. First, it has the ability to tolerate a certain incomplete modeling issues involved in existing event-triggered conditions. Second, the MATI condition better enhances the resiliency of the ACC system by guaranteeing that the controller can be triggered when MATI reaches.

Simulation validation: In simulations, the parameters of MPC for the ACC system are set up as the following [22]. $\tau=0.58$, $h=0.2$, $\Delta\bar{p}=100$, $x(0)=[20;2;0]$, $w(k)=0.01\times(\mathrm{rand}(1)-0.5)$, $a=1$, $b=0.5$, $c=0.5$, $d=1$, $\epsilon=0.65$, $M=10$, $\varrho=150$, $\Gamma=6$, $N=3$, $\eta^1=0.6$, $\eta^2=0.3$, $\eta^3=0.1$, $T=10$, $\omega_p=1$, $\omega_v=1$, $\omega_a=1$, $\Psi=\mathrm{diag}\{1,1,1\}$, $\delta=0.2$, $\Delta p_{\min}=80$ m, $\Delta p_{\max}=120$ m, $\Delta v_{\min}=-15$ m/s, $\Delta v_{\max}=15$ m/s, $\Delta a_{\min}=-8$ m/s^2, $\Delta a_{\max}=8$ m/s^2, $g(k)=[-2;1;0]$ from $k=100$.

Fig. 1 compares the system dynamics of position, velocity, and acceleration signals with and without the proposed χ^2 attack detection mechanism. It is observed from Fig. 1 that all three states become diverging without the χ^2 attack detection mechanism, which means the adversaries can destruct the ACC system and make vehicle accidents by attacking sensors if no countermeasures are taken. With the proposed χ^2 attack detection mechanism, all three states perform a short period of divergence and then quickly return to desired states.

Fig. 2 illustrates event-triggered instants and intervals under our presented event-triggered scheme. From Fig. 2 we can see that, the calculation volume of MPC is drastically reduced compared with the time-triggered mechanism. Moreover, the ACC system can also be triggered when MATI reaches.

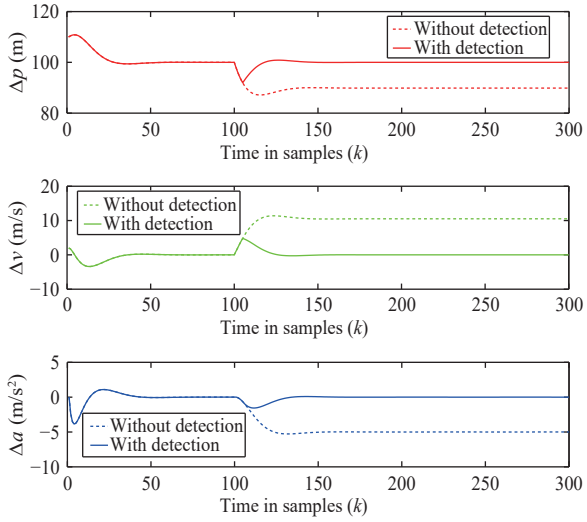

Fig. 1. Position, velocity, acceleration signals with and without χ^2 attack detection mechanism.

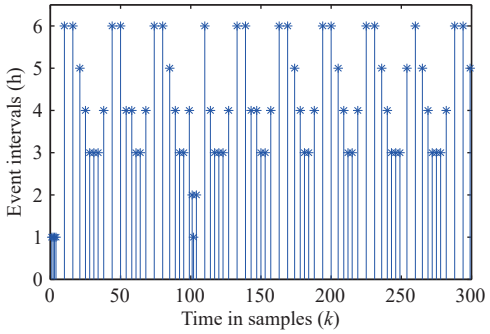

Fig. 2. Event-triggered instants and intervals.

Conclusion: In this letter, a resilient MPC method is investigated for ACC system under sensor attacks. To mitigate the impacts of sensor attacks on system dynamics, an intrusion detection mechanism is designed. To relieve the calculation burden in the implementation of MPC, traditional memory-based event-triggered scheme is improved by integrating of the maximum allowed time interval as a complementary event-triggered condition. Comparison simulations verify that both the proposed intrusion detection mechanism and the event-triggered scheme are effective.

Acknowledgments: This work was supported in part by A*STAR under its RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund-Pre Positioning (IAF-PP) (Award A19d6a 0053); the Agency for Science, Technology and Research (A*STAR) (I2001E0067) and the Schaeffler Hub for Advanced Research at NTU; National Natural Science Foundation of China (62203142); the China Postdoctoral Science Foundation (2022M710966, 2022TQ 0096). Any options, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of A*STAR.

References

[1] Z. Peng, D. Wang, Z. Chen, X. Hu, and W. Lan, "Adaptive dynamic surface control for formations of autonomous surface vehicles with uncertain dynamics," *IEEE Trans. Control Systems Technology*, vol. 21, no. 2, pp. 513–520, 2013.

[2] Z. Zuo, C. Liu, Q.-L. Han, and J. Song, "Unmanned aerial vehicles: Control methods and future challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 4, pp. 601–614, 2022.

[3] B. Wang and R. Su, " A distributed platoon control framework for connected automated vehicles in an urban traffic network," *IEEE Trans. Control Network Systems*, vol. 9, no. 4, pp. 1717–1730, 2022.

[4] Z. Peng, J. Wang, and Q.-L. Han, " Path-following control of autonomous underwater vehicles subject to velocity and input constraints via neurodynamic optimization," *IEEE Trans. Industrial Electronics*, vol. 66, no. 11, pp. 8724–8732, 2018.

[5] S. E. Li, Q. Guo, S. Xu, J. Duan, S. Li, C. Li, and K. Su, "Performance enhanced predictive control for adaptive cruise control system considering road elevation information," *IEEE Trans. Intelligent Vehicles*, vol. 2, no. 3, pp. 150–160, 2017.

[6] Z. Peng, C. Meng, L. Liu, D. Wang, and T. Li, "PWM-driven model predictive speed control for an unmanned surface vehicle with unknown propeller dynamics based on parameter identification and neural prediction," *Neurocomputing*, vol. 432, pp. 1–9, 2021.

[7] Y. Luo, T. Chen, S. Zhang, and K. Li, " Intelligent hybrid electric vehicle acc with coordinated control of tracking ability, fuel economy, and ride comfort," *IEEE Trans. Intelligent Transportation Systems*, vol. 16, no. 4, pp. 2303–2308, 2015.

[8] K. Zhang, L. Yang, and J. Tan, "SEMI-global finite-time stabilization of saturated spacecraft rendezvous system by dynamic event-triggered and self-triggered control," *IEEE Trans. Aerospace Electronic Systems*, vol. 58, no. 6, pp. 5030–5042, 2022.

[9] I. Ahmad, X. Ge, and Q.-L. Han, " Decentralized dynamic event-triggered communication and active suspension control of in-wheel motor driven electric vehicles with dynamic damping," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 5, pp. 971–986, 2021.

[10] L. Huang, J. Wang, E. Kung, Y. Mo, J. Wu, and L. Shi, "Stochastic event-based sensor schedules for remote state estimation in cognitive radio sensor networks," *IEEE Trans. Automatic Control* , vol. 66, no. 5, pp. 2407–2414, 2021.

[11] K. Zhang, B. Zhou, and G. Duan, " Event-triggered and self-triggered control of discrete-time systems with input constraints," *IEEE Trans. Systems, Man, Cybernetics: Systems*, vol. 52, no. 3, pp. 1948–1957, 2022.

[12] E. Tian and C. Peng, " Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks" *IEEE Trans. Cybernetics*, vol. 50, no. 11, pp. 4610–4618, 2020.

[13] R. Su, "On decidability of existence of nonblocking supervisors resilient to smart sensor attacks," arXiv preprint arXiv: 2009.02626, 2020.

[14] Zhang, H. Xue, S. Gao, X. Zuo, and J. Zhang, " Adaptive cooperative fault-tolerance tracking control for multi-agent system with hybrid actuator faults and multiple unknown control directions," *Expert Systems Applications*, vol. 197, p. 116711, 2022.

[15] Z. Hu, S. Liu, W. Luo, and L. Wu, " Resilient distributed fuzzy load frequency regulation for power systems under cross-layer random denial-of-service attacks," *IEEE Trans. Cybernetics* , vol. 52, no. 4, pp. 2396–2406, 2022.

[16] R. Ma, P. Shi, and L. Wu, "Sparse false injection attacks reconstruction via descriptor sliding mode observers," *IEEE Trans. Automatic Control*, vol. 66, no. 11, pp. 5369–5376, 2021.

[17] X. Jin, W. M. Haddad, Z.-P. Jiang, and K. G. Vamvoudakis, "Adaptive control for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," in *Proc. IEEE Conf. Decision Control*, 2018, pp. 2810–2815.

[18] Z. Xu, B. Xi, G. Yi, and D. Wang, "A novel model for fully closed-loop system of hemispherical resonator gyroscope under force-to-rebalance mode," *IEEE Trans. Instrumentation Measurement* , vol. 69, no. 12, pp. 9918–9930, 2020.

[19] Z. Hu, S. Liu, W. Luo, and L. Wu, "Credibility-based secure distributed load frequency control for power systems under false data injection attacks," *IET Generation, Transmission & Distribution*, vol. 14, no. 17, pp. 3498–3507, 2020.

[20] Z. Hu, S. Liu, L. Yang, and L. Wu, "Distributed fuzzy filtering for load frequency control of non-linear interconnected power systems under cyber-physical attacks," *IET Control Theory & Applications* , vol. 14, no. 4, pp. 527–538, 2020.

[21] S. Ding, X. Xie, and Y. Liu, "Event-triggered static/dynamic feedback control for discrete-time linear systems," *Information Sciences*, vol. 524, pp. 33–45, 2020.

[22] L. Ding, J. Li, M. Ye, and Y. Zhao, " Fully distributed resilient cooperative control of vehicular platoon systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 937–940, 2022.