An Efficient Resilient MPC Scheme via Constraint Tightening Against Cyberattacks: Application to Vehicle Cruise Control

Milad Farsi[1], Shuhao Bian[1], Nasser L. Azad[1], Xiaobing Shi[2] and Andrew Walenstein[2]
[1]*Department of Systems Design Engineering, University of Waterloo, Waterloo, Canada*
[2]*BlackBerry Limited, Waterloo, Canada*

Keywords: Resilient Control, Robust Control, Model Predictive Control, Denial of Service Attack.

Abstract: We propose a novel framework for designing a resilient Model Predictive Control (MPC) targeting uncertain linear systems under cyber attack. Assuming a periodic attack scenario, we model the system under Denial of Service (DoS) attack, also with measurement noise, as an uncertain linear system with parametric and additive uncertainty. To detect anomalies, we employ a Kalman filter-based approach. Then, through our observations of the intensity of the launched attack, we determine a range of possible values for the system matrices, as well as establish bounds of the additive uncertainty for the equivalent uncertain system. Leveraging a recent constraint tightening robust MPC method, we present an optimization-based resilient algorithm. Accordingly, we compute the uncertainty bounds and corresponding constraints offline for various attack magnitudes. Then, this data can be used efficiently in the MPC computations online. We demonstrate the effectiveness of the developed framework on the Adaptive Cruise Control (ACC) problem.

1 INTRODUCTION

Resilient control refers to the capability of a control system to maintain stable and optimal performance despite cyber-attacks (Sandberg et al., 2022), disturbances, uncertainties, and faults. Traditional control systems assume ideal conditions, leading to performance degradation or failure during unexpected events. Resilient controllers enhance robustness and adaptability, especially against cyber-attacks in critical systems. In the context of modern vehicles vulnerable to cyber threats, successful attacks can cause loss of control, safety compromises, and harm to passengers (Ju et al., 2022). Resilient control techniques detect, mitigate, and recover from cyber-attacks, preserving vehicle functionality and safety in adverse conditions.

Denial of Service (DoS) as one of the well-known cyber attacks have become increasingly prevalent in today's digital landscape that can gravely affect modern vehicle systems (Biron et al., 2018). These attacks aim to disrupt or disable the targeted system's services or resources, making them unavailable to legitimate users. Therefore, different techniques are employed in the literature to mitigate potential damages caused by such attacks. Game theory provides a framework for modeling strategic interactions and decision-making processes during cyber attacks (Gupta et al., 2016; Huang et al., 2020). Moreover, event-triggered control methods have been popular considering their advantages in cyber-physical systems, including vehicle control (Xiao et al., 2020; Wu et al., 2022).

Robust Model Predictive Control (RMPC) as a subcategory of Model Predictive Control (MPC) techniques is a powerful control framework that excels at handling uncertainty and disturbance in real-world applications (Bemporad and Morari, 2007). The inherent ability of RMPC to explicitly account for uncertainties makes it particularly well-suited for complex systems operating in dynamic environments. RMPC encompasses various approaches to handle uncertainties and disturbances in control systems. Min-Max RMPC approaches formulate the control problem as a min-max optimization, where the objective is to minimize online the worst-case performance subject to constraints (Raimondo et al., 2009). However, these techniques can involve overly expensive computations. Tube-based RMPC constructs an invariant set, known as the robust tube, that captures the possible system trajectories considering the uncertainties (Langson et al., 2004; Sakhdari and Azad, 2018). By formulating the optimization problem within this tube, the system stability and constraint satisfaction are obtained. In (Mayne et al., 2005), the authors

Farsi, M., Bian, S., Azad, N., Shi, X. and Walenstein, A.
An Efficient Resilient MPC Scheme via Constraint Tightening Against Cyberattacks: Application to Vehicle Cruise Control.
DOI: 10.5220/0012190900003543
In *Proceedings of the 20th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2023) - Volume 1*, pages 674-682
ISBN: 978-989-758-670-5; ISSN: 2184-2809

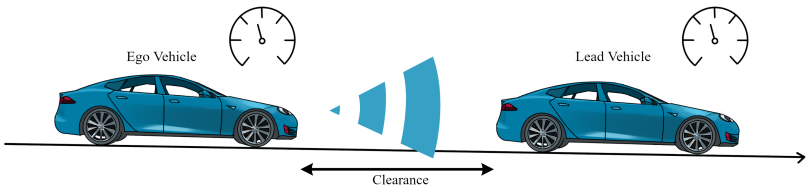

Figure 1: A view of the Adaptive Cruise Control (ACC) problem.

address RMPC problem in the presence of bounded disturbances for constrained linear discrete-time systems.

In (Aubouin-Pairault et al., 2022), to address the resilience issue in maintaining system operation under repeated DoS attacks, the concept of μ-step Robust Positively Invariant (μ-RPI) sets is introduced. These sets aim to restrict the impact of attacks, ensuring that any deviation from nominal operation remains limited in time and/or magnitude. Although such approaches offer different perspectives on robust control design and enable the handling of uncertainties and disturbances efficiently, they may result in rather conservative and computationally expensive solutions.

Constraint-tightening techniques involve iteratively refining the constraints in an optimization problem to enforce robustness (Köhler et al., 2018). In (Bujarbaruah et al., 2021), the authors demonstrated that by selecting appropriate terminal constraints and employing an adaptive horizon strategy, constraint tightening may not necessarily result in excessively conservative behavior where its Region of Attraction (ROA) can be as large as 98% of the tube-based techniques, such as (Langson et al., 2004). More importantly, it can run 15x faster.

Building upon this RMPC approach, in this paper, we develop an efficient resilient control framework against a class of cyber-attacks that can be potentially employed in real-time as an alternative to the current MPC implementations. Our approach involves the computation of a set of uncertain models that encompasses different levels of the strength of DoS attacks, as well as accounting for potential noise and unmodeled dynamics. Through an iterative scheme, we employ the Kalman filter to detect the occurrence of an attack. Subsequently, in the control loop, we estimate the intensity of the attack and adaptively evaluate the control based on the models pre-computed for different circumstances specifically. Hence, our contributions include: obtaining an overapproximate model with additive and parametric uncertainties based on a practical problem formulation, developing a resilient control framework that can be employed as an extension of (Bujarbaruah et al., 2021) against DoS, and validating it on the Adaptive Cruise Control (ACC) problem, illustrated in Fig.1.

The rest of the paper is organized as follows. In Section 2, we formulate the problem. Section 3 presents the resilient control framework and outlines the algorithms designed based on the obtained results. In Section 4, we summarize a commonly used anomaly detection method. In Section 5, we present a case study to validate and compare the proposed approach in the simulation environment.

Notations. We denote n-dimensional Euclidean space by $\mathbb{R}^n$, and the space of positive reals with the subscript as $\mathbb{R}^n_+$. We further denote by $|X|$ the absolute value of a variable X, where for non-scalars, it represents the component-wise absolute value. $||x||$ denotes the 2-norm of a vector $x \in \mathbb{R}^n$. A diagonal square matrix A with elements $a_1,\ldots,a_n$ on the diagonal is shortened as $A = \text{diag}([a_1,\ldots,a_n])$. We use the upper script as x^k for discrete-time signals, and $x^{k|j}$ represents the estimation of x^k at the time j. $diag(x_1,x_2,...,x_n)$ denotes a diagonal matrix of the elements $x_1,x_2,...,x_n$. The set $G[a,b]$ represents a grid with the bounds a and b.

2 PROBLEM FORMULATION

In this section, considering a class of systems, we formulate the effect of the DoS attack. Accordingly, we define the problem of interest.

Consider the following system

$$\dot{x} = Ax + \Delta(x) + Bu \tag{1}$$

where $x \in D \subset \mathbb{R}^n$ and $u \in U \subset \mathbb{R}^m$ are respectively the state and control input, and take values on the compact convex sets D and U. System matrices are given as $A \in \mathbb{R}^{n\times n}$, and $B \in \mathbb{R}^{n\times m}$. Furthermore, the unmodeled dynamics are given by $\Delta : D \to \mathbb{R}^n$.

Assumption 1. *Elements of $\Delta(x)$ are assumed to be a Lipschitz continuous function of the state, i.e. $\exists \eta \in \mathbb{R}^n_+$ such that we have*

$$|\Delta_i(x_0) - \Delta_i(y_0)| \leq \eta_i \|x_0 - y_0\|,$$

for any $x_0, y_0 \in D$, where $i \in \{1,\ldots,n\}$.

While more general classes of dynamical systems do exist, the specific formulation we adopt in this study enables efficient analysis of a wide range of engineering problems, encompassing domains such as robotics, automotive, power systems, and more. This formulation can be also applied to the ACC system, which is the focus of our investigation in this paper. In the subsequent section, we will proceed to model the impact of a DoS attack on this particular system.

2.1 Attack Model

Regarding the fact that the attacks are implemented in the cyber layer, one needs to take into account the interactions in the discrete space. Therefore, let us consider the Euler approximation of (1) under actuator attack and with measurement noise as the following

$$\begin{cases} x^{t+1} = A_\tau x^t + \Delta(x^k)\tau + B\tau u^t + d^t, & t \notin \alpha \\ x^{t+1} = A_\tau x^k + \Delta(x^k)\tau + d^t, & t \in \alpha \end{cases} \tag{2}$$

$$y^t = C(I+\chi^t)x^t + \varepsilon^t, \qquad t \in \{0,1,\dots\} \tag{3}$$

where τ is the sampling time and $A_\tau = A\tau + I$ and $B_\tau = B\tau$ are discretized system matrices. Moreover, we assume that we can measure all the states, i.e. $C = I$. Then, the term d^t lumps together the discretization error and some bounded input disturbance. Moreover, we denote the set of time steps during which the DoS attack is active using $\alpha \in S_\alpha$, where S_α represents the set of all possible sequences of attacks.

Moreover, to ensure a rather practical model of the problem we take also into account the effect of noise. Therefore, the measurements are given by $y^t \in \mathbb{R}^n$ for steps $t \in \{0,1,\dots\}$ that are affected by noise. The vector $\varepsilon^t \in \mathbb{R}^n$ and the diagonal matrix $\chi = \text{diag}([\chi_1,\dots,\chi_n]) \in \mathbb{R}^{n\times n}$ are the bounded additive and multiplicative noises affecting the measurements, i.e $|\varepsilon^t| \le \bar{\varepsilon} \in \mathbb{R}^n_+$ and $|\chi^t| \le \bar{\chi}$, where $\bar{\chi}$ is a diagonal matrix with positive values. The distributions of the noises applied are not necessarily uniform. In fact, the formulation can accommodate other distributions, such as truncated Gaussian noise.

2.2 Objective

Given the definition of the system under DoS attack, we can define the constrained control problem which is solved at each time step t in the rolling horizon fashion for the horizon length of N as

$$J^{*t} = \min_{u^t(.)} \sum_{k=t}^{t+N-1} ({y^k}^T Q y^k + {u^k}^T R u^k) + {y^N}^T Q^N y^N,$$
$$\text{subject to} \quad (2), (3),$$
$$x^k \in D, \text{ and } u^k \in U, \tag{4}$$

for all sequences of attacks $\alpha \in S_\alpha$, noises, and disturbances within their sets of definitions. The objective defined includes stage and terminal costs, respectively.

Addressing the uncertainties inherent in the model, it becomes apparent that a direct approach to solving the optimization problem is not viable. In light of this, the subsequent section explores an alternative technique that can effectively handle the problem by transforming it into the standard form, incorporating parametric and additive uncertainties. This approach capitalizes on the existence of efficient techniques specifically designed to tackle such formulations.

3 RESILIENT FRAMEWORK

In this section, we present the components required for establishing the proposed resilient control in detail. Having the model of the attack defined, we first derive an equivalent uncertain model that facilitates efficient analyses. Second, we present the tightening-based solutions for addressing this problem. Finally, we summarize the entire framework by presenting two algorithms that encapsulate the proposed resilient control approach.

3.1 Equivalent Uncertain Model

The following lemma provides regulation for the lumped disturbance present in the model.

Lemma 1. *The disturbance term d^t is bounded by $\bar{d} \in \mathbb{R}^+$.*

Proof. Considering the Assumption 1 and compact domains, it can be shown that the local truncation error resulting from the discretization remains bounded for all $(x^t, u^t) \in D \times U$. Moreover, according to our assumption, the system may be prone to some bounded input disturbance. Therefore, the lumped disturbance d^t is also bounded by some $\bar{d} \in \mathbb{R}^n_+$. □

Assuming a periodic DoS attack, as a well-known class of attacks (Cetinkaya et al., 2019), we can rewrite the system by averaging both modes of (2) as

$$x^{t+1} = A_\tau x^t + \Delta(x^t)\tau + B_\tau u^t(1-\omega^t) + d^t, \tag{5}$$

where $\omega^t \in [0,1]$ takes continuous values in this closed interval representing the intensity of the DoS attack.

Assumption 2. *The attack signals ω^t is bounded and the estimated values of the upper bounds are known at each time step, i.e. $\exists \bar{\omega} \in \mathbb{R}^+$ such that $|\omega^t| \leq \bar{\omega}$ for $k \in \{0,\dots,N-1\}$.*

Assumption 2 automatically holds for the type of attack considered and the problem formulation where a worst case of ω^t values is given by 1. However, in practice, based on the estimations of the attack intensity, smaller values than 1 may be considered for $\bar{\omega}$ at each step t.

In what follows, we investigate how the measurements deviate from the predictions given by the nominal dynamics

$$\bar{F}(x^t,u^t) = A_\tau x^t + B_\tau u^t.$$

Therefore, consider

$$\begin{aligned}
&y^{t+1} - \bar{F}(x^t,u^t)\\
&\quad = (I+\chi^{t+1})x^{t+1} + \varepsilon^{t+1} - A_\tau x^t - B_\tau u^t\\
&\quad = (I+\chi^{t+1})\Big(A_\tau x^t + \Delta(x^t)\tau + B_\tau u^t(1-\omega^t) + d^t\Big)\\
&\qquad + \varepsilon^{t+1} - A_\tau x^t - B_\tau u^t\\
&\quad = \chi^{t+1}A_\tau x^t + \big((I+\chi^{t+1})(1-\omega^t) - I\big)B_\tau u^t\\
&\qquad + (I+\chi^{t+1})\big(\Delta(x^t)\tau + d^t\big) + \varepsilon^{t+1}\\
&\quad = \chi^{t+1}A_\tau x^t + (\chi^{t+1} - (I+\chi^{t+1})\omega^t)B_\tau u^t\\
&\qquad + (I+\chi^{t+1})\Delta(x^t)\tau + (I+\chi^{t+1})d^t + \varepsilon^{t+1},
\end{aligned} \tag{6}$$

where we used (5) in the derivations. Starting with the first two terms, let us define the convex polytopic sets Π_A and Π_B as below that contain the uncertainty corresponding to A_τ and B_τ matrices of the nominal dynamic, respectively,

$$\begin{aligned}
\Pi_A &= \mathrm{conv}(\{\chi^{t+1}A_\tau | \chi^{t+1} \in \chi_v\}),\\
\Pi_B &= \mathrm{conv}(\{(\chi^{t+1} - (I+\chi^{t+1})\omega^t)B_\tau | \chi^{t+1} \in \chi_v,\\
&\qquad \omega^t \in \{0,\bar{\omega}\}\}),
\end{aligned} \tag{7}$$

for all vertices χ_v given by the extreme values of χ^{t+1}. Regarding that $\bar{\chi}$ is diagonal, χ_v can be easily calculated.

In the subsequent step, the remaining terms are treated as additive uncertainty. It is important to highlight that, in order to obtain specific bounds for each system dynamic specifically, component-wise calculations are employed, rather than considering a norm-based approach. In this regard, the non-scalar bounds defined and the Lipschitz constants in Assumption 1 facilitate these computations. Hence, we aim for a bound using equation (6) that yields

$$\begin{aligned}
&|y^{t+1} - (\bar{F}(x^t,u^t) + \chi^{t+1}A_\tau x^t\\
&\qquad + (\chi^{t+1} - (I+\chi^{t+1})\omega^t)B_\tau u^t)|\\
&\quad = |(I+\chi^{t+1})\Delta(x^t)\tau + (I+\chi^{t+1})d^t + \varepsilon^{t+1}|\\
&\quad \leq |(I+\chi^{t+1})\Delta(x^t)\tau| + |(I+\chi^{t+1})d^t| + |\varepsilon^{t+1}|\\
&\quad \leq |(I+\chi^{t+1})\tau||\Delta(x^t)| + |(I+\chi^{t+1})d^t| + |\varepsilon^{t+1}|\\
&\quad \leq |(I+\chi^{t+1})\tau|\eta\|x^t\| + |(I+\chi^{t+1})d^t| + |\varepsilon^{t+1}|\\
&\quad \leq |(I+\bar{\chi})\tau|\|x^t\|\eta + (I+\bar{\chi})\bar{d} + \bar{\varepsilon},
\end{aligned} \tag{8}$$

where we used Assumption 1 to derive the last two steps. This provides a bound for the remaining terms while one can use $\max_{x^t \in D}(\|x^t\|)$ to bound $\|x^t\|$. However, it may not offer a useful bound if η is not small. As an alternative, we can set different values for the bounds based on the current value of x^t, instead. In this case, considering that we do not measure x^t exactly, we can employ the measurements through (3) to obtain

$$\begin{aligned}
\|x^t\| &= \|(I+\chi^{t+1})^{-1}\|\|(y^t - \varepsilon^{t+1})\|\\
&\leq \|(I+\chi^{t+1})^{-1}\|(\|y^t\| + \|\varepsilon^{t+1}\|)\\
&\leq \|(I-\bar{\chi})^{-1}\|(\|y^t\| + \|\bar{\varepsilon}\|).
\end{aligned} \tag{9}$$

We summarize the computations by utilizing a discrete-time linear model that incorporates parametric and additive uncertainty. This model serves as an overapproximation of the continuous-time dynamics (1) in the presence of a DoS attack and uncertainty,

$$x^{t+1} = (A_\tau + \hat{\Delta}_A)x^t + (B_\tau + \hat{\Delta}_B)u^t + \hat{d}^t, \tag{10}$$

where $|\hat{d}^t| \leq \hat{\delta}$ with

$$\begin{aligned}
\hat{\delta} &= |(I+\bar{\chi})\tau|\|(I-\bar{\chi})^{-1}\|(\|y^t\| + \|\bar{\varepsilon}\|)\eta\\
&\quad + (I+\bar{\chi})\bar{d} + \bar{\varepsilon},
\end{aligned} \tag{11}$$

$\hat{\Delta}_A \in \Pi_A$ and $\hat{\Delta}_B \in \Pi_B$, with defined Π_A and Π_B by (7).

3.2 Resilience via Constraint Tightening

In this section, we summarize the constraint tightening technique employed for solving the RMPC problem. Accordingly, we deliver the resilient framework proposed using also the results obtained in the previous section.

Regarding the model in (10), although utilizing fixed bounds can be effective for addressing slight model uncertainty and noise effects, it may not adequately capture the impact of DoS attacks, which is considered the major source of uncertainty in the model. To address this, we propose a more adaptable approach that can accommodate various strengths of attacks while maintaining satisfactory system performance. Moreover, as previously suggested, the Lipschitz values may be large leading to large additive bounds in (11) that can be also addressed by a similar approach.

In order to overcome these limitations, let us define different quantities of bounds for ω^t and $\|y^t\|$ as $[\omega]_q$ and $[\|y\|]_q$ that are taken from a set of grid points, i.e. $([\omega]_j, [\|y\|]_i) \in G[0,\bar{\omega}] \times G[0, \sup(\|y\|)]$ for $j = 1,\ldots,N_\omega$ and $i = 1,\ldots,N_d$, where N_ω and N_d are the numbers of grid points for each dimension. Then, by online observations, one needs to ensure that the conditions $\omega^t \leq [\omega]_q$ and $\|y^t\| \leq [\|y\|]_q$ hold by choosing a suitable q from the set of indices $\{1,\ldots,N_\omega \times N_d\}$.

By employing a similar scheme as (Bujarbaruah et al., 2021), we consider an adaptive prediction horizon where at each time step, we solve the problem for different horizon lengths $N_t \in \{1,\ldots,N\}$, and proceed with the one with the least cost. However, there is a key distinction in our approach as we take into account a collection of uncertain models, which are defined by different bounds corresponding to varying levels of attack intensity. Accordingly, we apply one of the following two approaches in handling the uncertainties depending on the value of N_t.

- Case $N_t = 1$: Accordingly, the robust MPC problem is exactly solved for a horizon length of one. For this purpose, assuming that there exists a feedback gain K_q such that $(A_\tau + \hat{\Delta}_A) + (B_\tau + \hat{\Delta}_{Bq})K_q$ is stable for all $\hat{\Delta}_A \in \Pi_A$ and $\hat{\Delta}_{Bq} \in \Pi_{Bq}$, we can construct the terminal sets X_q^N as the maximal robust positive invariant set for $x^{t+1} = \Big((A_\tau + \hat{\Delta}_A) + (B_\tau + \hat{\Delta}_{Bq})K_q\Big)x^t + \hat{d}^t$, with $q \in \{1,\ldots,N_\omega \times N_d\}$. Therefore, in addition to the state and control input constraints, we need to satisfy the condition

$$\Big((A_\tau + \hat{\Delta}_A) + (B_\tau + \hat{\Delta}_{Bq})K_q\Big)x^t + \hat{d}^t \in X_q^N \quad (12)$$

  in the optimization problem, where X_q^N is a convex set defining the terminal set for the model given by the index q. It should be noted that, Δ_{Bq} and $|\hat{d}^t| \leq \hat{\delta}_q$ are characterized by the quantities $[\omega]_q$ and $[\|y\|]_q$ for given index q, according to relations (7) and (11).
- Case $N_t > 1$: Given the computational intensity of the method employed in the previous case for multi-step predictions, an alternative approach is taken. Bounds are utilized to over-approximate system uncertainty, rather than precise calculations by using the technique found in (Goulart et al., 2006). This allows for the treatment of all uncertainties as a net-additive component, utilizing a more constructive technique. The adoption of this approach aims to mitigate the computational burden while still effectively accounting for system uncertainties.

The presented resilient framework can be effectively implemented in two parts. In the first part, the model and uncertainty bounds are processed to characterize the constraints. These computations are conducted offline in advance which facilitates the preparation of constraints. By performing these computations beforehand, the constraints can be readily available for subsequent utilization. In Algorithm 1, which presents the offline procedure, we grid the space $G[0,\bar{\omega}] \times G[0, \sup(\|y\|)]$ to obtain different values $[\omega]_q$ and $[\|y\|]_q$. Then, we use (7) and (11) to calculate the corresponding bounds for all q.

Data: System matrices, $\bar{\chi}$, $\bar{\varepsilon}$, domain and control constraints $\leftarrow D$ and U

Result: $\hat{\Delta}_A$, $\hat{\Delta}_{Bq}$, and $\hat{\delta}_q$. Terminal sets X_q^N $\forall([\omega]_q, [\|y\|]_q)$ and weights Q^N.

% Number of grid points
N_ω and $N_d \leftarrow$ positive integers ;
% Grid points
$\omega_{List} \leftarrow \text{linspace}(0, \bar{\omega}, N_\omega)$;
$Y_{List} \leftarrow \text{linspace}(0, \sup(\|y\|), N_d)$;
%Using relation (7):
Calculate $\hat{\Delta}_A$;
for $([\omega]_q, [\|y\|]_q)$ *in* $\omega_{List} \times Y_{List}$ **do**
  %Using relation (7):
  Calculate $\hat{\Delta}_{Bq}$;
  % Using relation (11):
  Calculate $\hat{\delta}_q$;
  % Employing (Bujarbaruah et al., 2021):
  Calculate the terminal sets X_q^N;
  Calculate Q^N ;
end

Algorithm 1: Offline computations of the bounds and state constraints.

The second part of the implementation involves the utilization of the pre-determined constraints in an online optimization-based control approach. During the online phase, these prepared constraints are incorporated into an optimization framework to generate real-time control actions by exploiting (Bujarbaruah et al., 2021). For this purpose, we obtain an estimation of the intensity of an ongoing attack using an anomaly detection method and choose applicable $[\omega]_q$ and $[\|y\|]_q$. By integrating their corresponding constraints into the optimization process, the control approach ensures that the system operates within desired limits while effectively addressing uncertainties. This procedure is summarized in Algorithm 2.

Remark 1. *The offline computations enable the efficient characterization of constraints, resulting in*

computational time savings during online implementation. Furthermore, using a hybrid technique employing the two cases according to N_t facilitates a responsive optimization process, thereby potentially enabling realtime resilient control actions in real-world applications.

Data: A_τ, B_τ, $\hat{\Delta}_A$, $\hat{\Delta}_{Bq}$, and $\hat{\delta}_q$ $\forall([\omega]_q, [\|y\|]_q)$. X_q^N $\forall([\omega]_q, [\|y\|]_q)$ and weights Q^N.
Result: u^t
%initialization
$N \leftarrow$ positive integer;
for $t = 0, 1, \ldots$ **do**
  Measure y^t;
  Detect attack;
  Estimate $\hat{\omega}^t$ based on attack detected;
  Choose $([\omega]_q, [\|y\|]_q)$ based on $\hat{\omega}^t$ and y^t;
  for $N_t = 1, 2, \ldots, N$ **do**
    Solve RMPC for $\hat{\Delta}_A, \hat{\Delta}_{Bq}, \hat{\delta}_q, X_q^N, Q^N$;
  end
  Apply u^t: arg $\min_{N_t} J^*$;
end

Algorithm 2: Online computation of resilient control value.

4 ANOMALY DETECTION

To implement RMPC, we need to observe the intensity of the launched attack. Therefore, the Kalman filter (Bai et al., 2017; Bai and Gupta, 2014) technique is utilized to detect the launched attack. Accordingly, the system states are estimated, and the resulting residuals are employed to detect the attack.

The residual at tth step is defined as

$$r = y^t - y^{t|t-1} \tag{13}$$

s.t.

$$r = y^t - C\hat{x}^{t|t-1}. \tag{14}$$

Then, according to (Mo et al., 2010; Miao et al., 2014), we can determine if the system is under attack.

$$\begin{cases} t \notin \alpha, & \text{if } r^T \mathcal{P}^{-1} r \leq T, \\ t \in \alpha, & \text{if } r^T \mathcal{P}^{-1} r > T, \end{cases} \tag{15}$$

where $T \in \mathbb{R}_+$ is the threshold of the corresponding residue, to be tuned by the user. Moreover, $\mathcal{P}$ represents the covariance matrix of the residue r, and T is the threshold. According to (15), we can determine whether the system is under attack.

In the next section, the detection results are presented in more detail. For improved results, robust Kalman filters (Elsisi et al., 2023) can be exploited alternatively.

5 SIMULATION RESULTS

To demonstrate the efficacy of the proposed approach under DoS attacks, we validate Algorithm 1 and 2 on the ACC problem. Moreover, we present the details of the detection procedure and discuss some comparison results. All the simulations are conducted in Matlab on the Windows operating system with the hardware configuration of AMD Ryzen 9, 16-Core, 3.40 GHz, and 64GB of RAM.

As shown in Fig. 1, ACC system consists of two vehicles, one of which is the ego vehicle and the other is the lead vehicle. The control objective defined for the ego vehicle is to maintain the distance from the lead vehicle while satisfying the state and control constraints.

To describe the model, we employ the state variables $x = [\delta d, \delta v, \dot{v}_h]^T$ defined as the followings:

- δd is defined as the distance error which is the difference between the actual distance d and the desired distance d_r from the lead vehicle, i.e $\delta d = d - d_r$.
- δv denotes the velocity difference between the lead vehicle v_p and the ego vehicle v_h.
- $\dot{v}_h$ represents the acceleration of the ego vehicle.

According to (Takahama and Akasaka, 2018; Al-Gabalawy et al., 2021), the longitudinal dynamics of the ego vehicle is given as

$$\begin{aligned} \dot{v}_h &= A_f v_h + B_f u, \\ a_f &= C_f v_h, \end{aligned} \tag{16}$$

where a_f is the traction force of the vehicle converted to acceleration

$$A_f = -\frac{1}{T_{eng}}, \quad B_f = -\frac{K_{eng}}{T_{eng}}, \text{ and } \quad C_f = 1. \tag{17}$$

Furthermore, T_{eng} is the constant of acceleration of the engine, and K_{eng} is the gain of the engine.

In addition, the reference distance is defined with respect to the velocity of the ego vehicle using

$$d_r = T_{hw} v_h + d_0 \tag{18}$$

where T_{hw} is the constant time headway, and d_0 is the safety clearance when the lead vehicle comes to a full stop. However, for simplicity, it is assumed that the lead vehicle has some positive velocity, hence, $d_0 = 0$ can be used safely.

According to (16), (18), and the defined state vector x, we can obtain the discrete-time model as (2) with $A_\tau = I + \begin{bmatrix} 0 & 1 & -T_{hw} \\ 0 & 0 & -1 \\ 0 & 0 & A_f \end{bmatrix} \tau$, $B_\tau = \begin{bmatrix} 0 \\ 0 \\ B_f \end{bmatrix} \tau$ and $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

For more details, we refer the readers to (Takahama and Akasaka, 2018; Al-Gabalawy et al., 2021). Also, similar to these works, we set the values of the parameters T_{hw}, T_{eng}, and K_{eng}, as shown in Table 1.

Table 1: Parameters of ACC model.

T_{hw}	T_{eng}	K_{eng}
1.6	0.46 sec	0.732

5.1 Detection

In the simulated attack scenario, we generate a periodic attack characterized by varying active lengths for each period. Fig. 2 illustrates the attack signal profile that initiates at $t = 2$ seconds.

To detect this attack, we employ the Kalman filter approach, with noise covariances $Q_f = diag(0.01, 0.01, 0.01)$, $R = diag(0.01, 0.01, 0.01)$, the sampling time $t_{sample} = 0.01$, and the initial covariance matrix $P_{init} = diag(0.1, 0.1, 0.1)$. The residuals obtained from the detection process are also depicted in the same figure, showcasing the impact of the attack events. By appropriately setting threshold values, we are able to successfully detect the attack, as demonstrated in Fig. 2. It is important to note that while some false positive and negative cases may occur, the Kalman filter detector is effective in detecting DoS attacks in the majority of instances.

The bottom graph in Fig. 2 shows the results for the estimation of attack intensity, i.e. $\hat{\omega}^t$, together with the exact signal ω^t, which is obtained based on the true attack signal. In fact, we use a backward-moving average of the attack signal to generate such an estimation and it illustrates how effectively one can reconstruct a signal representing the attack intensity. By comparing the estimated attack strength $\hat{\omega}^t$ with the exact signal, we observe a close correspondence between the two. This demonstrates the ability of the estimation process to capture and reconstruct the features of the attack signal that can be used to establish the resilient controller accordingly.

5.2 Control

For validation, we apply the resilient control approach proposed on the ACC system specified. For the control computations, we consider a discretized system $\tau = 0.2$ sec. To characterize the objective function (4), we set $Q = diag(10, 10, 10)$, $R = 2$, and $N = 5$ for all simulation if not mentioned otherwise. Moreover, the state and control are constrained within intervals $[-100, -100, -100]^T < x^t < [10, 100, 100]^T$ and $-20 < u^t < 20$, respectively.

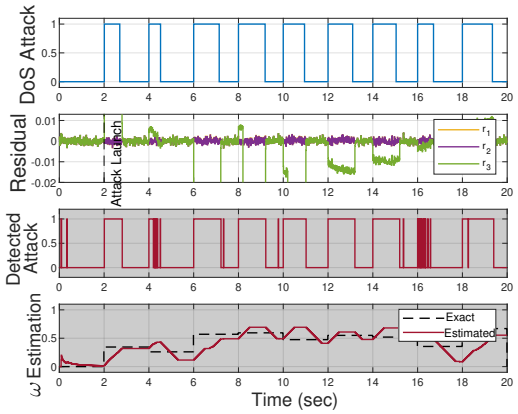

Figure 2: The result of anomaly detection together with the estimation of the strength of attack ω^t.

For the preparation of constraints, we employ the proposed Algorithm 1 in Matlab, with $N_\omega = 10$, $N_d = 3$, $|\chi| \leq diag([1,1,1]) \times 10^{-2}$, $|\varepsilon| \leq [0.1, 0.1, 0.1]^T$, and $\eta = [1,1,1] \times 10^{-2}$.

Having the uncertainty bounds and the terminal sets calculated in our deposit, Algorithm 2 can be executed within the control loop to handle the attack profile discussed in the previous section. In Fig. 3, we present the evolutions of the ACC system under attack, controlled by the proposed resilient controller. The control plot demonstrates that the control signal becomes zero when a DoS attack is initiated, as it cannot be transmitted to the vehicle. Therefore, the control strategy must efficiently compensate for this absence of control during attack periods.

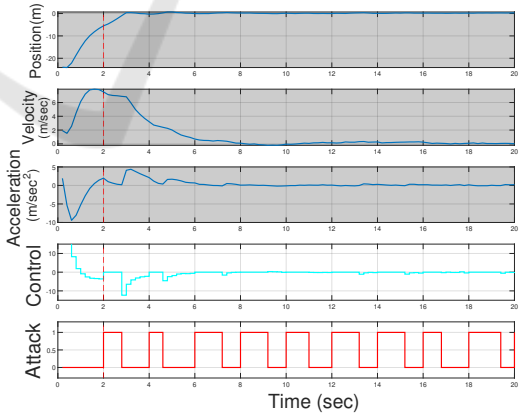

Figure 3: Details of the resilient control responses against DoS attack.

Regarding the system states, including relative position, velocity, and acceleration, the primary objective of the control is to regulate the system to the origin, represented by $x = [0,0,0]^T$. Remarkably, despite the occurrence of the DoS attack on the system, all the states effectively converge to zero starting

from a random initial condition with the utilization of the proposed resilient control strategy. These results clearly indicate the effectiveness and resilience of the proposed control approach in managing the impact of DoS attacks on the ACC system.

5.3 Comparison Results

For a better demonstration of the effectiveness of the proposed resilient control, we also apply the standard MPC in the same attack scenario and ACC system configuration. Therefore, we employ CasADi optimization library (Andersson et al., 2018) in Matlab.

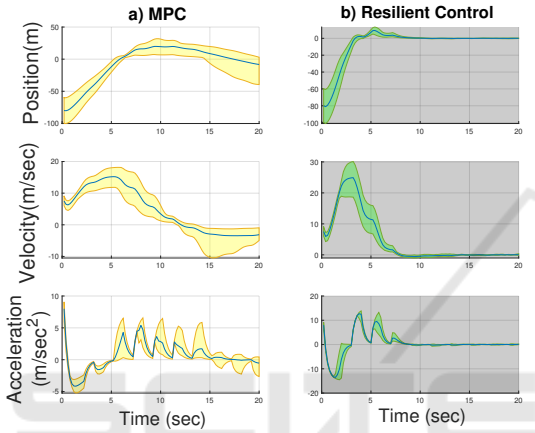

Figure 4: Comparison between MPC and the proposed resilient control for a set of initial conditions.

In Fig. 4, we illustrate the comparison between the proposed resilient control and MPC in terms of the convergence of system trajectories. For this result, we consider a set of initial conditions, then we show the mean and upper/lower bound of the trajectories using the line curves and the shaded areas, respectively. It is evident that the proposed method results in faster convergence while MPC fails to effectively regulate the system trajectories to zero. The performance can be also quantitatively compared by keeping track of the cost function over time, i.e. the summation in (4), for both techniques. These values of cost can be shown as two signals as in Fig. 5. In Table 2, the numerical values of costs are reported by averaging for all initial conditions. Accordingly, in the simulated scenario, the mean cost value shows about 38% improvement for the proposed approach in comparison to standard MPC.

Table 2: Comparison of mean cost values obtained.

MPC	Resilient Control	Improvement
9.2163×10^5	5.7300×10^5	38%

Computational Time. Finally, as a comparison of the computational complexity of the proposed approach, we illustrate the runtime results for both presented and MPC techniques in Fig. 6. We run the proposed technique in two different configurations with $N = 1$ and $N = 5$. By comparing these results, the basic MPC runs faster as expected since it solves a less complicated problem. However, the runtime results for both settings of the proposed technique are comparable to MPC, making it a potential candidate for replacing non-resilient controllers in real-world implementations. This is mostly because the main part of the computations is done offline using Algorithm 1.

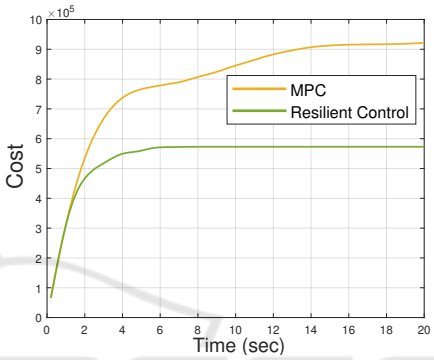

Figure 5: In this graph, by keeping track of the cost function for the proposed resilient control and MPC, we compare the performance, where the proposed method clearly outperforms by resulting in a lower control cost.

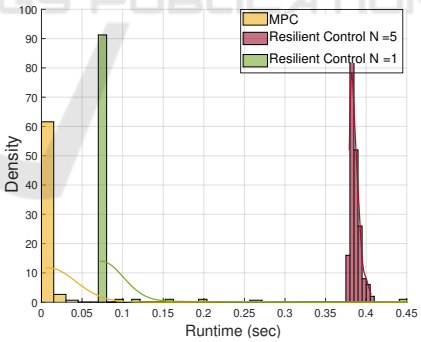

Figure 6: We compared the runtime results for both techniques: the basic MPC and two different configurations of the proposed method with $N = 1$ and $N = 5$.

5.4 Conclusion

This study proposed a novel framework for designing a resilient MPC system to handle uncertain linear systems under periodic DoS attacks. The DoS attack was modeled as an uncertain parameter-varying system with additive disturbance, and the Kalman filter was used for anomaly detection. An optimization-based resilient algorithm was developed using a ro-

bust constraint-tightening MPC approach. We implemented the approach to the ACC problem, showcasing its effectiveness in mitigating the impact of periodic attacks and ensuring system stability. Overall, the study provided a solution to enhance the resilience of control systems in the presence of DoS attacks. Incorporating robust attack detection methods and extending the framework to encompass various types of attacks can be potentially promising for future research.

REFERENCES

Al-Gabalawy, M., Hosny, N. S., and Aborisha, A.-h. S. (2021). Model predictive control for a basic adaptive cruise control. *International Journal of Dynamics and Control*, 9(3):1132–1143.

Andersson, J. A. E., Gillis, J., Horn, G., Rawlings, J. B., and Diehl, M. (2018). CasADi – A software framework for nonlinear optimization and optimal control. *Mathematical Programming Computation*.

Aubouin-Pairault, B., Perodou, A., Combastel, C., and Zolghadri, A. (2022). Resilient tube-based mpc for cyber-physical systems under dos attacks. *IFAC-PapersOnLine*, 55(6):278–284.

Bai, C.-Z. and Gupta, V. (2014). On kalman filtering in the presence of a compromised sensor: Fundamental performance bounds. In *2014 American Control Conference*, pages 3029–3034.

Bai, C.-Z., Gupta, V., and Pasqualetti, F. (2017). On kalman filtering with compromised sensors: Attack stealthiness and performance bounds. *IEEE Transactions on Automatic Control*, 62(12):6641–6648.

Bemporad, A. and Morari, M. (2007). Robust model predictive control: A survey. In *Robustness in identification and control*, pages 207–226. Springer.

Biron, Z. A., Dey, S., and Pisu, P. (2018). Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, 19(12):3893–3902.

Bujarbaruah, M., Rosolia, U., Stürz, Y. R., and Borrelli, F. (2021). A simple robust mpc for linear systems with parametric and additive uncertainty. In *2021 American Control Conference (ACC)*, pages 2108–2113. IEEE.

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2019). An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, 21(2):210.

Elsisi, M., Altius, M., Su, S.-F., and Su, C.-L. (2023). Robust kalman filter for position estimation of automated guided vehicles under cyberattacks. *IEEE Transactions on Instrumentation and Measurement*, 72:1–12.

Goulart, P. J., Kerrigan, E. C., and Maciejowski, J. M. (2006). Optimization over state feedback policies for robust control with constraints. *Automatica*, 42(4):523–533.

Gupta, A., Langbort, C., and Başar, T. (2016). Dynamic games with asymmetric information and resource constrained players with applications to security of cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 4(1):71–81.

Huang, Y., Chen, J., Huang, L., and Zhu, Q. (2020). Dynamic games for secure and resilient control system design. *National Science Review*, 7(7):1125–1141.

Ju, Z., Zhang, H., Li, X., Chen, X., Han, J., and Yang, M. (2022). A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective. *IEEE Transactions on Intelligent Vehicles*.

Köhler, J., Müller, M. A., and Allgöwer, F. (2018). A novel constraint tightening approach for nonlinear robust model predictive control. In *2018 Annual American Control Conference (ACC)*, pages 728–734. IEEE.

Langson, W., Chryssochoos, I., Raković, S., and Mayne, D. Q. (2004). Robust model predictive control using tubes. *Automatica*, 40(1):125–133.

Mayne, D. Q., Seron, M. M., and Raković, S. (2005). Robust model predictive control of constrained linear systems with bounded disturbances. *Automatica*, 41(2):219–224.

Miao, F., Zhu, Q., Pajic, M., and Pappas, G. J. (2014). Coding sensor outputs for injection attacks detection. In *53rd IEEE Conference on Decision and Control*, pages 5776–5781.

Mo, Y., Garone, E., Casavola, A., and Sinopoli, B. (2010). False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5967–5972.

Raimondo, D. M., Limon, D., Lazar, M., Magni, L., and ndez Camacho, E. F. (2009). Min-max model predictive control of nonlinear systems: A unifying overview on stability. *European Journal of Control*, 15(1):5–21.

Sakhdari, B. and Azad, N. L. (2018). Adaptive tube-based nonlinear mpc for economic autonomous cruise control of plug-in hybrid electric vehicles. *IEEE Transactions on Vehicular Technology*, 67(12):11390–11401.

Sandberg, H., Gupta, V., and Johansson, K. H. (2022). Secure networked control systems. *Annual Review of Control, Robotics, and Autonomous Systems*, 5:445–464.

Takahama, T. and Akasaka, D. (2018). Model predictive control approach to design practical adaptive cruise control for traffic jam. *International journal of automotive engineering*, 9(3):99–104.

Wu, J., Peng, C., Yang, H., and Wang, Y.-L. (2022). Recent advances in event-triggered security control of networked systems: a survey. *International Journal of Systems Science*, 53(12):2624–2643.

Xiao, S., Ge, X., Han, Q.-L., Cao, Z., Zhang, Y., and Wang, H. (2020). Resilient distributed event-triggered control of vehicle platooning under dos attacks. *IFAC-PapersOnLine*, 53(2):1807–1812.