A Resilient Design for Cyber Physical Systems under Attack

Yang Yan, Panos Antsaklis and Vijay Gupta

Abstract—One challenge for engineered cyber physical systems (CPSs) is the possibility for a malicious intruder to change the data transmitted across the cyber channel as a means to degrade the performance of the physical system. In this paper, we consider a data injection attack on a cyber physical system. We propose a hybrid framework for detecting the presence of an attack and operating the plant in spite of the attack. Our method uses an observer-based detection mechanism and a passivity balance defense framework in the hybrid architecture. By switching the controller, passivity and exponential stability are established under the proposed framework.

I. INTRODUCTION

In Cyber Physical Systems, the strong dependence on the cyberinfrastructure in the overall system increase the risk of cyber attacks, such as injection attacks. Security of cyber physical systems needs to be considered and designed carefully [1]. Cyber-physical security has now developed into a comprehensive discipline that extends classic fault detection, and complements cyber security [2]. The aim in this area is to build a resilient mechanism to make the system be aware of any attacks in progress and to adjust its dynamics if needed to guarantee desired performance even with attacks or failures.

Much interesting research has been done in this field and we can provide only a brief summary. Numerous papers have emphasized modeling and detecting adversarial attacks [3] [4] [5] [6]. In particular, Pasqualetti et al. [7] characterize detectability of an attack using the system output. Fawzi et al. [8] give the threshold value of the number of channels that when attacked can be successfully corrected. Zhang et al. [9] provide a stability condition for a system under Bernoulli DoS attack. Li et al. [10] formulate a game-theoretical framework and provide optimal strategies for the attacker and the plant using Markov chain theory for the case when the channel between sensor and estimator is jammed. Mo and Sinopoli [11] analyze the effect of replay attacks and the trade off between linear quadratic Gaussian (LQG) performance and the accuracy of a $\lambda_2$ failure detector.

How to guarantee system performance even in the presence of an attack still remains an open challenge. Specifically, most of the existing work focuses on detecting an ongoing attack with the assumption that, once detected, the attacker will be removed from the system. However, often, the plant must be run even in the presence of an attack by altering the controller suitably if needed. This would require a joint design of an attack detector and a controller that switches to maintain suitable performance both in the absence and presence of an attack. Such an architecture has not yet received sufficient attention in the literature. While some recent work [12] [13] [14] has considered this architecture in the context of fault detection, such works typically do not consider security threats and impose restrictions on the form and evolution of the disturbance signals. Thus such architectures are more useful for situations when assumptions attached on attack signals about linearity or stochastic dynamics stand, see [7] [15] [3] [16]. A design that simultaneously guarantee system security and control performance has not been explored much.

The contributions of this paper are as follows. A unified model for cyber physical systems under attack is presented as a time-invariant system subject to unknown inputs that affect the state. The evolution of this system is described via a hybrid automaton, which describes the interaction between the continuous plant dynamics and discrete events pertaining to start and end of attacks. We do not make any stochastic assumption on the disturbance signals and design a monitor capable of detecting arbitrary data injection attacks. By distinguishing user data and unanticipated bad data, the administrator prevents attackers from performing actions to jeopardize the system performance. Further, we assume that the plant operates even after an attack has been detected and the desired performance is realized with a switch in the controller structure. The switched controller is designed using a passivation $M$-matrix approach. By properly designing a local $M$ controller implemented at the plant side, passivity of the hybrid system is guaranteed and, in addition, the system operates with desired performance even under attack. Note that the passivity based design makes it feasible to shape the energy flow inside the system. It avoids the very involved computations from applying traditional signal-processing control methods, such as Kalman filter, LQG controller or linear-optimization-based game theoretical methods.

This paper is organized as follows. A brief background on passivity theory is provided in Section II. Section III states the problem statement. Section IV presents the main results of this paper. The attack monitor is covered first, and then a passivation defense mechanism is presented followed by a case study in Section V. Section VI concludes the paper.

II. BACKGROUND

Dissipativity theory in general, and passivity in particular, provide a fundamental perspective for design and analysis of
dynamical systems based on a generalized energy concept. Of note, passivity implies stability under weak assumptions.

Consider a continuous system with dynamics given by
\[
\begin{align*}
\dot{x} &= f(x, u), \\
y &= h(x, u),
\end{align*}
\]  
where \( x \in \mathcal{X} \subseteq \mathbb{R}^n \), \( u \in \mathcal{U} \subseteq \mathbb{R}^m \), and \( y \in \mathcal{Y} \subseteq \mathbb{R}^m \) are the system state, input and output spaces respectively. \( f \) and \( h \) are smooth mappings of appropriate dimensions.

Definition 1: [17] A state-space system (1) is said to be dissipative with respect to supply rate \( \omega(u(t), y(t)) \), if there exists a nonnegative storage function \( V(x) : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0} \), satisfying \( V(0) = 0 \), such that for all \( x_0 \in \mathcal{X} \), all \( t_1 \geq t_0 \), and \( u \in \mathcal{U} \),
\[
V(x(t_1)) \leq V(x(t_0)) + \int_{t_0}^{t_1} \omega(u(t), y(t)) \, dt.
\]

where \( x(t_0) = x_0 \) and \( x(t_1) = \phi(t_1, t_0, x_0, u) \).

Definition 2: [17] [18] Suppose system (1) is dissipative. It is called:

1) passive, if (2) holds for
\[
\omega(u, y) = u^T y.
\]

2) QSR-dissipative, if (2) holds and there exist matrices \( Q=Q^T \), \( S, R=R^T \) such that
\[
\omega(u, y) = u^T Ru + 2y^T Su + y^T Qy.
\]

3) \( L_2 \) stable with finite gain \( \gamma > 0 \), if system is dissipative with supply rate given by (4) where \( R=\gamma^2 I \), \( S=0 \), \( Q=-I \) such that with a \( \alpha \leq 0 \),
\[
y^T y \geq -\beta + \gamma^2 u^T u.
\]

III. Problem Statement

In this paper, we consider the detection of a data injection attack and operation of the plant even after an attack has been detected by switching the controller. Through an appropriate passivation approach, local passivity and exponential stability are guaranteed even under attack. Because passivity is compositional, this provides a preliminary setup for possible passivity-based control of large scale interconnected networks. The overall system framework is shown in Figure 1.

Fig. 1: System Framework Considered in the Paper

We consider a linear model (6) for the plant and we assume that the attacker knows the parameters \( \{A, B, C, D\} \) for the system under attack, see (6). The intelligent attacker intends to corrupt the system state and the measurements based on this knowledge. To this end, he injects data through the external control inputs. Conversely, the controller seeks to monitor the measured output to identify if an attacker is present. If an attack is detected, the controller switches to another configuration to maintain performance in spite of the attack.

One possible strategy for designing the controller that guarantees a desired level of performance in spite of the presence of an attack is to design using a non-switching \( H^\infty \) controller. However, this procedure may lead to a design that is too conservative when an attack is only rarely present. Instead, we design a controller using a passivity framework that ensures that the passivity levels of the closed loop system are guaranteed even when an attack is present. For this, we use the input-output transformation matrix \( M \) as introduced in [19] that does not require knowledge of the passivity levels of either the plant or the controller.

IV. Main Results

A. System Model

Consider a system with dynamics given as follows.
\[
\begin{align*}
\dot{x}(t) &= Ax(t) + Bu(t) + w(t), \\
y(t) &= Cx(t) + Du(t),
\end{align*}
\]

where \( x(t) \in \mathbb{R}^n \), \( u(t) \in \mathbb{R}^m \), \( y(t) \in \mathbb{R}^p \) are state, system input and output respectively. \( w \) is the unknown external control input that the attacker may possibly inject into the system. This term is set to 0 when the system is in normal operation. We refer to the signal \( w(t) \) as the attack signal. We assume that the system input signal is smooth. With a switching controller, the evolution of the system is described in Figure 2.

Fig. 2: A Hybrid Automaton Framework. Event Attack is triggered if the attacker injects attack signal into the system. Event Detect is triggered if the attack monitor successfully detects the existence of attack signal. Event Defense is triggered if the system becomes passive by switching the controller.

B. Attack Monitor

Lemma 1: (Following [7]) An attack is undetectable by any attack monitor if there exist initial conditions \( x_1, x_2 \) and an attack signal \( w \) such that, for all \( t \geq 0 \), the input
injected by this attack generates zero-dynamics on the plant as
\[ y(x_1, w, t) = y(x_2, 0, t). \]  
(7)

Remark 1: In view of the fundamental limitation of an attack monitor as illustrated in [7], we limit our consideration to detectable attacks. We use a modified Luenberger observer for attack monitoring.

Assume that the unknown external control input that the attacker injects into the system is expressed as
\[ w(t) = \hat{w}(t) + \Delta w, \]  
(8)
where \( \hat{w}(t) \) is the estimate of \( w(t) \) and \( \Delta w \) is the corresponding estimation error. Let \( L \) denote the observer gain matrix. The classic Luenberger type disturbance observer can be written as
\[ \dot{\hat{w}}(t) = -L\hat{w}(t) + L(\dot{x} - Ax - Bu), \]  
(9)
from which we can get the equalities
\[ \dot{\hat{w}}(t) = L\Delta w, \]  
(10)
and
\[ \Delta \dot{w} = \dot{\hat{w}}(t) - L\Delta w. \]  
(11)

Since a nonlinear dependency on \( x \) is not realizable in practice, see [20], we need to modify the design for the monitor as follows.

**Theorem 1:** Consider system (6) and assume that the attacks are detectable. The attack detection filter can be obtained as
\[ \dot{\epsilon} = -l(x)\epsilon + l(x)(-Ax - Bu - \rho(x)), \]  
\[ \dot{\hat{w}} = \epsilon + \rho(x), \]  
(12)
\[ \frac{d}{dt} \rho(x) = l(x)\dot{x}, \]
where \( \epsilon \) is the internal state variable of the monitor, \( \rho(x) \) is a nonlinear function to be designed and \( l(x) \) is the gain of the modified detection filter that can possibly depend on \( x \). The output of the detection filter is the residual signal
\[ \nu(t) = \dot{\hat{w}}(t). \]  
(13)

**Proof:** We let the internal state variable
\[ \epsilon = \dot{\hat{w}} - \rho(x), \]  
(14)
where \( \rho(x) \) can be determined by the modified detection filter gain \( l(x) \) as
\[ \frac{d}{dt} \rho(x) = l(x)\dot{x}. \]
Then according to (6), (8), (10) and (14), we have
\[ \dot{\epsilon} = \dot{\hat{w}} - \rho(x) \]
\[ = l(x)\Delta w - l(x)\dot{x} \]
\[ = -l(x)(\epsilon + \rho(x)) + l(x)(Ax + Bu + \rho(x)) - l(x)\dot{x} \]
\[ = -l(x)\epsilon + l(x)(-Ax - Bu - \rho(x)). \]
Thus, the modified attack detection filter (12) can be achieved.

The error dynamics is given by
\[ \Delta \dot{w} = \dot{\hat{w}}(t) - \hat{w}(t) - \dot{\hat{w}} - \frac{dp(x)}{dt} \]
\[ = l(x)[\hat{w} - \rho(x)] + l(x)[Ax + Bu + \rho(x)] + \hat{w} - l(x)\dot{x} \]
\[ = \dot{w}(t) - l(x)[w(t) - \hat{w}(t)]. \]
Thus, we obtain that
\[ \Delta \dot{w} = \hat{w}(t) - l(x)\Delta w. \]  
(15)

Remark 2: Note that the modified attack monitor does not need the derivative term \( \dot{x} \), yet it has similar error dynamics as the basic disturbance observer error dynamics. This attack monitor can not only detect the existence of an attack, but also track its trajectory. We can also use the detected signal as an estimated value of the unexpected input.

The following theorem gives us the criteria to design the filter gain \( l(x) \).

**Theorem 2:** If there exists an invertible matrix \( X \) and a positive definite matrix \( \Gamma \) such that with the gain \( l(x) \),
\[ l(x)^T X^T X + X^T X l(x) \geq \Gamma, \]  
(16)
and further the derivative of \( w(t) \) is negligible compared with \( \Delta w \) as in estimation error dynamics (8), i.e. \( \dot{\hat{w}}(t) \approx 0 \), then the designed disturbance observer is exponential stable.

**Proof:** Consider the candidate Lyapunov function as
\[ W(\Delta w, x) = (X\Delta w)^T (X\Delta w) = \Delta w^T X^T X \Delta w. \]  
(17)
We can see that the scalar function \( W \) is positive definite. With the equations (15) (16) and (17), when \( \dot{\hat{w}}(t) \approx 0 \), we get
\[ \dot{W}(\Delta w, x) = \Delta \dot{w}^T X^T X \Delta w + \Delta w^T X^T X \Delta \dot{w} \]
\[ = (\dot{w} - l(x)\Delta w)^T X^T X \Delta w + \Delta w^T X^T X \dot{\hat{w}} - l(x)\Delta w \]
\[ = -\Delta \dot{w}^T \left[ (l(x)^T X^T X + X^T X l(x)) \right] \Delta w. \]
Since the condition in Theorem 2 is satisfied, \( \dot{W}(\Delta w, x) \) is negative definite for all \( \Delta w \) and \( \lim_{t \to -\infty} \Delta w(t) = 0 \) for all \( \forall \Delta w \in \mathbb{R}^n \). Moreover, from (15), the disturbance tracking error will converge exponentially to zero for all \( \forall \Delta w \in \mathbb{R}^n \). It implies \( \dot{\hat{w}} \) will exponentially approach to \( w \) if the detection gain \( l(x) \) is chosen with (16) regardless of \( x \).

### C. Switching the Controller

Once an attack is detected, the controller switches to a new structure that ensures that the system continues to be stable and perform well. For this purpose, we use the framework of transformation \( M \)-matrix that is pictorially depicted in Figure 3. The parameters \( m_{11}, m_{12}, m_{21}, \) and \( m_{22} \) are chosen such that closed loop system guarantees desired passivity level even when no priori knowledge of passivity indices of the system and controller is available.

We proceed as follows. Consider the unforced system [21]
\[ \dot{x}(t) = \sum_{i=1}^2 \sigma_i A_i x(t) + \sum_{i=1}^2 \sigma_i w(t), \]
\[ y(t) = \sum_{i=1}^2 \sigma_i C_i x(t), \]  
(18)
where $\sigma_i(t) = \begin{cases} 1, \text{when } \Sigma_i \text{ is active} \\ 0, \text{otherwise} \end{cases}$. We define the indicator function $\sigma(t) = [\sigma_1(t) \quad \sigma_2(t)]^T$ with $\sigma_1(t) + \sigma_2(t) = 1$.

The optimal control goal is to guarantee the passivity of the closed-loop switching system. If the passivation transformation $M$ is chosen appropriately such that the hybrid automaton is passive, we can say that event, defense, is triggered.

A quadratic cost function is defined as

$$L_r(u, w) = \int |y(t)|^2 dt - \gamma^2 \int |w(t)|^2 dt. \tag{19}$$

An optimal control policy [22] guarantees the desired system performance

$$\frac{\|y\|}{\|w\|} \leq \gamma. \tag{20}$$

where $\|w(t)\|^2 = \int |w(t)|^2 dt$, $\|y(t)\|^2 = \int |y(t)|^2 dt$. The following theorem illustrates the condition that automaton mode $\Sigma_i$ is stable when that mode is active.

Theorem 3: For fixed $\gamma \geq 0$, the system has stable performance (20) under attack, if there exist $\beta_{ij} \geq 0$ and symmetric positive definite matrix $P_i$, $i, j \in \mathcal{M} = \{1, 2\}$ such that

$$A^T P_i + P_i A + \gamma^{-1} C^T C + \Sigma_i \beta_{ij} (P_i - P_j) P_i - \gamma I < 0, \tag{21}$$

Proof: Choose a transition law between $\Sigma_1$ and $\Sigma_2$ mode as

$$\sigma(t) = \arg \min_{i \in \mathcal{M}} \theta(t) P_i \theta(t), \tag{22}$$

where $\theta(t)^T = [x(t)^T \quad w(t)^T]$. Choose a candidate Lyapunov function for the hybrid system as

$$V(t, x(t)) = x(t)^T (\Sigma_i=1 \sigma_i(t) P_i) x(t). \tag{23}$$

Based on whether the transition between modes happens or not, we consider two cases.

1) When $\sigma(t + \Delta t) = \sigma(t) = i$, i.e. there is no transition between two modes. Based on (18) (23),

$$\dot{V} = x^T (\Sigma_i=1 \sigma_i(t) P_i) x(t) + x(t)^T (\Sigma_i=1 \sigma_i(t) P_i) \dot{x}$$
$$= [\Sigma A x + \Sigma u] (\Sigma_i=1 \sigma_i(t) P_i) x + x^T (\Sigma_i=1 \sigma_i(t) P_i) [\Sigma A x + \Sigma u]$$
$$= \theta(t)^T [A^T P_i + P_i A + \gamma I \theta(t)] \dot{x}(t).$$

2) When $\sigma(t + \Delta t) = \sigma(t) = j$, $\sigma(t) = i \neq j$, i.e. the transition between modes happens, using (22),

$$\dot{V}(t, x) = \lim_{\Delta t \to 0} \frac{\sigma(t)^T P_i x(t) - \sigma(t)^T P_j x(t)}{\Delta t}$$
$$\leq \lim_{\Delta t \to 0} \frac{\sigma(t)^T P_i x(t) - \sigma(t)^T P_j x(t)}{\Delta t} \leq \gamma [A^T P_i + P_i A + \gamma I] \theta(t).$$

Define $L(y(t), w(t)) = \gamma (y(t)^T w(t) - \gamma^{-1} y(t)^T y(t))$, based on (18),

$$\dot{V}(t, x) - L(y, w) \leq \theta^T [A^T P_i + P_i A + \gamma^{-1} C^T C + \Sigma_i \beta_{ij} (P_i - P_j) P_i - \gamma I] \theta(t).$$

If (21) is satisfied, $\dot{V}(x) - L(y, w) < \theta^T (\Sigma_i \beta_{ij} (P_i - P_j)) \theta(t)$. Based on (22), we get

$$\dot{V}(t, x) < L(y, w), \text{ for } \forall t. \tag{24}$$

a) When $w = 0$, $\dot{V}(t, x) < L(y, w) = -\gamma^{-1} y(t)^T y(t)$, the system is stable.

b) Under zero initial condition, we have $\int_0^\infty \dot{V}(t, x) dt < \int_0^\infty w(t) dt$. Since $\int_0^\infty \dot{V} dt = V(\infty)$, this implies that

$$\int_0^\infty |y(t)|^2 dt < \gamma^2 \int_0^\infty |w(t)|^2 dt, \tag{25}$$

Optimal performance $\gamma$ is satisfied. Under condition (21), $\Sigma_i$ is finite gain stable. The objective is to obtain the criteria of how to choose passivation parameters in Figure 3 such that the closed-loop hybrid system is passive without any prior knowledge of the passivity levels for plant $G$ and the preset controller $H$. The following theorem discusses how to select $M$-matrix in order to render active automaton mode $\Sigma_i$ be passive.

Theorem 4: Consider system $\Sigma_i$ with (21) satisfied. Assume the pre-designed controller $H$ is passive. If we select passivation transformation $M$-matrix with

$$\begin{align*}
m_{11} m_{12} &+ m_{12} m_{22} \geq 0, \tag{26} \\
m_{12} m_{22} &+ m_{11} m_{22} = 0,
\end{align*}$$

then the interconnected feedback system $\Sigma_i$ under attack is passive.

Proof: Now $u_0 = w - y_2$, $u_1 = \frac{1}{m_{11}} u_0 - \frac{m_{12}}{m_{11}} y_1$, $y_0 = u_2 = m_{21} u_1 + m_{22} y_1$. We have

$$w = u_0 + y_2 = m_{11} u_1 + m_{12} y_1 + y_2. \tag{27}$$

Since system $G$ is finite gain stable under (21), let its finite gain be $\gamma_1 > 0$. We have supply rate

$$\omega(u_1, y_1) = \gamma_1^2 u_1^T u_1 - y_1^T y_1 \geq 0. \tag{28}$$

When interconnected system is passive, we have

$$\omega(w, y_0) = w^T y_0$$
$$= m_{11} m_{21} u_1^T u_1 + m_{12} m_{22} y_1^T y_1 + (m_{12} m_{21} + m_{11} m_{22}) x^T y_1 + m_{21} y_1^T u_1 + m_{22} y_1^T y_1$$
$$= \left[ u_1^T y_1 \right]^T \left[ m_{11} m_{21} \quad m_{11} m_{22} \quad m_{12} m_{21} \quad m_{12} m_{22} \right] \left[ u_1 \right] + y_1^T u_2 \geq 0.$$
The interconnected system is passive, if (26) is satisfied with assumption that the pre-designed controller $H$ is passive.

**Theorem 5:** Consider the automaton framework in Figure 2. If we select passivation transformation $M$-matrix with criteria (26), passivity of the overall hybrid automaton is guaranteed under condition (21).

**Proof:** If we select transformation $M$-matrix with (26), each active mode $\Sigma_i$ is passive under condition (21). Similarly, consider inactive mode $\Sigma_j$, $j \neq i$, we have $u_0 = m_{11}u_1 + m_{12}y_1$, $y_0 = m_{21}u_1 + m_{22}y_1$, and $w = u_0 + y_2$.

Arbitrary choose $M$-matrix with $m_{11} \neq 0$, there exists supply rate

$$\omega(w, y_0) = y_0^T y_0 = u_2^T u_2 \geq 0. \quad (29)$$

Each mode $\Sigma_i$ is dissipative when it is inactive. Moreover, since the accumulated energy flows from active subsystem $i$ to inactive subsystem $j$ at each switching instant $t_{ik}$, $\forall i, k$ is finite without external supply, i.e.

$$V_0(x(t_0)) + \sum_{i=1}^{\infty} [V_{ik}(x(t_{ik})) - V_{ik-1}(x(t_{ik}))] \leq \infty. \quad (30)$$

according to Definition 3.3 in [23], the hybrid automaton is passive.

**V. SIMULATION RESULTS**

**Example 1:** Consider a cyber-physical vehicle as in Figure 4.

Let the dynamics of the vehicle dynamic system be [24].

$$\begin{bmatrix}
\dot{\phi}_1 \\
\dot{\phi}_2 \\
\dot{\delta}
\end{bmatrix} =
\begin{bmatrix}
-2.11 & -6.61 & 9.48 & -357.05 \\
73.54 & -61.70 & 11.71 & -757.81 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{bmatrix}
\begin{bmatrix}
\phi_1 \\
\phi_2 \\
\delta
\end{bmatrix}
+ \begin{bmatrix}
T_{\phi} & T_{\phi} & 0 & 0
\end{bmatrix} u + \begin{bmatrix}
0 & 8 & 0 & 0
\end{bmatrix}^T w.
$$

$$g(t) = \begin{bmatrix}
0 \\
20 \\
8 \\
0
\end{bmatrix}^T \begin{bmatrix}
\phi_1 \\
\phi_2 \\
\phi \\
\delta
\end{bmatrix}^T,$$

Lean rotation $\phi$ is the angular rotation about $x$-axis. Steering angle $\delta$ is the rotation of front tires with respect to rear tires about the steering axis, $T_\phi$ represents right lean torque and $T_\delta$ is an action-reaction steering torque. Here we set $T_\phi=1.2$ and $T_\delta=10$. $w$ is the unknown external input that injected by attacker. Assume the forward speed $V = 20ms^{-1}$.

In this example, first we choose the detector gain independently of $x$ based on Theorem 1 as $l(x) = X^{-1} = 2$. The attack detector can be designed as

$$\dot{\epsilon} = -2\epsilon + \begin{bmatrix}
0.22 & 13.22 & -18.96 & 714.1 \\
-147.67 & 119.39 & -23.42 & 1515.62 \\
-4 & -2 & -4 & 0 \\
0 & 0 & 0 & -4
\end{bmatrix} \begin{bmatrix}
\phi \\
\delta \\
\phi \\
\delta
\end{bmatrix} - \begin{bmatrix}
-2.4 & 0 \\
0 & -20
\end{bmatrix} u,$$

$$\dot{\epsilon} = \epsilon + \rho(x),
$$

$$\frac{d}{dt} \rho(x) = l(x) \dot{x} = 2\dot{x}. \quad (32)$$

We implement the designed attack monitor. The attacker generates an aperiodic rectangular signal with sample time 5 seconds. The simulation result for the designed attack monitor is shown in Figure 5.

The first part in Figure 5 represents the dynamic response of the system under irregular pulse injected by the attacker. The blue dash line depicts the dynamic of angular lean velocity $\phi$ and the red solid line represents the response of angular steering velocity $\delta$ for the initial condition $(\dot{\phi}, \dot{\delta}) = (8rad/s, 10rad/s)$.

In the second part of Figure 5, the blue dash line represents the real signal the attacker injected to the system and the red solid line represents the output of the attack monitor. We can see that the monitor designed tracks the unknown input well.
The first part of Figure 6 depicts the dynamic response of \( \dot{\phi} \) after correction with blue dash line and the response of \( \dot{\phi} \) after defense mechanism being triggered with red solid line. As we can see, the velocities become smoother after correction. At the mean time, the angular lean velocity becomes more gentle such that the driving process is robust in spite of the irregular force applied to the vehicle. The discomfort of driver and passengers in vehicle after being attacked has been reduced. The second part of Figure 6 depicts the supply rate of the system after correction. Define supply rate as the inner product of injected input and output of the system. Output supply rate of the system shown here is always positive after the settling time. This demonstrates that the system under attack is passive with designed passivation \( M \)-matrix.

VI. CONCLUSION

In this paper, we adopt a hybrid automaton approach to describe the dynamic transitions between the nominal CPS and the system under attack. The unified modeling framework of CPS under attack is described as a time-invariant system subject to unknown input. The monitor designed in this paper is capable of detecting exogenous attacks and triggering the discrete event, Attack, in the hybrid automaton. The defense mechanism is achieved via a passivation transformation \( M \)-matrix design. Passivity is guaranteed for the hybrid automaton under attack.

REFERENCES


Figure 6: Dynamic Response and Supply Rate after Correction