Design and Operation of Secure Cyber-Physical Systems

Fabio Pasqualetti and Qi Zhu

***Abstract*—This paper proposes a holistic framework to design and operate secure, real-time, and computationally efficient cyber-physical systems. The proposed framework combines control-theoretic methods, information security notions and computational models to characterize tradeoffs among different design and operation objectives. The intricate relation among control performance, system security and platform schedulability is captured through a minimal set of interface variables, and it is argued that security mechanisms and control algorithms need to be co-designed and co-managed with the embedded platform, so as to avoid the design of algorithms that are too expensive to implement on the embedded platform, or significantly impede design objectives such as performance and timing robustness.**

I. Introduction

Cyber-physical systems are the core of most modern technological domains, including health care and biomedicine, telecommunications, and energy management. Real-time cyber-physical systems embody complex control functions that run concurrently on a single platform and share computation and communication resources; see Fig. 1. The implementation platform needs to guarantee the execution of multi-rate control laws – requiring communications with sensors and actuators – at the highest possible rate, so as to optimize the performance of each control function.

Due to standardization and the need to reduce costs, some of the core hardware and protocols adopted in cyber-physical systems are of public domain, thus vulnerable to cyber and physical attacks. Attacks can have major consequences, ranging from significant social and economic losses to instabilities and service disruption [1], [2], [3], [4], [5], [6]. Ensuring security is increasingly challenging in cyber-physical systems, where information security methods such as key management, secure communication, and code execution may guarantee the integrity of the cyber components and data, but are ineffective against insider and physical attacks. Furthermore, in real-time cyber-physical systems the platform can reserve only limited computation resources for security purposes, as the control performance significantly depends on the control sampling period, and the sampling period depends on the available computation and communication resources. Given their tight dependency, control algorithms, security methods, and implementation platforms need to be co-designed for optimal performance in resource-constrained cyber-physical systems. Surprisingly, to the best of our knowledge no framework exists to exploit tradeoffs among platform implementability, system security, and control performance, and to adapt the system parameters to favor implementability, security or performance.

Fabio Pasqualetti is with the Mechanical Engineering Department, University of California at Riverside, fabiopas@engr.ucr.edu .

Qi Zhu is with the Electrical Engineering Department, University of California at Riverside, qzhu@ee.ucr.edu .

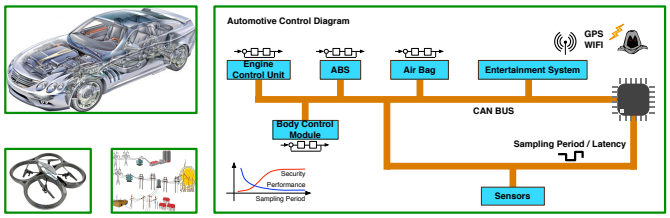


Fig. 1. In modern real-time cyber-physical systems control performance and cyber-physical security are significantly affected by the implementation platform's sampling period and end-to-end (sensors-to-controller-to-actuators) latency. A larger sampling period and end-to-end latency limit the control performance, but allow for an easier system schedulability and more computationally intensive security mechanisms. In this paper we characterize tradeoffs among control performance, system security and platform schedulability in constrained cyber-physical systems, such as automotive, aerospace, and resource-constrained industrial automation systems.

Related work In the last years several control-theoretic methods have been proposed to ensure security and robustness against failures and intentional attacks in cyber-physical systems; see for instance [7], [8], [9], [10]. To the best of our knowledge, all these methods have been developed for unconstrained systems, and often exhibit either high computational cost, or no performance guarantees. Instead, in this paper we design security mechanisms while accounting for the platform limitations. From the perspective of embedded platform design, several approaches have been proposed in the literature to account for control performance and stability [11], [12], [13], [14], [15], [16]. These works address co-design of control algorithm and embedded platform, yet they do not address and ensure cyber-physical security, which is instead the main objective of this paper.

Contributions The main contributions of this paper are twofold. First, we propose a holistic framework based on control theory, information security, and infrastructure management to design and operate secure, real-time, and computationally efficient cyber-physical systems. Our framework relies on simple, yet informative, mathematical models for different system objectives, including control performance, system security, and platform schedulability. Second, we characterize the interdependency among control performance, system security, and platform schedulability by means of a minimal set of interface variables. Our study suggests that the implementation platform should be co-designed with control and security algorithms to optimize performance and robustness, as design and operation objectives typically compete in a resource-constrained environment. Finally, we illustrate the application of the proposed approach to a model of an F-8 aircraft.

II. Control Performance, System Security, and Platform Schedulability

We consider a cyber-physical system consisting of a set of physical plants, a digital controller, and a set of actuators and sensors, where control packets and measurements are transmitted over communication channels subject to external attacks; see Fig. 1. Our objective is to characterize tradeoffs between platform implementability, system security and control performance. We start by describing our models.

A. Model of control performance

We let the physical plant be described by the linear continuous-time dynamics

$$\begin{aligned} \dot{x} &= Ax + Bu, \\ y &= Cx, \end{aligned} \tag{1}$$

where $x : \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ is the system state, $u : \mathbb{R}_{\geq 0} \to \mathbb{R}^m$ is the control input, and $y : \mathbb{R}_{\geq 0} \to \mathbb{R}^p$ is the measured output. The plant is controlled by a digital controller, with sample times t_k satisfying $t_0 = 0$, $\lim_{k\to\infty} t_k = \infty$, and $t_{k+1} - t_k = T$ for all $k \in \mathbb{N}_{\geq 0}$. Let $x_k = x(t_k)$, $u_k = u(t_k)$, and $y_k = y(t_k)$, and let the control input be piecewise constant and defined by

$$u(t) = u_k = \mathcal{K}(y_k), \quad t_k \leq t \leq t_{k+1}, \tag{2}$$

where $\mathcal{K} : \mathbb{R}^p \to \mathbb{R}^m$ is an output-based control law.

The performance of the control system depends on several factors, including the sampling time T. Following [17], [18], in this work we assume that the control performance depends exponentially on the sampling time and, specifically,

$$J(T) := \alpha^{-\beta T}, \tag{3}$$

where $J : \mathbb{R} \to \mathbb{R}$ is the map describing the performance of the control system, and $\alpha \in \mathbb{R}_{>1}$, $\beta \in \mathbb{R}_{>0}$ are appropriate constants. In Example 1 we validate the exponential model performance loss (3) for single-input single-output systems with quadratic performance function. A numerical example is in Section III.

Example 1: ***(Sampling period and control performance)*** In this example we derive the relation between the control performance and the sampling time for a single-input single-output system. Let the system dynamics be described by

$$\dot{x} = ax + u, \quad y = x, \quad u = \ell x,$$

where $a > 0$ and $\ell \in \mathbb{R}$ is a static feedback controller. The plant dynamics at the sampling times can be written as

$$x_{k+1} = (a_{\mathrm{d}} + b_{\mathrm{d}}\ell)x_k, \tag{4}$$

where

$$a_{\mathrm{d}} = e^{aT}, \quad b_{\mathrm{d}} = \frac{1}{a}\left(e^{aT} - 1\right). \tag{5}$$

Assume that the system performance is measured according to the quadratic function

$$J = \int_0^\infty x^2 + u^2 \, d\tau.$$

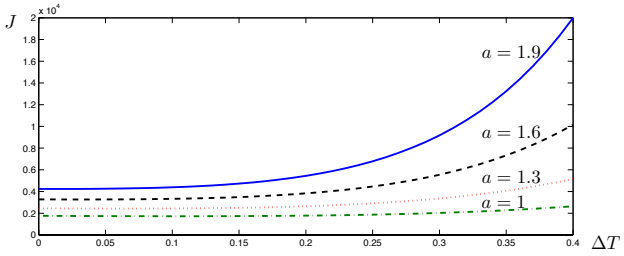


Fig. 2. In this figure we report the performance loss as a function of the sampling period, as described in Example 1. The performance degrades at least exponentially as a function of the variation of the sampling period from its nominal value (ΔT). The system parameter a affect the rate of degradation.

By using equations (4) and (5) the function J becomes

$$\begin{aligned} &\sum_{k=0}^{\infty} x_k \begin{bmatrix} 1 & \ell \end{bmatrix} \begin{bmatrix} e^{2aT} & \frac{e^{aT}}{a}\left(e^{aT}-1\right) \\ \frac{e^{aT}}{a}\left(e^{aT}-1\right) & \frac{1}{a^2}\left(e^{aT}-1\right)^2 + 1 \end{bmatrix} \begin{bmatrix} 1 \\ \ell \end{bmatrix} x_k \\ &= \sum_{j=0}^{\infty} x_j^2 \left(\frac{\ell^2 a^2 + \ell^2 e^{2aT}(e^{aT}-1)^2}{a^2} + \frac{2\ell e^{aT}(e^{aT}-1)}{a} + e^{2aT} \right), \end{aligned}$$

where

$$x_j = \left(e^{aT} + \frac{k}{a}\left(e^{aT} - 1\right)\right)^j x_0.$$

Notice that, when T increases and the feedback gain is constant, the performance degrades at least exponentially. See Fig. 2 for an illustration of this behavior. □

B. Model of security level

Attackers compromise the behavior of control systems with specific objectives. In order to drive a system to a desired state, attackers need to identify the system dynamics, reconstruct the system state, and maliciously modify the control input. The difficulty for an attacker to accomplish these actions determines the security level of a control system.

In this work we identify the security level of a control system with the extent an attacker can estimate the system state from encrypted measurements. We assume that measurements are independently transmitted by the sensors to the controller, and we allow a subset of sensors to encrypt their measurements. We parametrize the encryption method with a scalar value $n_{\mathrm{b}} \in \mathbb{R}_{\geq 0}$, and we let the *probability* for an attacker to decode an encryption key be described by the map $\mathcal{D} : \mathbb{R}_{\geq 0} \to [0, 1]$, with[1]

$$\mathcal{D}(n_{\mathrm{b}}) := 2^{-n_{\mathrm{b}}}. \tag{6}$$

The encryption of sensor measurements (i) increases the system security level, as it is more difficult for the attacker to retrieve truthful information about the system, (ii) increases the system sampling period, as it increases the computational load on the controller and, consequently, (iii) decreases the performance of the control loop as described by equation (3).

We next quantify the difficulty for an attacker to estimate the system state given a set of decrypted measurements. Let $\mathcal{K} \subseteq \{1, \ldots, p\}$ be the set of measurements obtained by the

[1]Equation (6) assumes a *brute force* decryption mechanism.

attacker, and let $y_{\mathcal{K}} : \mathbb{R} \to \mathbb{R}^{|K|}$ be the map of the decrypted measurements. Define the *Observability Gramian* by [19]

$$\mathcal{O}_{\mathcal{K}} := \sum_{\tau=0}^{\infty} A^{\tau} C_{\mathcal{K}}^{\mathsf{T}} C_{\mathcal{K}} (A^{\mathsf{T}})^{\tau},$$

where $C_{\mathcal{K}}$ is the output matrix associated with the decrypted measurements, that is, $y_{\mathcal{K}} = C_{\mathcal{K}} x$. The energy associated with the system state x with decrypted measurements $\mathcal{K}$ is

$$\mathrm{E}(x) := \sum_{\tau=0}^{\infty} \|y_{\mathcal{K}}(\tau)\|_2^2 = x^{\mathsf{T}} \mathcal{O}_{\mathcal{K}} x \geq \lambda_{\min}(\mathcal{O}_{\mathcal{K}}), \qquad (7)$$

where $y_{\mathcal{K}} : \mathbb{N}_{\geq 0} \to \mathbb{R}$ contains the measurements taken by the observing nodes $\mathcal{K}$. The larger the smallest eigenvalue of the Observability Gramian, the easier for the attacker to reconstruct the system state from measurements [20]. We identify the security level of a system with the inverse of the smallest eigenvalue of the Observability Gramian for a set of decrypted measurements. It can be shown that both the cardinality as well as the specific elements of the set of decrypted measurements determine the eigenvalues of the Observability Gramian [21], and hence the security level.

The expected security level of a system can be computed by combining the probabilistic decryption mechanism (6) and the deterministic observability degree (7). In particular, let $\mathcal{Y}$ be the set of measurement channels, and let $\mathcal{Y}_{\mathrm{e}} \subseteq \mathcal{Y}$ be the subset of encrypted channels, with $|\mathcal{Y}_{\mathrm{e}}| = n_{\mathrm{e}}$. The expected information retrieved by an attacker is

$$\mathcal{I}(n_{\mathrm{e}}, n_{\mathrm{b}}) = \sum_{\tau=0}^{n_{\mathrm{e}}} \sum_{\rho=1}^{\binom{n_{\mathrm{e}}}{\tau}} \underbrace{2^{-\tau n_{\mathrm{b}}} (1 - 2^{-n_{\mathrm{b}}})^{n_{\mathrm{e}} - \tau}}_{\text{prob. to decrypt } \tau \text{ sensors}} \overbrace{\lambda_{\min}(\mathcal{O}_{\Omega_\rho(\tau)})}^{\text{obsv. degree of } \Omega_\rho(\tau)}, \qquad (8)$$

where $\Omega_\rho(\tau)$ is the ρ-th element of the ordered set

$$\Omega(\tau) := \{\lambda \cup (\mathcal{Y} \setminus \mathcal{Y}_{\mathrm{e}}) \ : \ \lambda \subseteq \mathcal{Y}_{\mathrm{e}}, \ |\lambda| = \tau\}.$$

In other words, the set $\Omega_\rho(\tau)$ contains the measurement channels available to the attacker, and it comprises a set of decrypted channels of cardinality τ and the set $\mathcal{Y} \setminus \mathcal{Y}_{\mathrm{e}}$ of channels without encryption. We define the *security level* of a system to be

$$S(n_{\mathrm{e}}, n_{\mathrm{b}}) = \mathcal{I}(n_{\mathrm{e}}, n_{\mathrm{b}})^{-1}.$$

The evaluation of the security level requires a substantial computational effort because it involves the computation of the Observability Gramian for each possible set of corrupted measurements. The computation of analytical bounds on the security level is left as the subject of future investigation.

C. Model of implementation platform

We focus on a *federated architecture*, where each control function is implemented on its own embedded platform resources. Let c_s^i and e_s^i denote the sensing time and the encryption time of the ith sensor, respectively. Let m_{sp}^i denote the communication time for transferring the data from the ith sensor to the embedded processor, let d_p^i denote the time for the embedded processor to decode the data from the ith sensor, and let c_p denote the total computation time of the processor. Finally, let m_{pa}^j denote the communication time for transferring the data from the processor to the jth actuator.[2] The end-to-end (sensor-to-processor-actuator) delay l_p of a control functional path p can then be written as

$$l_p = \max_{i \in \{1,\ldots,p\}} \{c_s^i + e_s^i + m_{sp}^i\} + c_p + \sum_{i=1}^{p} d_p^i, \qquad (9)$$

In equation (9), the sensor encryption time e_s^i, the communication time m_{sp}^i, and the processor decryption time d_p^i depend (as specified by the implementation platform) on the encryption level n_{b} described in Section II-B. Moreover, the delay l_p limit the sampling period of the control loop. From equations (3), (8) and (9) we conclude that the control performance and the security level are competing objectives, which are tighten together by the sensing, computation, and communication limitations of the implementation platform. The discussed tradeoff among system security, control performance, and platform schedulability is summarized in Fig. 3.

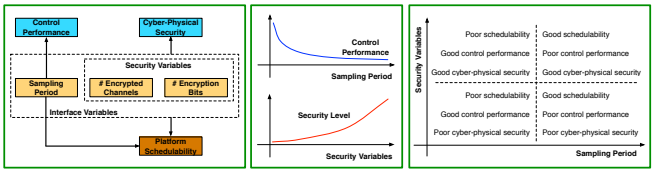


Fig. 3. This figure shows the interface variables (sampling period, number of encrypted communication channels, and number of encryption bits) and their relation to system security, control performance, and platform schedulability. The control performance is determined by the sampling period in a monotonic fashion. The level of security depends on the security variables, including the number of encrypted channels, and the number of encryption bits. Control performance and cyber-physical security are linked to the platform schedulability through the interface variables. Ensuring a desirable level of cyber-physical security is challenging in real-time and resource-constrained systems, because the control performance significantly depends on the sampling period, the sampling period limit the platform schedulability, and cyber-physical security can be enhanced only at the cost of increasing the computation and communication loads on the platform, thereby limiting platform schedulability.

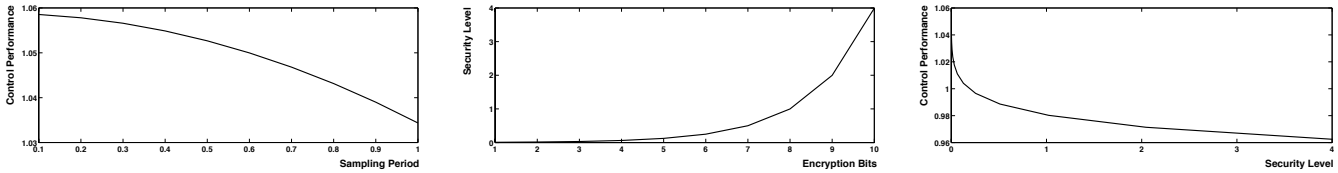
III. An Illustrative Example

Consider the following model for the linearized longitudinal dynamics of an F-8 aircraft [22]:

$$\dot{x} = Ax + Bu + L,$$
$$y = Cx,$$

where $x = \begin{bmatrix} V & \gamma & \alpha & q \end{bmatrix}^{\mathsf{T}}$, V is the velocity of the aircraft, γ is the flight-path angle, α is the angle-of-attack, q is the

[2] For the easy of notation, we assume that control packets are not encrypted. Our analysis extends in a straightforward way to the case where both control and measurement packets are encrypted.



(a) (b) (c)

Fig. 4. For the F-8 aircraft model in Section III, this figure shows the (scaled) control performance as a function of the sampling period (Fig. 4(a)), the (scaled) security level as a function of the number of encryption bits (Fig. 4(b)), and the tradeoff between the control performance and the security level (Fig. 4(c)). The assumption that sampling period is linearly proportional to the number of encryption bits. Because the control performance and the security level are competing objectives in resource constrained systems, control and security algorithms should be co-designed with the implementation platform.

pitch rate, and

$$A = \begin{bmatrix} -1.357/10^2 & -32.20 & -46.30 & 0.000 \\ 1.200/10^4 & 0.000 & 1.214 & 0.000 \\ -1.212/10^4 & 0.000 & -1.214 & 1.000 \\ 5.700/10^4 & 0.000 & -9.010 & -6.696/10 \end{bmatrix},$$

$$B = 10^{-1} \begin{bmatrix} -4.330 \\ 1.394 \\ -1.394 \\ -1.577 \end{bmatrix}, \; C^{\mathsf{T}} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, \; L = \begin{bmatrix} -46.30 \\ 1.214 \\ -1.214 \\ -9.010 \end{bmatrix}.$$

Assume that (i) $u : \mathbb{R} \to \mathbb{R}$ is an optimal linear-quadratic-Gaussian controller with unit state and input weights[19], (ii) the two measurement channels are protected by an encryption scheme with n_{b} bits, and (iii) the sampling period equals $n_{\mathrm{b}}/10$.[3] The control performance as a function of the sampling period, the system security level as a function of the number of encryption bits, and the relation between the control performance and the security level are reported in Fig. 4. Notice that the security level and the control performance are competing objective, which should be optimized at the design stage depending on the implementation platform.

IV. Conclusion

In this paper we characterize a tradeoff among control performance, system security, and schedulability in resource-constrained cyber-physical systems. Based on our analysis, control and security algorithms should be co-designed with the implementation platform to ensure performance and robustness in resource-constrained cyber-physical systems. Aspects requiring further investigation include (i) the design of online optimization algorithms to adapt the system parameters against attacks and failures, (ii) the characterization of simplified bounds for the tradeoff among design and operation objectives, and (iii) the analysis of alternative performance metrics.

References

[1] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *Critical Infrastructure Protection*, vol. 253, pp. 73–82, 2007.

[2] S. Kuvshinkova, "SQL Slammer worm lessons learned for consideration by the electricity sector," *North American Electric Reliability Council*, 2003.

[3] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[4] J. P. Conti, "The day the samba stopped," *Engineering Technology*, vol. 5, no. 4, pp. 46–47, 06 March - 26 March, 2010.

[5] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, 2011, pp. 528–533.

[6] F. Koushanfar, A.-R. Sadeghi, and H. Seudie, "Eda for secure and dependable cybercars: Challenges and opportunities," in *Design Automation Conference*, San Francisco, CA, USA, 2012, pp. 220–228.

[7] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[8] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1495–1508, 2011.

[9] R. Smith, "A decoupled feedback structure for covertly appropriating network control systems," in *IFAC World Congress*, Milan, Italy, Aug. 2011, pp. 90–95.

[10] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Stealthy deception attacks on water SCADA systems," in *Hybrid Systems: Computation and Control*, Stockholm, Sweden, Apr. 2010, pp. 161–170.

[11] H. Voit, A. Annaswamy, R. Schneider, D. Goswami, and S. Chakraborty, "Adaptive switching controllers for systems with hybrid communication protocols," in *American Control Conference*, June 2012, pp. 4921–4926.

[12] A. Anta and P. Tabuada, "To sample or not to sample: Self-triggered control for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2030–2042, Sept 2010.

[13] D. Seto, J. Lehoczky, L. Sha, and K. Shin, "On task schedulability in real-time control systems," in *Real-Time Systems Symposium, 1996., 17th IEEE*, dec 1996, pp. 13 –21.

[14] E. Bini and A. Cervin, "Delay-aware period assignment in control systems," in *Real-Time Systems Symposium, 2008*, Nov 2008, pp. 291–300.

[15] S. Samii, A. Cervin, P. Eles, and Z. Peng, "Integrated scheduling and synthesis of control applications on distributed embedded systems," in *Design, Automation Test in Europe Conference Exhibition*, April 2009, pp. 57–62.

[16] D. Goswami, M. Lukasiewycz, R. Schneider, and S. Chakraborty, "Time-triggered implementations of mixed-criticality automotive software," in *Design, Automation Test in Europe Conference Exhibition*, march 2012, pp. 1227 –1232.

[17] D. Seto, J. Lehoczky, L. Sha, and K. Shin, "On task schedulability in real-time control systems," in *Real-Time Systems Symposium*, Dec. 1996, pp. 13–21.

[18] L. Sha, X. Liu, M. Caccamo, and G. Buttazzo, "Online control optimization using load driven scheduling," in *IEEE Conf. on Decision and Control*, vol. 5, Sydney, Australia, Dec. 2000, pp. 4877 –4882 vol.5.

[19] J. P. Hespanha, *Linear Systems Theory*, 2009.

[20] D. Georges, "The use of observability and controllability Gramians or functions for optimal sensor and actuator location in finite-dimensional systems," in *IEEE Conf. on Decision and Control*, New Orleans, LA, USA, Dec. 1995, pp. 3319–3324.

[21] F. Pasqualetti, S. Zampieri, and F. Bullo, "Controllability metrics, limitations and algorithms for complex networks," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 1, pp. 40–52, 2014.

[22] D. Teneketzis and N. R. Sandell, "Linear regulator design for stochastic systems by a multiple time-scales method," *IEEE Transactions on Automatic Control*, vol. 22, no. 4, pp. 615–621, Aug 1977.

[3] More sophisticated relations between the number of encryption bits and the sampling period are unlikely to change the basic conclusions of this work.