Design and Operation of Secure Cyber-Physical Systems

Fabio Pasqualetti and Qi Zhu

***Abstract*—This letter proposes a holistic framework for the design and operation of secure and reliable resource-constrained 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. We quantify the intricate relation among control performance, system security and platform schedulability through a minimal set of interface variables. We argue that security mechanisms and control algorithms need to be codesigned and comanaged 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.**

***Index Terms*—Automotive systems, control theory, cyber-physical system, embedded systems, security.**

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 multirate control algorithms and communications with sensors and actuators at the highest possible rate, so as to optimize the performance of each control, security, and management 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]–[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 *codesigned* for optimal performance in resource-constrained cyber-physical systems. 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.

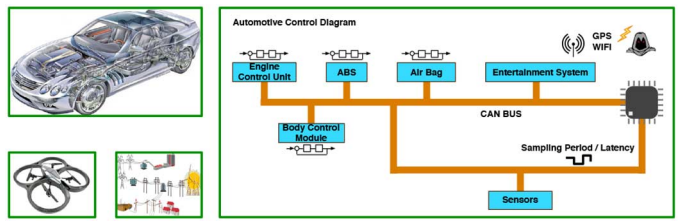


Fig. 1. In modern real-time cyber-physical systems control performance and cyber-physical security are significantly affected by the implementation platform's sampling period and end-to-end (sensors-to-controller-to-actuators) latency. A larger sampling period and end-to-end latency limit the control performance, but allow for an easier system schedulability and more computationally intensive security mechanisms. In this letter we quantify tradeoffs among control performance, system security and platform schedulability in constrained cyber-physical systems, such as automotive, aerospace, and resource-constrained industrial automation systems. Our study informs both the design and the operation of secure and reliable cyber-physical 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]–[10]. These methods have been developed for unconstrained systems, and often exhibit either high computational cost, or no performance guarantees. Instead, in this letter we design security mechanisms while accounting for resource constraints and limitations. From the perspective of embedded platform design, several approaches have been proposed in the literature to account for control performance and stability [11]–[16]. These works address codesign of control algorithm and embedded platform, yet they do not address and ensure cyber-physical security, which is instead the main objective of this letter.

Contributions This letter studies a simplified framework for the design and operation of secure cyber-physical systems based on control theory, information security, and embedded system design. The proposed holistic framework relies on informative mathematical models for various system objectives, including control performance, system security, and platform schedulability, and it quantifies their interdependency by means of a minimal set of interface variables and relations. Our study suggests that the implementation platform should be codesigned with control and security algorithms to optimize performance and robustness, as design and operation objectives typically compete

Manuscript received August 10, 2014; accepted October 22, 2014. Date of publication November 04, 2014; date of current version February 24, 2015. This work is supported by ONR grant N00014-14-1-0816. This manuscript was recommended for publication by T. Eisenbarth.

F. Pasqualetti is with the Mechanical Engineering Department, University of California at Riverside, Riverside, CA 92521 USA (e-mail: fabiopas@engr.ucr.edu).

Q. Zhu is with the Electrical and Computer Engineering Department, University of California at Riverside, Riverside, CA 92521 USA (e-mail: qzhu@ece.ucr.edu).

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

Digital Object Identifier 10.1109/LES.2014.2367100

in a resource-constrained environment. Our work supports the design and operation of cyber-physical systems, for example by providing methods to determine the necessary resources for desired security and control performance, and to design algorithms to dynamically adapt the security resources based on the difficulty of the control task. Results are numerically illustrated on a model of F-8 aircraft.

II. Control Performance, System Security, and Platform Schedulability

We consider a cyber-physical system consisting of a physical plant, 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. [1]

System model and 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 $t_{k+1} - t_k = T \in \mathbb{R}_{>0}$ 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] and [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. A numerical example validating our model of performance loss (3) is in Section III.

Model of attack Attackers compromise the behavior of a control system with specific objectives. In this work we focus on attackers that: 1) know the system dynamics, that is, the matrices A, B, and C in the model (1); and 2) aim to reconstruct the state of the system from measurements. Thus, a successful attack would result, for instance, in a loss of system privacy, and it would constitute the basis for the design of a malicious input compromising the system dynamics. We assume that measurements are independently transmitted by the sensors to the controller, and are possibly protected by some encryption method. 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 the encryption key be described by the map $\mathcal{D} : \mathbb{R}_{\geq 0} \to (0, 1]$. In this work, we assume a brute force decryption mechanism with

$$\mathcal{D}(n_{\mathrm{b}}) := 2^{-n_{\mathrm{b}}}. \tag{4}$$

The encryption of sensor measurements: 1) increases the system security level, as it is more difficult for the attacker to retrieve truthful information about the system; 2) increases the system sampling period, as it increases the computational load on the controller and, consequently; 3) decreases the performance of the control loop as described by equation (3).

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

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

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 $x \in \mathbb{R}^n$ with decrypted measurements $\mathcal{K}$ is

$$\mathrm{E}(x) := \sum_{\tau=0}^{\infty} \|y_{\mathcal{K}}(\tau)\|_2^2 = x^{\mathrm{T}} \mathcal{O}_{\mathcal{K}} x \geq \lambda_{\min}(\mathcal{O}_{\mathcal{K}}) \tag{5}$$

where $\lambda_{\min}(\mathcal{O}_{\mathcal{K}})$ denotes the smallest modulus of the eigenvalues of $\mathcal{O}_{\mathcal{K}}$. The following observations are in order. First, the larger $\lambda_{\min}(\mathcal{O}_{\mathcal{K}})$, the easier for the attacker to reconstruct the system state from measurements [20]. Hence, $\lambda_{\min}(\mathcal{O}_{\mathcal{K}})$ can be interpreted as the information of the system state contained in the measurements $y_{\mathcal{K}}$. Second, the value $\lambda_{\min}(\mathcal{O}_{\mathcal{K}})$ depends on both the cardinality and the actual decrypted channels; see Fig. 3(b). Third, the bound in (5) holds with equality for certain system states and for an infinite observation horizon [21]. Otherwise, $\lambda_{\min}(\mathcal{O}_{\mathcal{K}})$ is a lower bound on the information retrieved by the attacker from the decrypted measurements $y_{\mathcal{K}}$.

The expected information retrieved by an attacker is computed by combining the probabilistic decryption mechanism (4) and the deterministic observability degree (5). In particular, assume that the measurement channels $\mathcal{Y}_{\mathrm{e}} \subseteq \mathcal{Y}$, with $|\mathcal{Y}_{\mathrm{e}}| = n_{\mathrm{e}}$, are mutually independent and protected by the same encryption method (the measurement channels $\mathcal{Y} \backslash \mathcal{Y}_{\mathrm{e}}$ are not protected). The expected information retrieved by an attacker is defined as

$$\mathcal{I}(n_{\mathrm{e}}, n_{\mathrm{b}}) = \sum_{\tau=0}^{n_{\mathrm{e}}} \sum_{\rho=1}^{\binom{n_e}{\tau}} \underbrace{2^{-\tau n_{\mathrm{b}}} (1 - 2^{-n_{\mathrm{b}}})^{n_{\mathrm{e}} - \tau}}_{\text{prob. to decrypt } \tau \text{ channels}} \overbrace{\lambda_{\min}(\mathcal{O}_{\Omega_\tau(\rho)})}^{\text{inf. of meas.} \Omega_\tau(\rho)} \tag{6}$$

where $2^{-\tau n_{\mathrm{b}}} (1 - 2^{-n_{\mathrm{b}}})^{n_{\mathrm{e}} - \tau}$ is the attacker probability to access τ encrypted channels, $\lambda_{\min}(\mathcal{O}_{\Omega_\tau(\rho)})$ is the information obtained from the τ decrypted channels (together with the unprotected channels), Ω_τ contains all possible subsets of τ encrypted channels, $\binom{n_e}{\tau}$ is the cardinality of Ω_τ, and $\Omega_\tau(\rho)$ is the ρ-th element of Ω_τ. Specifically, Ω_τ is the ordered set

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

In other words, the expected information available to the attacker is given by the weighted sum of the information given

[1] The methodology of our framework is general, and its applicability is not restricted by the mathematical models assumed below for the purpose of analysis. More sophisticated models are needed for complex systems, but the fundamental idea of codesigning security mechanisms, control algorithms and embedded platforms remains valid across different models.

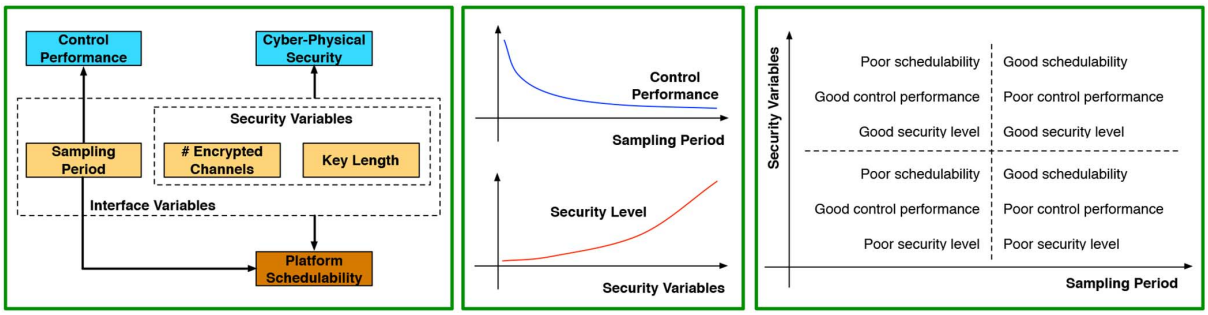


Fig. 2. A conceptual diagram illustrating the relation among certain interface variables, such as the sampling period, the number of encrypted channels and the encryption key length, and system security, control performance, and platform schedulability. The control performance depends on the sampling period in a monotonic fashion; see (3). The level of security depends on the security variables as described in (7). Control performance and cyber-physical security are linked to the platform schedulability through the interface variables; see (9). Ensuring a desirable level of 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 security can be enhanced only at the cost of increasing the computation and communication loads on the platform, thereby limiting platform schedulability.

by each set of measurement channels, where the weights are the probabilities of decrypting such channels. Notice that the set $\Omega_\tau(\rho)$ contains the measurement channels available to the attacker, and it comprises a set of decrypted channels of cardinality τ and the set $\mathcal{Y}\backslash\mathcal{Y}_\mathrm{e}$ of channels without encryption.

We define the *security level* of a system to be

$$S(n_\mathrm{e}, n_\mathrm{b}) = \mathcal{I}(n_\mathrm{e}, n_\mathrm{b})^{-1}. \tag{7}$$

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 decrypted channels. The characterization of analytical bounds on the security level, as well as the design of methods for selection of encrypted channels are left as the subject of future research.

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 to transfer 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 be written as

$$l_p = \max_{i\in\{1,\dots,p\}} \{c_s^i + e_s^i + m_{sp}^i\} + c_p + \sum_{i=1}^{p} d_p^i. \tag{8}$$

Furthermore, if the channels have homogeneous sensing, encryption and communication times, then equation (8) becomes

$$l_p = c_s + e_s + m_{sp} + c_p + n_e d_p \leq T \tag{9}$$

where the last inequality follows because the end-to-end latency is typically constrained to be within the sampling period T.[3] Equation (9) reveals a constraint between the number of encrypted channels and the sampling period. Together with equations (3) and (6), we notice that the control performance and the security level are competing objectives, which are constrained 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. 2.

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 $x = [\,V \quad \gamma \quad \alpha \quad q\,]^\top$, V is the velocity of the aircraft, γ is the flight-path angle, α is the angle-of-attack, q is the pitch rate, and

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

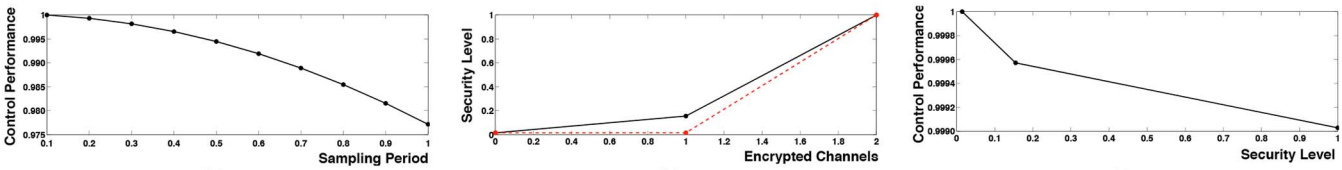
$$B = 10^{-1}\begin{bmatrix} -4.330 \\ 1.394 \\ -1.394 \\ -1.577 \end{bmatrix}, \quad C^\top = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad L = \begin{bmatrix} -46.30 \\ 1.214 \\ -1.214 \\ -9.010 \end{bmatrix}.$$

The control input $u : \mathbb{R} \to \mathbb{R}$ follows a digital LQR/LQG output controller with unit cost matrices [19]. The control performance equals the largest eigenvalue of the solution to the algebraic Riccati equation associated with the LQR problem, which corresponds to the worst case performance over all system states [19]. The control performance is computed with the Matlab [23] routine *lqrd* for different values of the sampling period.

We let the communication channels be encrypted with the AES (Advanced Encryption Standard) algorithm with a key length of 128 bits. The encryption and decryption times of AES on various embedded processors are reported in [24] and [25]. In our numerical study we let the data size be 12 000 bits, the encryption time e_s and d_p be 50 ms (assuming an encryption throughput of 300 kbits/s, a constant key setup time of 10 ms on the Texas Instruments MSP430 platform [24], and equal decryption time), the sensing time c_s be 30 ms, the communication time m_{sp} be 40 ms, and the computation time c_p be 30 ms. The normalized results of our numerical study are reported in Fig. 3. In particular, the control performance as

[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.

[3]Sample delays are introduced when the end-to-end latency is larger than the sampling period. In this case the constraint between sampling period and end-to-end latency is formulated differently, but the general trends are similar.



(a) (b) (c)

Fig. 3. For the F-8 aircraft model in Section 3, this figure shows the normalized control performance as a function of the sampling period [see Fig. 3(a)],the normalized security level as a function of the encrypted channels [see Fig. 3(b)] and the tradeoff between control performance and security [see Fig. 3(c)] Fig. 3(b) shows that the encryption of the first communication channel (solid black) yields a higher security level than the encryption of the second communication channel (dashed red). Thus, our analysis allows for an optimal selection of the communication channels to be encrypted. Finally, because control performance and security are competing objectives in resource-constrained systems, control and security algorithms should be codesigned with the implementation platform.

a function of the sampling period is reported in Fig. 3(a), the security level as a function of the number of encrypted channels in Fig. 3(b), and the tradeoff between control performance and security in Fig. 3(c). The security level and the sampling period are computed with equations (6) and (9), respectively. Our numerical results show the effectiveness of our methods to quantify the competitive relation between control performance and security in resource-constrained systems, and to enable an optimal selection of control and security parameters.

IV. Conclusion

In this letter we quantify 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 codesigned with the implementation platform to ensure performance and robustness in resource-constrained cyber-physical systems. Future research directions include: 1) the design of online optimization algorithms to adapt the system parameters against attacks and failures; 2) the characterization of simplified bounds for the tradeoff among design and operation objectives; and 3) the analysis of alternative attack models and objectives.

References

[1] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Crit. Infrastructure Protect.*, vol. 253, pp. 73–82, 2007.
[2] S. Kuvshinkova, "SQL Slammer worm lessons learned for consideration by the electricity sector," *North Amer. Electr. Rel. 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," *Eng. Technol.*, vol. 5, no. 4, pp. 46–47, Mar. 2010, 06 March - 26.
[5] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Proc. IEEE Intell. Veh. Symp. (IV),*, 2011, pp. 528–533.
[6] F. Koushanfar, A.-R. Sadeghi, and H. Seudie, "Eda for secure and dependable cybercars: Challenges and opportunities," in *Proc. Conf. Design Autom.*, 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 Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[8] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.
[9] R. Smith, "A decoupled feedback structure for covertly appropriating network control systems," in *Proc. 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 *Proc. 13th ACM Int. Conf. Hybrid Syst.: Comput.Contr.*, 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 *Proc. Conf. Amer. Contr.*, Jun. 2012, pp. 4921–4926.
[12] A. Anta and P. Tabuada, "To sample or not to sample: Self-triggered control for nonlinear systems," *IEEE Trans. Autom. Control*, vol. 55, no. 9, pp. 2030–2042, Sep. 2010.
[13] D. Seto, J. Lehoczky, L. Sha, and K. Shin, "On task schedulability in real-time control systems," in *Proc. 17th IEEE Real-Time Syst. Symp.*, Dec. 1996, pp. 13–21.
[14] E. Bini and A. Cervin, "Delay-aware period assignment in control systems," in *Proc. IEEE Real-Time Syst. Symp.*, 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 *Proc. Design, Autom., Test Eur. Conf. Exhib.*, Apr. 2009, pp. 57–62.
[16] D. Goswami, M. Lukasiewycz, R. Schneider, and S. Chakraborty, "Time-triggered implementations of mixed-criticality automotive software," in *Proc. Design, Autom., Test Eur. Conf. Exhib*, Mar. 2012, pp. 1227–1232.
[17] D. Seto, J. Lehoczky, L. Sha, and K. Shin, "On task schedulability in real-time control systems," in *Proc. IEEE Real-Time Syst. Symp.*, Dec. 1996, pp. 13–21.
[18] L. Sha, X. Liu, M. Caccamo, and G. Buttazzo, "Online control optimization using load driven scheduling," in *Proc. IEEE Conf. Decision Contr.*, Sydney, Australia, Dec. 2000, vol. 5, pp. 4877–4882.
[19] J. P. Hespanha, *Linear Systems Theory*. Princeton, NJ, USA: Princeton Univ. Press, 2009.
[20] D. Georges, "The use of observability and controllability gramians or functions for optimal sensor and actuator location in finite-dimensional systems," in *Proc. IEEE Conf. Decision Contr.*, 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 Trans. Control Netw. Syst.*, vol. 1, no. 1, pp. 40–52, Mar. 2014.
[22] D. Teneketzis and N. R. Sandell, "Linear regulator design for stochastic systems by a multiple time-scales method," *IEEE Trans. Autom. Control*, vol. AC-22, no. 4, pp. 615–621, Aug. 1977.
[23] MATLAB, "The MathWorks Inc.," Natick, MA, USA, Version 8.1. 0.604 (R2013a), 2013.
[24] O. Hyncica, P. Kucera, P. Honzik, and P. Fiedler, "Performance evaluation of symmetric cryptography in embedded systems," in *IEEE 6th Int. Conf. Intell. Data Acquisition Adv. Comput. Syst. (IDAACS)*, Sep. 2011, vol. 1, pp. 277–282.
[25] H. Lee, K. Lee, and Y. Shin, "Aes implementation and performance evaluation on 8-bit microcontrollers," *CoRR*, vol. abs/0911.0482, 2009.