Privacy and Performance Trade-off in Cyber-Physical Systems

Heng Zhang, Yuanchao Shu, Peng Cheng, Jiming Chen
Department of Control, Zhejiang University, China
Email: ezhangheng@gmail.com, ycshu@zju.edu.cn, pcheng@iipc.zju.edu.cn, jmchen@iipc.zju.edu.cn

***Abstract*—Increasing number of instances of privacy leakage in Cyber-Physical Systems (CPS) and the corresponding serious consequences have arisen great worries in our society. In most privacy preserving mechanisms proposed to protect the sensitive individual information, system performances are compromised at the same time. In this article, we consider the trade-off between individual privacy and system performance in CPS. After introducing the CPS architecture and the basic definition of differential privacy, we formulate the performance optimization problem subject to a given differential privacy requirement. For a simplified system, we derive the close-form optimal system performance under desired privacy requirement. Simulation results are provided to verify the proposed mechanism, which balances tradeoff between system performance and privacy. We also identify the future research topics on privacy preserving problem in CPS.**

I. Introduction

Cyber-physical systems (CPS), as the next generation of engineered systems, deeply integrate modern computing, communication, and control technologies to dramatically improve the efficiency, stability, reliability, safety and other performances in operating real systems [1], [2]. CPS has attracted much attentions by academic researchers, industrial and technical staff, government decision-makers due to growing number of applications in national economy and critical infrastructure, such as industrial control, smart grid, and intelligent transportation. In particular, national defense has been highly dependent on the development of CPS, since the defense systems, including unmanned aerial vehicles, Naval Vessels, and unmanned ground vehicles, all belong to cyber-physical systems in essence [3].

Though CPS can clearly yield enormous benefits for us, it is also vulnerable to an increasing number of malicious attacks due to the employment of communication networks and heterogeneous IT elements. Thus, security and privacy are becoming critical issues in the field of CPS theoretical research and technical implementation, and many literatures have studied these issues from different points of view [1], [2]. An important issue of security in CPS is confidentiality, which refers to the ability of protecting the database from unauthorized users. However, different from confidentiality related to data, privacy is about people and refers to the personal sensitive information [1]. An example is that attackers can use None-Intrusive Load Monitoring (NILM) techniques from smart meters to obtain the resident's private information, such as living habit, and then break into people's home when the house is vacant [4].

Encryption, a traditional privacy protection technique, is widely used to prevent the data from unauthorized users and adversaries [5]. However in CPS, this technique can be hardly applied due to the limitation of sensors' computing capacity. In addition, brute-force attack can be used by the adversary against any encrypted data [6]. Therefore, a critical issue is how to preserve the privacy when the adversaries can access to the data and the encryption techniques are invalid. Differential privacy is recently proposed by Dwork as an effective privacy protection approach which prevent data recovery by adversaries [7]. Essentially, it is a perturbation technique that conceals the original data with proper noises. Due to its significant advantages including easy realization and mathematical theoretical basis, differential privacy has been widely applied to preserve individual privacy in CPS. Furthermore, individual can sell his private information to corporations and get rewards when the privacy level of his information is measured by differential privacy [8].

However, most existing privacy preserving works put emphasis on the design of privacy preserving approaches, which on the other hand, neglect the optimization of system performance at the same time. In fact, CPS is a feedback close-loop system with dynamic evolution of states. Thus, the optimization of system control performances should be considered. For example, Linear Quadratic Gaussian controller (LQG) is used to keep the level of energy storage and reduces the the power flow in microgrid network system [9], and H_∞ controller is synthesized to achieve stabilization with guaranteed performance in F18/HARV fighter aircraft system [10]. Therefore, a new challenging issue is how to balance the privacy requirements and system performance in CPS. Specifically, in this article we optimize the system performance with a given privacy-preserving requirement.We describe the privacy-preserving requirement by the parameters ϵ and δ in differential privacy, and then formulate an optimal controller design problem with guaranteed privacy-preserving requirement. In a special case study, we obtain the optimal controller which minimizes the LQG cost function.

The contribution of this article is threefold. First, to our best knowledge, this is the first work to propose an optimization problem which jointly considers the controller design and privacy preserving in CPS. Second, we derive the explicit expression of optimal LQG controller for the system under guaranteed privacy requirement. Third, we bring both theoretical analysis and simulations to demonstrate how to balance the tradeoff between control performance and privacy.

II. Differential private controller design

A. System architecture

Cárdenas et al. [1] pointed out that a typical CPS (see Fig. 1) is composed of

- plants, the physical systems;
- sensors, to observe the plants and get the information;
- controllers, to make decisions and issue control commands;
- actuators, to implement the control commands;
- networks, the communication medium through which the plants, sensors, controllers and actuators exchange information with each other.

These entities are tightly working together to improve the system performance with advanced computing, communication and control technologies.

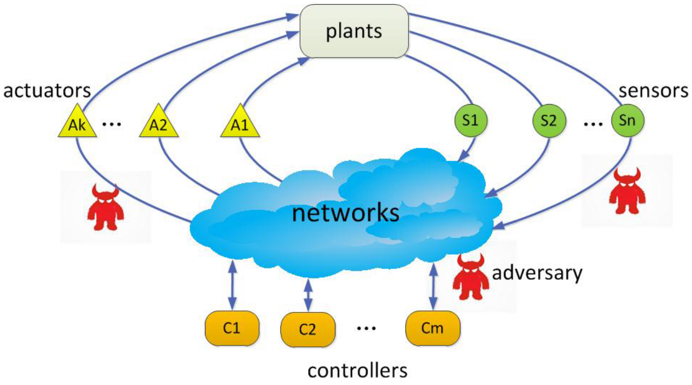


Fig. 1. Typical architecture of cyber-physical systems

From the systematic viewpoint, physical plants and other entities interact with each other in CPS, and essentially formed a feedback loop. We denote x_k as the state vector of physical plants at time k. The sensor S_i observes the state and sends the observations $y_{i,k}$ to the controllers. After receiving the observations, the controller C_j computes the state estimate $\widehat{x}_{j,k}$, and then sends the control command $u_{j,k} = f_u(\widehat{x}_{j,k})$ to the actuators, where f_u is the designed control law. Then actuators implement these control commands at time k. Note that the controllers are designed to optimize the performance $J = J(u)$. For example, optimal control of instantaneous power flows is designed to keep the energy level of each local storage close to the ideal level, and reduce the power flow among the grids simultaneously [9]. This objective can be formulated as a LQG function, which is an important system performance in smart grid.

B. Differential privacy in CPS

In CPS, the adversaries can eavesdrop the sensor-to-controller communication channels and controller-to-actuator communication channels in networks, and then exploit the collected data to infer the state of system and deduce some sensitive personal information [1]. In order to preserve the privacy of CPS, we leverage differential privacy approach to protect the observation data sending from sensors to controllers and the command data sending from controllers to actuators.

In [11], (ϵ, δ)-differential privacy is defined by probability inequality. From this definition, the original information is randomly mapped to a subset of the output range, and the adversary cannot infer the original information from the output dataset. The parameters ϵ, δ determines the privacy level. More privacy will be achieved when the parameters are closer to 0. We also can see that this new privacy preserving approach is independent of the acquired background knowledge by the adversaries. It means that this method does not need to update when the new type attack appears. Another advantage of differential privacy is the solid mathematical definition which provides a rigorous and self-contained theory basis and quantitative evaluation method for privacy.

In practical, several mechanisms have been proposed to realize the privacy preserving for numeric data, e.g., Gaussian mechanism, Laplace mechanism [7]. For the Gaussian mechanism, independent and identically distributed (i.i.d.) Gaussian noises with zero-mean are added to the measurements to achieve (ϵ, δ)-differential privacy. In this article, we make use of this type mechanism to protect the privacy in CPS.

According to the differential privacy approach, we preserve the privacy by adding noises $y^a_k \in \mathbb{R}^n$ and $u^a_k \in \mathbb{R}^m$ to the sensor's transmitting data $y_k = (y_{1,k}, y_{2,k}, \ldots, y_{n,k})'$ and the control data $u_k = (u_{1,k}, u_{2,k}, \ldots, u_{m,k})'$ in each time k respectively. Thus, the sensor transmitting data and control data will become $\widetilde{y}_k = y_k + y^a_k$, and $\widetilde{u}_k = u_k + u^a_k$.

In fact, differential privacy can guarantee the accuracy of statistical information without revealing individual privacy. An example is the privacy preservation in smart grid. If we are interested in the average of power consumption in a period, we can see that the average value without privacy protect and that with differential privacy are very close in the sense of mathematical expectation. Meanwhile, the adversary cannot know the accurate power consumption in any individual time when the system has differential privacy mechanism. Thus the adversary cannot easily infer the personal habits from the data, which is obtained from eavesdropping the communication network. The variance of added noise is the indicator of average deviation between the measurement without privacy protect and that with privacy preserving. Note that this deviation is determined by differential privacy parameters ϵ, δ. The larger artificial noises are added to the data before transmission, the better privacy is preserved. Meanwhile, the system performance will become worse. Thus, a crucial problem is how to balance the privacy requirement and system performance requirement. This motivates us to study the following problem.

C. Optimization problem

From the viewpoint of system, our objective is to optimize the performance of CPS, i.e., $J = J(u)$, by designing control law f_u and preserving the privacy by designing stochastic mapping M simultaneously. Specifically, we aim to minimize the performance J under privacy requirements $\epsilon = \epsilon_0$, and $\delta = \delta_0$ for the control data sequence $u_1, u_2, \ldots$, and measurement sequence $y_1, y_2, \ldots$, under given adjacency operation Adj. Then this optimization problem can be formulated as follows:

Problem 1

$$\begin{aligned} & J^* = \min(or\ \max) J(u, u^a, y^a) \\ & s.t.\ \ \epsilon = \epsilon_0, \delta = \delta_0. \end{aligned}$$

When the system works with optimal control strategy $u^* = (u_1^*, u_2^*, \ldots, u_k^*, \ldots)$ and optimal differential privacy variables $u^{a*} = (u_1^{a*}, u_2^{a*}, \ldots, u_k^{a*}, \ldots)$, $y^{a*} = (y_1^{a*}, y_2^{a*}, \ldots, y_k^{a*}, \ldots)$, its performance can reach the minimum or maximum. Different from classical optimal control problem, this new problem can not only optimize the system performance, but also preserve the individual privacy.

Note that individual privacy requirement constraint ϵ_0, δ_0 can be determined by his expected rewards from privacy selling [8]. For example, if his expected rewards $reward(\varepsilon, \delta)$ are more than a given value r_0, i.e., $reward(\varepsilon, \delta) \geq r_0$, we can obtain the optimal privacy requirement ϵ_0, δ_0 from this inequality of reward requirement.

III. A case study: LQG control

LQG control has a wide range of applications in CPS, such as smart grid [9], marine [12], etc. It focuses on linear system model with additive white Gaussian noise, and aims to optimally control the system subject to quadratic costs. We have pointed out that the adversary can infer the user's individual habits with the accurate data from sensors in smart grid. When the system exploits differential privacy to preserve the privacy, it can add some noises to the data, and then the adversary cannot infer the information of individual habits easily. The parameters ε, δ in differential privacy can be deem as the indicator of the privacy preserving level. Thus, the problem becomes how to optimize the quadratic costs when the privacy preserving level is given. Thus, we consider optimal LQG controller design with privacy requirement constraint in this section.

Modeling the dynamics of CPS is a challenging work since it involves the complex interactions between control, communication and computing entities. From the viewpoint of networked control society, a basic characteristic of CPS is that the communication network mediates between control and physical entities [1]. Thus, the dynamics of physical entities can be modelled as general difference equations with state variables, control variables, and the noises. For example, the linear difference equations have been exploited to depict the state dynamics of smart grid on the amount of generated power, the amount of consumed power, the time integral of the difference in power supply and power demand, and the price of a unit of power in [13]. In this section, we consider a specific linear CPS, e.g., a smart grid system [13], in which the system evolves as follows:

$$\begin{aligned} x_{k+1} &= Ax_k + u_k + w_k, \\ y_k \quad &= Cx_k + v_k, \end{aligned} \tag{1}$$

where $w_k, k = 1, 2, \ldots,$ are i.i.d. zero mean Gaussian process noises with covariance σ_w^2, and $v_k, k = 1, 2, \ldots,$ are i.i.d. zero mean Gaussian measurement noises with covariance σ_v^2, respectively. For brevity, we assume that there is one sensor, one controller, and one actuator in this system.

A. Parameters design of Gaussian mechanism

Gaussian noises are added to measurements $y_k, k = 1, 2, \ldots,$ and control variables $u_k, k = 1, 2, \ldots,$ in order to prevent the adversary inferring private information from these data. Then the system dynamics becomes

$$\begin{aligned} x_{k+1} &= Ax_k + u_k + u_k^a + w_k, \\ y_k \quad &= Cx_k + v_k + y_k^a, \end{aligned} \tag{2}$$

where $u_k^a, k = 1, 2 \ldots,$ and $y_k^a, k = 1, 2 \ldots,$ are i.i.d. zero mean Gaussian random variables with covariance σ_u^2, σ_y^2, respectively. Note that the process noises and measurement noises are all Gaussian. When artificial Gaussian noises are added to protect the privacy, new process noise, i.e., $u_k^a + w_k$, and new measurement noise, i.e., $v_k + y_k^a$, are still Gaussian. Then the well-known Kalman filtering method can be exploited to filter the noises when the estimator computes the system state. However, if artificial Gaussian noises are replaced by other types of noises, e.g., Laplace noises, this method is not available and more complex filtering method needs to be designed. Thus, for the brevity, we utilize Gaussian mechanism to preserve the privacy in this article.

We assume that the data privacy requirements are given as $\epsilon = \epsilon_0, \delta = \delta_0$. From [7], we have

$$\sigma_u \geq \sigma_{u0} = \frac{d}{2\epsilon_0}(K + \sqrt{K^2 + 2\epsilon_0}), \tag{3}$$

$$\sigma_y \geq \sigma_{y0} = \frac{d}{2\epsilon_0}(K + \sqrt{K^2 + 2\epsilon_0}), \tag{4}$$

where $K = \left(\frac{1}{\sqrt{2\pi}} \int_{\delta_0}^{+\infty} e^{-\frac{t^2}{2}} dt\right)^{-1}$, and the constant d is from the adjacency operation $Adj(z^{(1)}, z^{(2)})$. Then the privacy requirements can be achieved with (3) and (4). Note that d indicates the sensitivity of the data since $z^{(1)}, z^{(2)}$ will be treated as equivalent if $|z^{(1)} - z^{(2)}| \leq d$.

In fact, (3) and (4) can guarantee that the individual privacy information cannot be inferred by the adversaries in CPS. For example, the adversaries can hardly obtain the accurate system state in smart grid, and then the individual private information, e.g., personal habits, is almost impossible to be obtained by the adversaries.

It is obvious that the differential privacy affects the design of controller. The natural question is, how to design the optimal LQG controller when the transmission data is under differential privacy protect with the given privacy requirement. We will give the answer below.

B. Optimal LQG controller design with given privacy requirement

We aim to minimize the following Linear Quadratic Gaussian (LQG) control cost

$$J = \lim_{T \to \infty} \frac{1}{T} \sum_{k=1}^{T} \mathbb{E}[x_k^2 + \lambda \widetilde{u}_k^2]$$

when the transmission data are under given privacy requirement. Note that this cost function can be seen as the trade-off between regulation performance and control cost, and λ is the weight between them.

We have designed the Gaussian mechanism on y_k and u_k respectively. The remaining work is to design the optimal LQG controller with given Gaussian mechanism.

Similar to [14], we exploit dynamic programming method, and then obtain the optimal linear static controller $u_k = L\hat{x}_k = -SA(S+\lambda)^{-1}\hat{x}_k$, where L is the feedback control gain, $S = \frac{1}{2}(-\lambda + \lambda A^2 + 1 + \sqrt{\Delta})$ is the solution of Riccati difference equation $S_k = A^2 S_{k+1}^2[1-(S_{k+1}+\lambda)^{-1}]+1$ and $\Delta = (\lambda - \lambda A^2 - 1)^2 + 4\lambda$, and $\hat{x}_k$ can be obtained from Kalman filtering [14].

If we only focus on the privacy in sensor side or controller side, Gaussian noises can be injected to the sensor measurements or control commands alone. It means that $\sigma_u = 0$ or $\sigma_y = 0$ in our solution. Hence, our solution can also handle the case when only one side privacy is considered. Note that the above result is on the scaler linear system, and can be easily generalized to multi-variable case. In some practical systems, there may be multiple state variables and control commands. We can add multi-dimension zero mean Gaussian noise vectors to the sensor measurements and the control commands, respectively. Similarly, the optimal solution can be obtained for the multi-variable case.

C. Simulation and system performance analysis

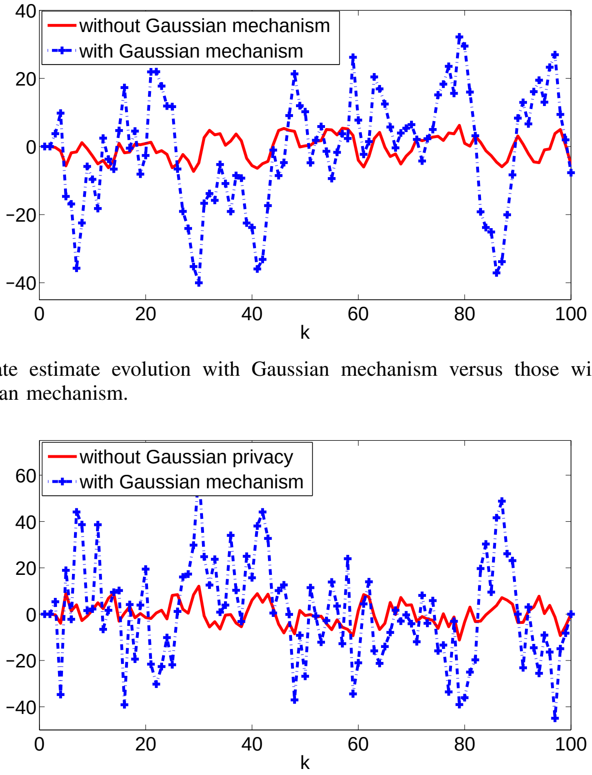
In order to investigate how much the designed privacy mechanism influences the system performance, consider a linear system with parameters in Table I. In accordance with Section III, we add Gaussian noises to the sensor measurements and control data, respectively.

Parameters	Setting
system parameters	$A = 2, C = 1.5$
system noise covariance	$\sigma_w = 1$
measurement noise covariance	$\sigma_v = 1$
weight	$\lambda = 0.5$
initial system state	$x_0 = 0$

TABLE I
System parameters for simulation.

To achieve the goal of system privacy preserving level with given differential private parameters $\epsilon = 0.1, \delta = 0.5$, it can be calculated that the adding measurement noises and control data noise can both be distributed with $\sigma_u \geq 4.2593, \sigma_y \geq 4.2593$. Since the system performance J is composed of two parts, i.e., system states and control data, we show the variation of the system state and control data in Fig. 2 under Gaussian mechanism with $\sigma_u = 4.2593, \sigma_y = 4.2593$. Due to the influence of artificial interference, the fluctuations of state estimation and control data under privacy preserving are all larger than those without Gaussian mechanism.

From Section III-B, one can see that the optimal controller is composed of control gain L and state estimate $\widehat{x}_k$. Thus the state estimation quality will impact the system performance J. State estimation quality is often measured by state estimation errors, the difference between state estimates and corresponding real states. Fig. 3 shows the variation of state estimation errors with given privacy requirements. It can be seen that a higher value of privacy parameters ϵ, δ will lead to a smaller estimate error.



(a) State estimate evolution with Gaussian mechanism versus those without Gaussian mechanism.

(b) Control data with Gaussian mechanism versus those without Gaussian mechanism.

Fig. 2. Illustrate the effectiveness of differential privacy on the state estimation and control data.

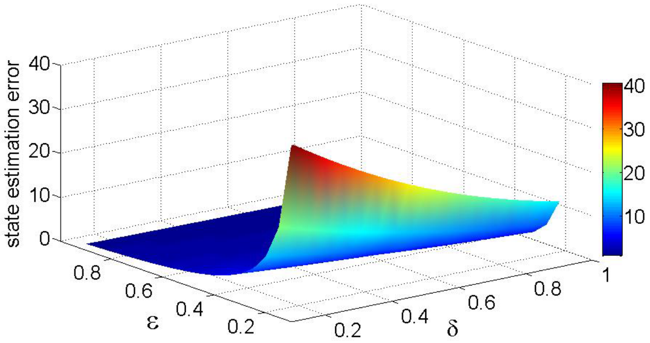
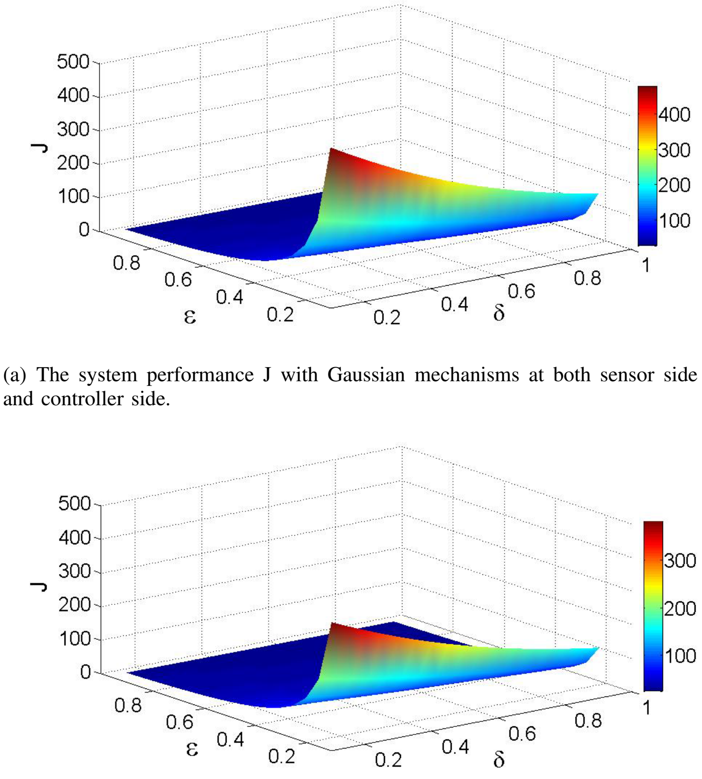


Fig. 3. State estimation errors under different privacy preserving requirements.

We analyze the effectiveness of differential privacy on the system performance J and the variations of J with parameters δ, ϵ are shown in Fig. 4. When the Gaussian noises are added to measurements and control data, jointly consider the influence of parameters δ, ϵ on the system performance J, we can see the variations of J from Fig 4(a). Fig 4(b) shows the variation of J when the Gaussian noises are only added to measurements. From Fig. 4, one can conclude that the larger privacy requirement, the greater cost J.

IV. Future prospective work

To our best knowledge, this is the first work to balance the tradeoff between the system performance and privacy



(a) The system performance J with Gaussian mechanisms at both sensor side and controller side.

(b) The system performance J with Gaussian mechanism at sensor side.

Fig. 4. Illustrate the effectiveness of differential privacy on the system performance J.

requirement in CPS. This article opens a door to a new research field, i.e., the privacy and performance trade-off in CPS. Here we identify three major challenges in this field in the future research:

First, investigate the privacy preserving problem on more general system models, e.g., the networked control system with multiple variables and multiple controllers, nonlinear system model and so on. We only study the problem on a simple system in this article, and it is more challenging to balance the privacy requirement and system performance on complex CPS system. The reason is that a complex CPS system may be dynamic space-time coupling. Then privacy preserving mechanism and system performance cannot be optimized separately, and new joint optimization methods are needed.

Second, design more efficient privacy preserving mechanism, e.g., to modify the existing differential privacy mechanism or propose a new mechanism in order to decrease the system cost as much as possible. If we add too much noises to the measurement data or control data which are not including individual privacy, the system may have to pay additional cost. Thus, we should further refine the privacy requirements, and design a more efficient privacy preserving mechanism to reduce the system cost.

Third, jointly exploit feedback control technology and differential privacy mechanism to investigate new challenging issues of privacy in specific CPS systems, e.g., smart grid, social network systems. For example, users need to protect the identity information, electricity consumption data, and other private information in smart grid. These different types of privacy need to be protected simultaneously with differential privacy. A challenging problem is how to balance the control performance and multiple privacy preserving requirements.

V. Conclusion

In this article, we investigate the optimal privacy-preserving controller design for CPS. We introduce the system architecture and the definition of differential privacy in CPS, and then we formulate an optimization problem in which system cost is optimized subject to privacy requirement. For linear system, we design optimal control law to minimize the LQG cost under the given privacy requirement and obtain the corresponding cost. A simulation example is presented to show the system state evolutions, estimation errors and system costs under differential privacy protection.

References

[1] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. IEEE ICDCS Workshops*, 2008, pp. 495–500.

[2] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," *IEEE Network*, vol. 27, no. 1, pp. 19–24, 2013.

[3] "Broad agency announcement meta," Tactical Technology Office, Defense Advanced Research Projects Agency, Tech. Rep. DARPA-BAA-10-21, 2009.

[4] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser, "Neighborhood watch: Security and privacy analysis of automatic meter reading systems," in *Proc. ACM CCS*, 2012, pp. 462–473.

[5] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," *IEEE Network*, vol. 28, no. 4, pp. 46–50, 2014.

[6] K. Apostol, *Brute-force Attack*. SaluPress, 2012.

[7] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[8] A. Ghosh and A. Roth, "Selling privacy at auction," *Games and Economic Behavior*, 2013.

[9] R. Minciardi and R. Sacile, "Optimal control in a cooperative network of smart power grids," *IEEE Systems Journal*, vol. 6, no. 1, pp. 126–133, 2012.

[10] B.-S. Chen and Y.-M. Cheng, "A structure-specified h∞ optimal control design for practical applications: a genetic approach," *IEEE Trans. Control Systems Technology*, vol. 6, no. 6, pp. 707–718, 1998.

[11] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*, 2008, pp. 1–19.

[12] M. Grimble, "Lqg feedforward/feedback stochastic optimal control and marine application," *Transactions of the Institute of Measurement and Control*, vol. 21, no. 1, pp. 30–48, 1999.

[13] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 476–486, 2011.

[14] D. P. Bertsekas, D. P. Bertsekas, D. P. Bertsekas, and D. P. Bertsekas, *Dynamic programming and optimal control*. Athena Scientific Belmont, MA, 1995, vol. 1, no. 2.

Heng Zhang is currently a Ph.D candidate as a member of the Group of Networked Sensing and Control (IIPC-NeSC) in the State Key Laboratory of Industrial Control Technology at Zhejiang University. His research interests include security and privacy in cyber-physical systems, control and optimization theory.

Yuanchao Shu is a Ph.D candidate in Control Science and Engineering at Zhejiang University, China and a joint PhD student in Computer Science at University of Michigan, Ann Arbor. He is the author and co-author of over 10 papers in premier journals and conferences, and is the recipient of the Best Demo Award of IEEE INFOCOM 2014. His research interests include Mobile Computing and networked control, optimization and systems design in Cyber-Physical Systems and Wireless Sensor Networks. He is a student member of ACM and IEEE.

Peng Cheng (IEEE M'10) received the B.E. degree in Automation, and the Ph.D. degree in Control Science and Engineering in 2004 and 2009 respectively, both from Zhejiang University, China. Currently he is an associate professor with the Department of Control Science and Engineering, Zhejiang University. He serves as Associate Editor for Wireless Networks, International Journal of Distributed Sensor Networks, and International Journal of Communication systems. He also served as publicity co-Chair for IEEE MASS 2013 and Local Arrangement Chair for ACM MobiHoc 2015. His research interests include networked sensing and control, cyber-physical systems, and robust control.

Jiming Chen (IEEE M'08 SM'11) is a full professor with Department of control science and engineering, and the coordinator of group of Networked Sensing and Control in the State Key laboratory of Industrial Control Technology, Vice Director of Institute of Industrial Process Control at Zhejiang University, China. He currently serves associate editors for several international Journals including IEEE Transactions on Parallel and Distributed System, IEEE Transactions on Industrial Electronics, IEEE Network, IEEE Transactions on Control of Network Systems, *etc.* He was a guest editor of IEEE Transactions on Automatic Control, Computer Communication (Elsevier), Wireless Communication and Mobile Computer (Wiley) and Journal of Network and Computer Applications (Elsevier). He also served/serves as General vice Chair, ACM MobhiHoc 2015, IEEE ICDCS 2012 Publicity Co-Chair, IEEE MASS 2013 Local Chair, and TPC member for IEEE ICDCS'10,'12,'13,'14, IEEE MASS'10,11,'13, IEEE SECON'11,'12,IEEE INFOCOM'11,'12,'13,'14 *etc.*