Paper: **Secure State Estimation and Control of Cyber-Physical Systems: A Survey**

Derui Ding , Senior Member, IEEE,
Qing-Long Han , Fellow, IEEE,
Xiaohua Ge , Member, IEEE, and
Jun Wang , Fellow, IEEE

Presented by: Oscar Llerena

Abstract

- Cyber-physical systems (CPSs) integrate physical processes and cyber infrastructure using computation resources and communication capabilities.
- CPSs have a wide variety of applications in areas such as energy, transportation, advanced manufacturing, and medical health.
- The security of CPSs against cyberattacks is a long-standing concern due to their extendable vulnerabilities beyond classical networked systems.
- Sophisticated and malicious cyberattacks can adversely impact CPS operation, resulting in performance degradation, service interruption, and system failure.
- Secure state estimation and control technologies are essential for reliable monitoring and operation of safety-critical CPSs.
- The article provides a review of the state-of-the-art results for secure state estimation and control of CPSs.
- The latest development of secure state estimation is summarized in light of different performance indicators and defense strategies.
- Recent results on secure control are discussed and classified into three categories: centralized secure control, distributed secure control, and resource-aware secure control.
- Two specific application examples of water supply distribution systems and wide-area power systems are presented to demonstrate the applicability of secure state estimation and control approaches.
- Several challenging issues are discussed to direct future research.

Content

I. CYBER-PHYSICAL SYSTEMS

II. TYPICAL CYBERATTACKS

III. SECURE STATE ESTIMATION OF CPSS

   A. Variance-Based Secure State Estimation

   B. Stability-Based Secure State Estimation

IV. SECURE CONTROL OF CPSS

   A. Centralized Secure Control

   B. Distributed Secure Control

   C. Resource-Aware Secure Control

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

   A. Secure State Estimation of Water Distribution Systems

   B. Security Control of Wide-Area Power Systems

VI. CONCLUSION AND CHALLENGING ISSUES

I. CYBER-PHYSICAL SYSTEMS

- CPSs employ networks of multifunctional sensors and actuators as well as cyber components. CPSs are playing a critical role in the 4th industrial revolution.
- CPSs are essentially complex, large-scale, geographically dispersed, and safety-critical. Ubiquitous computing and communication resources enable pervasive multilayered CPSs, which gives rise to additional security vulnerabilities.
- Secure state estimation and control constitute an effective and promising means for addressing various security-related issues of CPSs. The main objective is to keep an acceptable performance level of the CPS.
- In the past few years, there are several survey papers of security-oriented CPSs. From a systems and control perspective, the CPS security issue is evaluated. Emerging techniques improving the safety and security of CPSs are surveyed.
- Security analysis and synthesis of CPSs rely on suitable dynamical models of CPSs and reasonable mathematical descriptions of cyberattacks. The inherently unknown attack knowledge and generally complex system dynamics induce several major roadblocks.

II. TYPICAL CYBERATTACKS

- Cyberattacks on CPSs can be roughly classified into two types: 1) denial-of-service (DoS) attacks and 2) deception attacks. Deception attacks intend to compromise data integrity and trustworthiness by manipulating packets over communication networks.
- Security performance analysis is reliant on a priori statistical information of the random DoS attacks. The motivation for sophisticated adversaries adopting such probabilistic attack models requires further justification in realistic scenarios.
- Replay attacks generally do not require preliminary model knowledge. In the first step, some disclosure attacks are launched to record sensor measurements or control signals for some prescribed time.
- The central aim of FDI attacks is to mislead the system components, including estimators, filters, controllers, and actuators. FDI attacks on CPSs can target both physical equipment and cyber infrastructure.

III. SECURE STATE ESTIMATION OF CPSS

- For capturing the real-time dynamics of CPSs, it is crucial to reconstruct system states based on only measured yet possibly corrupted information from sensors.
- Different from traditional control systems, the tight integration of physical and cyber components pose nontrivial challenges to design of state estimators or filters.
- Table 1 summarizes existing secure state estimation approaches according to performance indicators and defense strategies against cyberattacks.

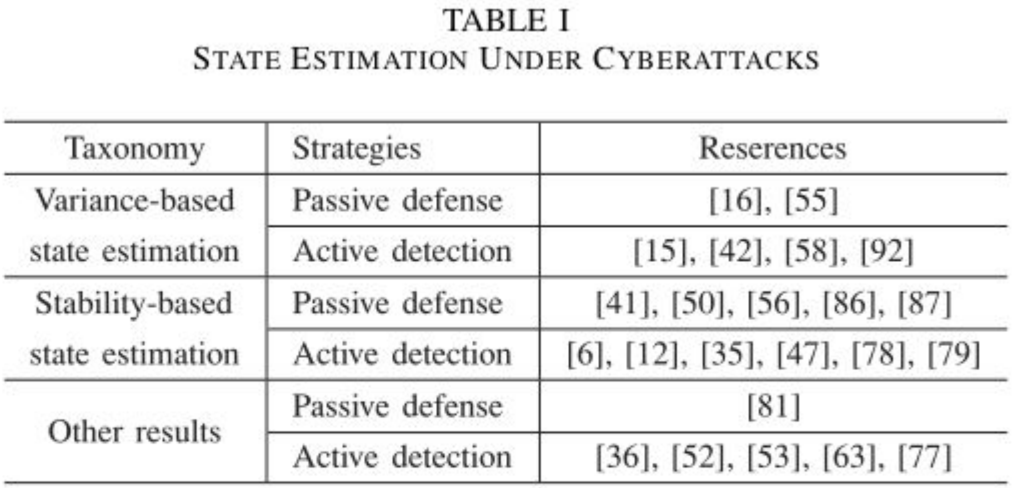


TABLE I
STATE ESTIMATION UNDER CYBERATTACKS

Taxonomy	Strategies	Reserences
Variance-based state estimation	Passive defense	[16], [55]
	Active detection	[15], [42], [58], [92]
Stability-based state estimation	Passive defense	[41], [50], [56], [86], [87]
	Active detection	[6], [12], [35], [47], [78], [79]
Other results	Passive defense	[81]
	Active detection	[36], [52], [53], [63], [77]

III. SECURE STATE ESTIMATION OF CPSS

A. Variance-Based Secure State Estimation

- The variance-based state estimation aims to select appropriate gain parameters to minimize estimation error variance as far as possible. In doing so, an indispensable assumption is that the structured information of cyberattacks is a priori known.
- Estimators or filters can also actively integrate some detection mechanisms to remove the compromised data generated by malicious attacks. For example, the adverse impact of FDI attacks for wireless sensor networks is effectively relieved by resorting to a protector.
- In practice, it is not uncommon that only a subset of sensors can be arbitrarily tampered with by attackers. It is worth noting that the estimation performance can be properly warranted if the corrupted sensor is accurately detected.

III. SECURE STATE ESTIMATION OF CPSS

B. Stability-Based Secure State Estimation

- Disturbance attenuation analysis provides an alternative framework for optimizing system performance in the presence of malicious attacks. Secure filtering issues under this framework are investigated in [86] for positive systems in a distributed way, in [41] for complex networks.
- Attack isolation and attack attenuation from the active defense perspective represent two typical approaches to counteract the negative effects of malicious attacks. In the past few years, attack identification and state estimation of CPSs subject to sparse attacks have been attracting ever-increasing interest.
- Employing some artificial saturation constraint on state estimators is regarded as a promising security measure for constraining attacker capability and mitigating the impulsive and/or outlier-like effects of cyberattacks. Dynamic saturations with an adaptive rule are further developed.
- Ellipsoidal and maximum correntropy indicators are used to evaluate security and estimation performance for CPSs. Cyberattacks on sensor measurements could result in significant deviations between the predicted ellipsoidal set and the updated ellipsoidal set during attack occurrence.

IV. SECURE CONTROL OF CPSS

- There are two substantial lines of research on secure control for CPSs under cyberattacks.
- The first category focuses on the design of a suitable control policy/law to tolerate unpredictable anomalies.
- The second category is concerned with the design of preferable compensation schemes to prevent the system performance and stability from getting severely deteriorative or even becoming unstable.
- A summary of some existing secure control results is provided in Table II.

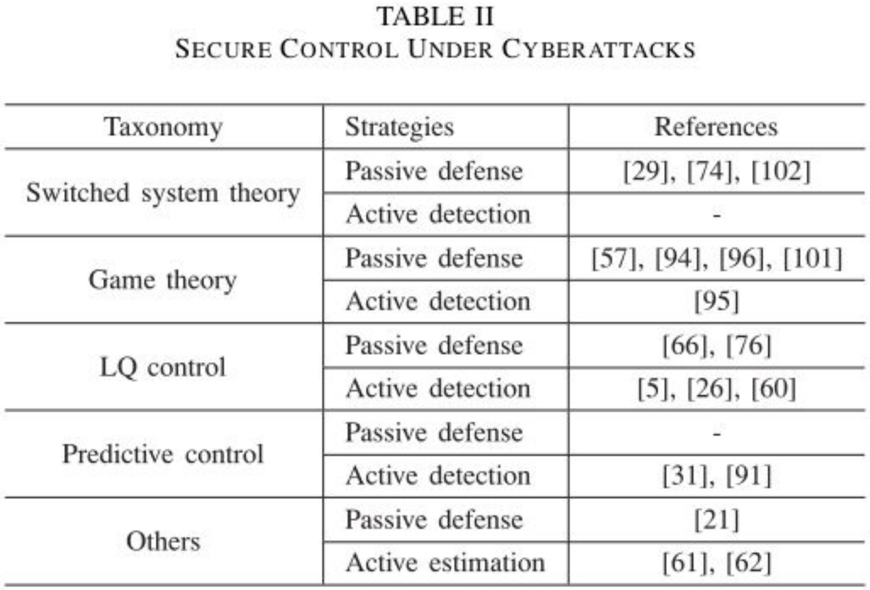


TABLE II
SECURE CONTROL UNDER CYBERATTACKS

Taxonomy	Strategies	References
Switched system theory	Passive defense	[29], [74], [102]
	Active detection	-
Game theory	Passive defense	[57], [94], [96], [101]
	Active detection	[95]
LQ control	Passive defense	[66], [76]
	Active detection	[5], [26], [60]
Predictive control	Passive defense	-
	Active detection	[31], [91]
Others	Passive defense	[21]
	Active estimation	[61], [62]

IV. SECURE CONTROL OF CPSS

A. Centralized Secure Control

- A direct consequence of DoS attacks on CPSs is that the system is operated in an open-loop manner. The primary goal of secure control is to find the tolerant duration and/or attack frequency such that the desired system performance remains achievable.
- Active detection of cyberattacks offers an effective means to enhance the system's adaptation to malicious attacks. Making existing attacks detected and removed largely promotes the system security.
- Defenders and attackers essentially play a noncooperative game, which contributes to the development of game theory. The derived saddle-point equilibrium, from the perspective of attackers, reflects the lowest attack intensity.
- Security of a practical CPS is regarded as a hard constraint that describes a guard line guaranteeing economic benefit and life safety. It is nontrivial to achieve absolute security for CPSs suffering from various stochastic disturbances and randomly occurring cyberattacks. As a result, an alternative indicator, known as security in probability is exploited.

IV. SECURE CONTROL OF CPSS

B. Distributed Secure Control

- The physical components of practical CPSs could be deployed in a spatially distributed way. This results in broader attack surfaces than traditional networked control systems.
- Distributed secure control that embeds attack model information (i.e., statistical or structured information) is proved to exhibit the capability of attack attenuation. For example, an impulsive controller against randomly occurring deception attacks is developed.
- The issue of a resilient consensus issue of distributed CPSs is extensively investigated. The effect of the trusted equipment (or nodes) is further explored in the past few years. The classical fault detection and estimation approaches provide a foundation to deal with the secure control issue.

IV. SECURE CONTROL OF CPSS

C. Resource-Aware Secure Control

- The efficient utilization of limited communication resources in CPSs stimulates extensive research interest from the control realm. In the past few years, various communication scheduling protocols are employed to govern the token.
- Time series of data transmissions or updates under communication schedules become more complex due mainly to the interference of malicious attacks. An event-triggered scheduling and control co-design algorithm is developed to obtain both the triggering parameter and the control gain.
- In the context of distributed secure control, there are considerable results reported for CPSs under event-triggered communication scheduling. It should be noted that the presence of cyberattacks makes the exclusion of Zeno behavior from the designed distributed event-triggered secure controllers.
- Attack detection and secure control are required to be seamlessly integrated. This leads to a tradeoff between detection precision and real-time control performance.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

- SCADA systems are broadly employed to provide remote monitoring and control solutions for geographically dispersed assets.
  a. [3]: Remote water pilfering attack is performed over a SCADA irrigation canal system.
  b. [4]: Attack signals performed in a water distribution network. Detection and isolation.
  c. [59]: Detection of replay attacks on SCADA system sensors.
- A water distribution system is made up a range of physical elements coupled with integrated computerized and communications technology, connecting a range of users, facilities, plants, stations, distribution, etc. A clear need to quantify the impact of adversarial attacks and evaluate countermeasures.

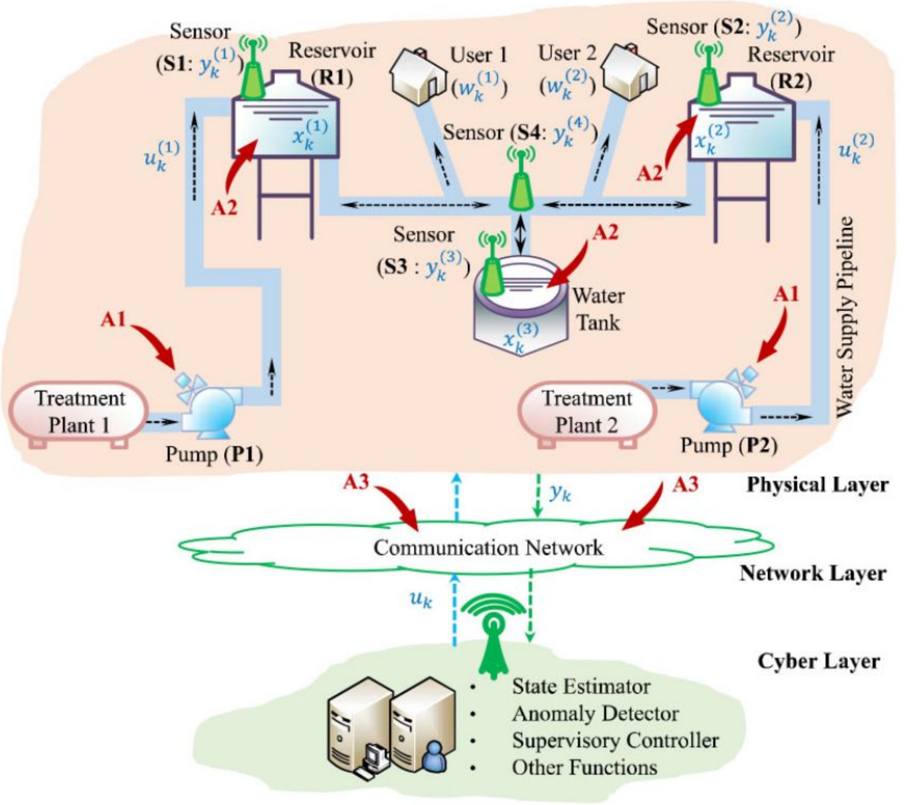


Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

- A SCADA water supply distribution system has 3 layers:
  a. Physical layer: waste-water treatment plants, water storage reservoirs, tanks, pipelines, sensors, junctions, actuators and other hydraulic devices.
  b. Cyber layer: a remote SCADA control center with state estimators, anomaly detectors, controllers, communication devices and more others, for real-time monitoring and supervising control.
  c. Network layer: enabling two-way data transmission among smart sensors, control center and actuators
- Discrete-time state-space model to describe a SCADA monitoring and control system:

$$\begin{cases} x_{k+1} = Ax_k + B_u u_k + B_w w_k + B_a a_k \\ y_k = Cx_k + D_w w_k + D_v v_k + D_a a_k \end{cases} \quad (1)$$

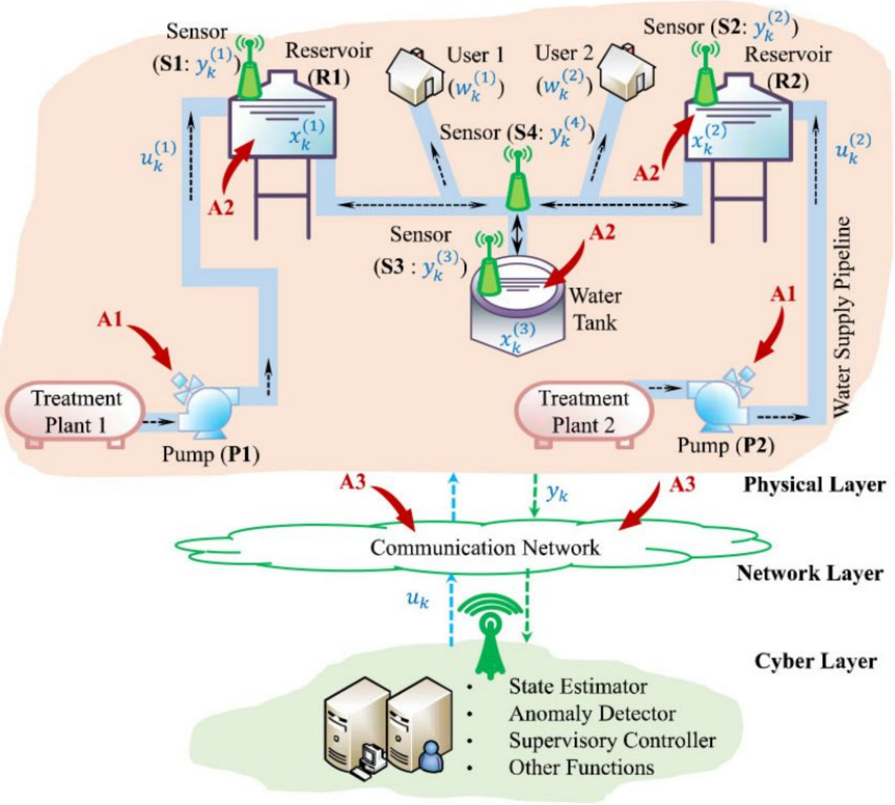


Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

$$\begin{cases} x_{k+1} = Ax_k + B_u u_k + B_w w_k + B_a a_k \\ y_k = Cx_k + D_w w_k + D_v v_k + D_a a_k \end{cases} \quad (1)$$

🟦 system state	⬛ disturbance	🟥 attacks
🟩 control signal	▢ Measurement noise	🟨 Sensor measurement at control center

attacks

$$a_k = \begin{cases} \phi_{k-k_0+1}, & k \in \mathcal{T}_L \\ \mathbf{0}, & k \notin \mathcal{T}_L \end{cases} \quad (2)$$

Attack duration $\mathcal{T}_L = \{k_0, k_0+1, \ldots, k_0+L-1\}$

Attack profiles $\mathcal{F}_L = \{\phi_1, \phi_2, \ldots, \phi_L\}$

$A, B_u, B_w, B_a, C, D_w, D_v,$ and D_a are real-valued matrices

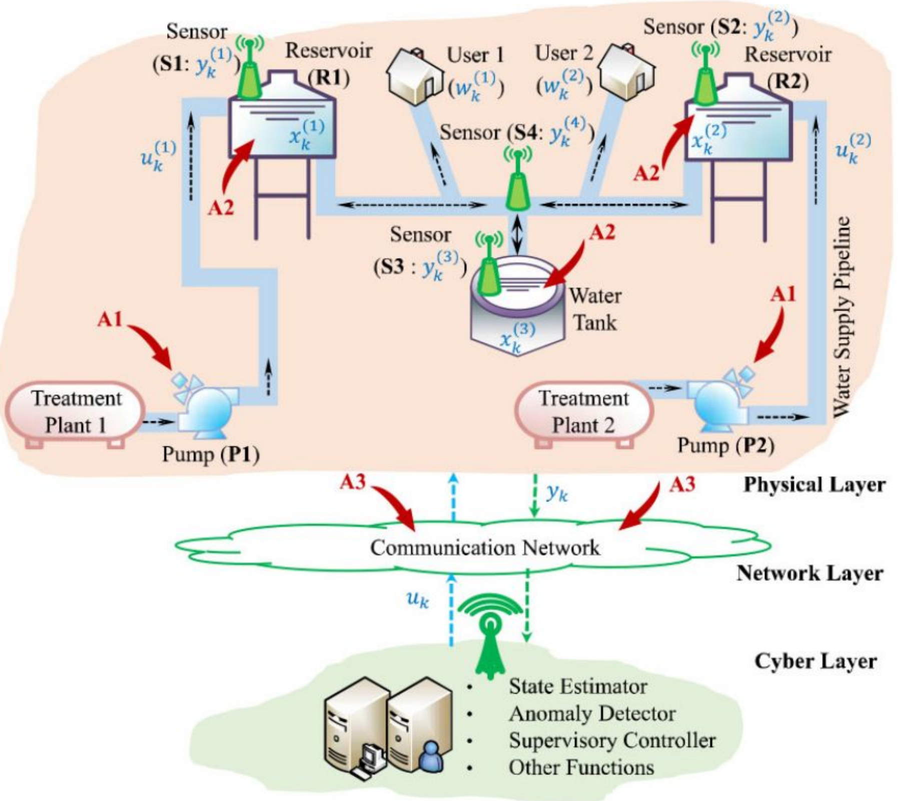
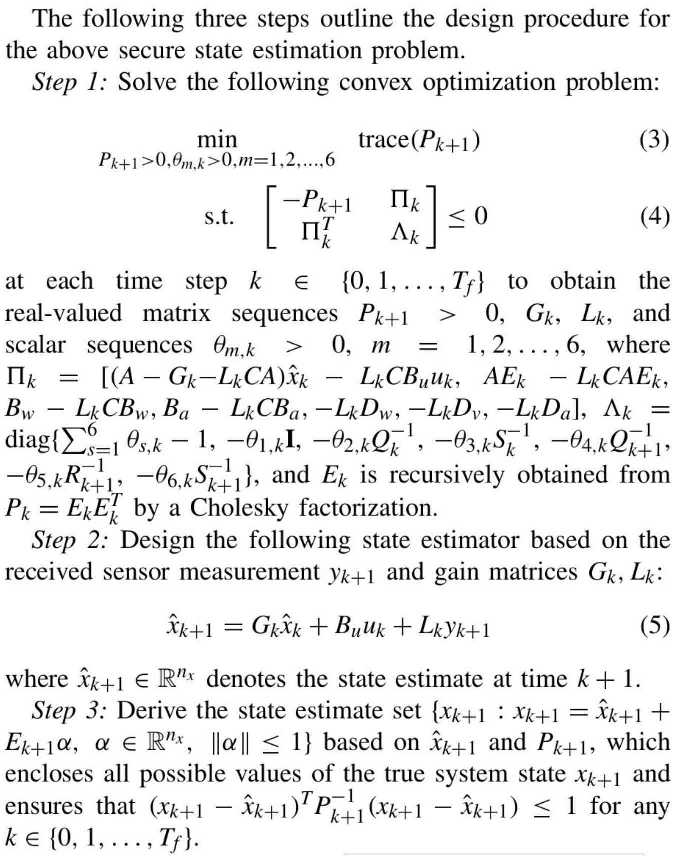


Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems



The following three steps outline the design procedure for the above secure state estimation problem.

Step 1: Solve the following convex optimization problem:

$$\min_{P_{k+1}>0,\theta_{m,k}>0,m=1,2,\ldots,6} \quad \mathrm{trace}(P_{k+1}) \tag{3}$$

$$\text{s.t.} \quad \begin{bmatrix} -P_{k+1} & \Pi_k \\ \Pi_k^T & \Lambda_k \end{bmatrix} \leq 0 \tag{4}$$

at each time step $k \in \{0, 1, \ldots, T_f\}$ to obtain the real-valued matrix sequences $P_{k+1} > 0$, G_k, L_k, and scalar sequences $\theta_{m,k} > 0$, $m = 1, 2, \ldots, 6$, where $\Pi_k = [(A - G_k - L_kCA)\hat{x}_k - L_kCB_uu_k,\ AE_k - L_kCAE_k,\ B_w - L_kCB_w, B_a - L_kCB_a, -L_kD_w, -L_kD_v, -L_kD_a]$, $\Lambda_k = \mathrm{diag}\{\sum_{s=1}^{6} \theta_{s,k} - 1,\ -\theta_{1,k}\mathbf{I},\ -\theta_{2,k}Q_k^{-1},\ -\theta_{3,k}S_k^{-1},\ -\theta_{4,k}Q_{k+1}^{-1},\ -\theta_{5,k}R_{k+1}^{-1},\ -\theta_{6,k}S_{k+1}^{-1}\}$, and E_k is recursively obtained from $P_k = E_kE_k^T$ by a Cholesky factorization.

Step 2: Design the following state estimator based on the received sensor measurement y_{k+1} and gain matrices G_k, L_k:

$$\hat{x}_{k+1} = G_k\hat{x}_k + B_uu_k + L_ky_{k+1} \tag{5}$$

where $\hat{x}_{k+1} \in \mathbb{R}^{n_x}$ denotes the state estimate at time $k + 1$.

Step 3: Derive the state estimate set $\{x_{k+1} : x_{k+1} = \hat{x}_{k+1} + E_{k+1}\alpha,\ \alpha \in \mathbb{R}^{n_x},\ \|\alpha\| \leq 1\}$ based on $\hat{x}_{k+1}$ and P_{k+1}, which encloses all possible values of the true system state x_{k+1} and ensures that $(x_{k+1} - \hat{x}_{k+1})^TP_{k+1}^{-1}(x_{k+1} - \hat{x}_{k+1}) \leq 1$ for any $k \in \{0, 1, \ldots, T_f\}$.

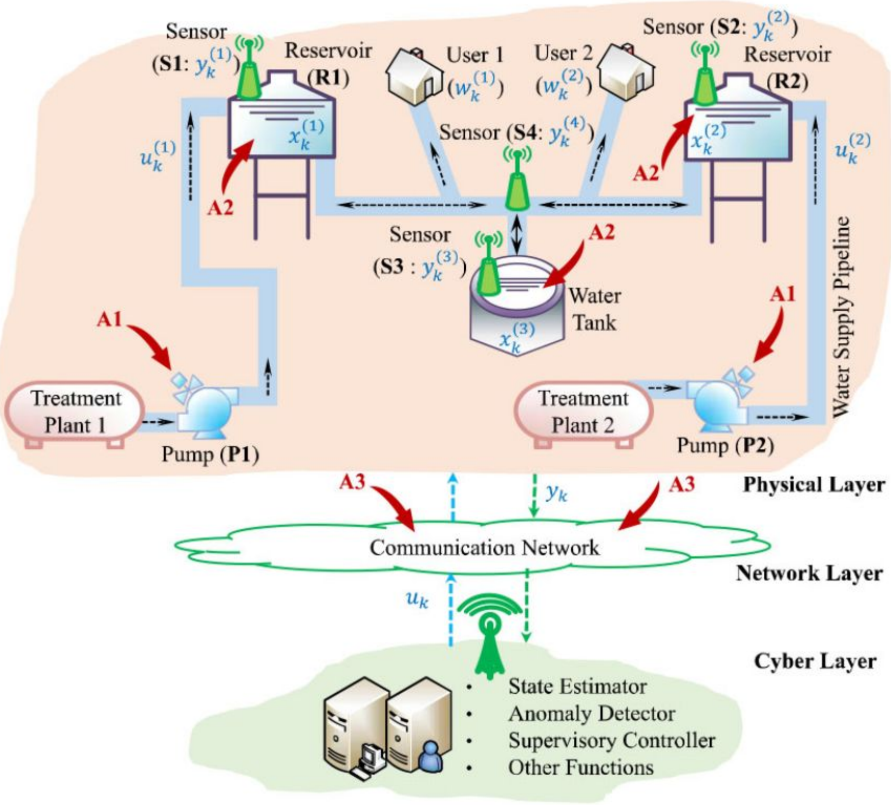


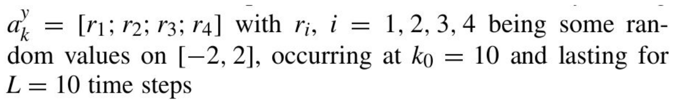
Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

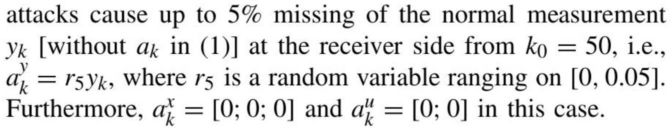
Next, authors evaluate the secure estimation of the SCADA system under attacks.

- Case I (FDI and DoS Attacks): first consider that an adversary deliberately alters the measurements of all sensors via concurrent FDI and DoS attacks (A3). The FDI attacks inject some erroneous/misleading information into sensor data over the communication network.
  a. FDI:



$a_k^y = [r_1; r_2; r_3; r_4]$ with r_i, $i = 1, 2, 3, 4$ being some random values on $[-2, 2]$, occurring at $k_0 = 10$ and lasting for $L = 10$ time steps

  b. DoS:



attacks cause up to 5% missing of the normal measurement y_k [without a_k in (1)] at the receiver side from $k_0 = 50$, i.e., $a_k^y = r_5 y_k$, where r_5 is a random variable ranging on $[0, 0.05]$. Furthermore, $a_k^x = [0; 0; 0]$ and $a_k^u = [0; 0]$ in this case.

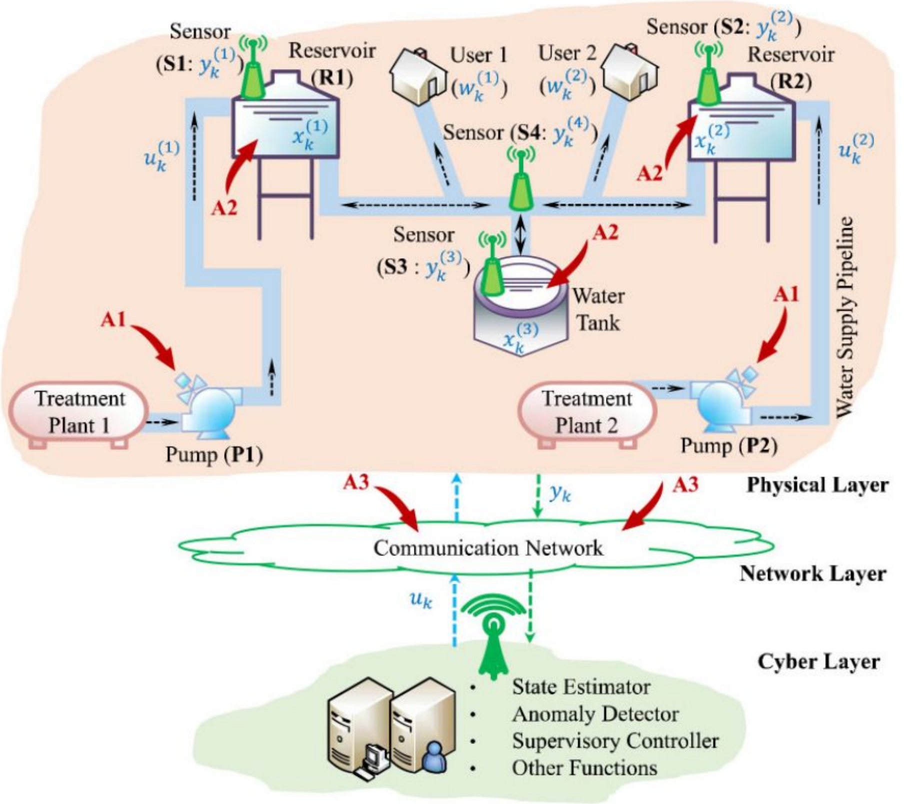


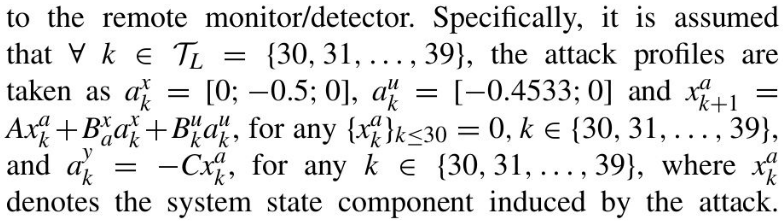
Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

Next, authors evaluate the secure estimation of the SCADA system under attacks.

- Case II (Stealthy Attacks): Disrupt the normal water distribution without being monitored or detected. The adversary performs some physical attacks on water reservoir and pump, causing the reservoir water levels to decrease significantly, while at the same time implementing some cyberattack strategy, such as FDI attacks to cover up the changes within the recorded sensor measurements, rendering the attacks stealthy



to the remote monitor/detector. Specifically, it is assumed that $\forall\ k \in \mathcal{T}_L = \{30, 31, \ldots, 39\}$, the attack profiles are taken as $a_k^x = [0; -0.5; 0]$, $a_k^u = [-0.4533; 0]$ and $x_{k+1}^a = Ax_k^a + B_a^x a_k^x + B_k^u a_k^u$, for any $\{x_k^a\}_{k \leq 30} = 0, k \in \{30, 31, \ldots, 39\}$, and $a_k^y = -Cx_k^a$, for any $k \in \{30, 31, \ldots, 39\}$, where x_k^a denotes the system state component induced by the attack.

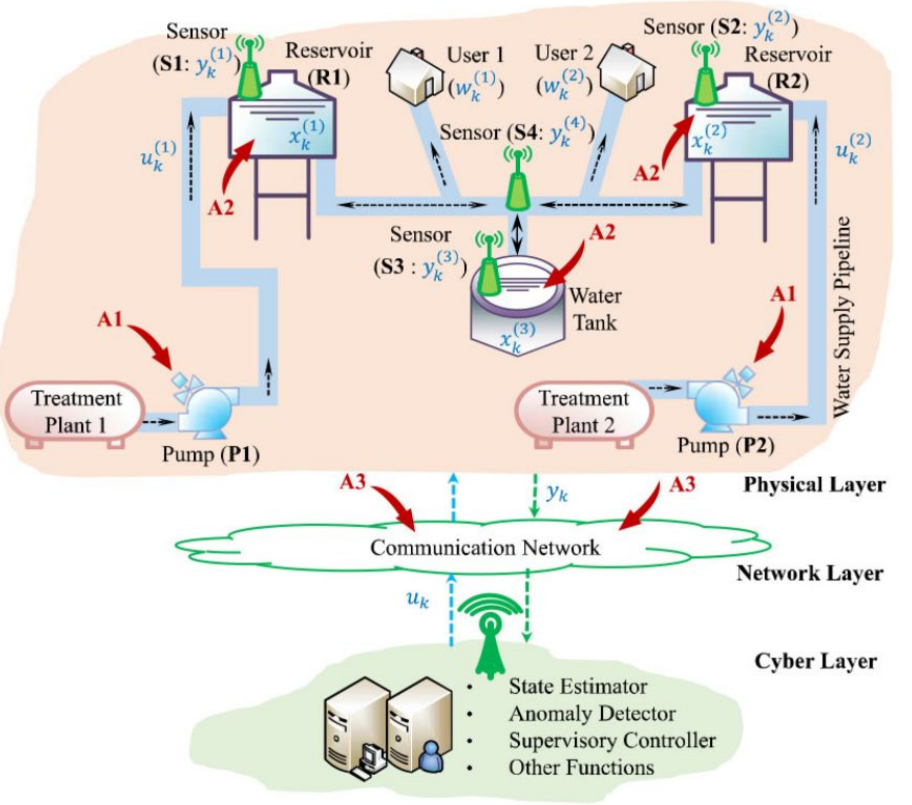


Fig. 1. SCADA water distribution system under attacks, pressure heads, sensor measurements, users, control signals, physical attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

A. Secure State Estimation of Water Distribution Systems

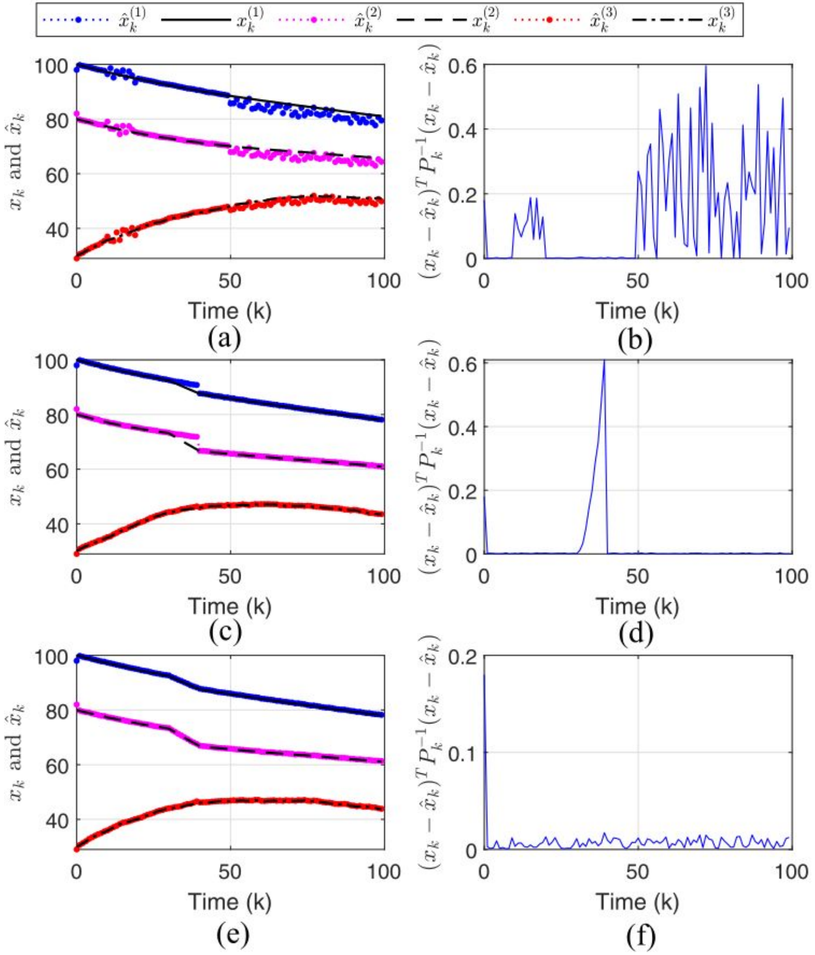
Simulation results: Case I,

- The state estimate ellipsoid guarantees the enclosing of the true system state regardless of the disturbance and noise as well as the simulated cyber FDI and DoS attacks on the sensor data.
- This also shows that simple cyberattack strategies via corrupting data availability and integrity may not cause sufficient disruption of the CPS.

Simulation results: Case II,

- Although the true system state resides in the state estimate ellipsoid, the pressure heads at R1 and R2 decrease notably from k = 30 since the water was being withdrawn from R1 and the pump P2 was turned off.
- However, the state estimator cannot track accurately the true system state because of the concealed measurement changes on sensors S1–S4, and thus the attacks are stealthy to the remote monitor.

When the channels of the critical sensors S1 and S2 are protected (e.g., via encryption) but the channel of S4 remains attacked, the state estimator offers accurate and prompt observations of the true system state, as depicted in Fig. 2(e) and (f).



V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems

- Smart grids as well as traditional power systems are more vulnerable to various malicious attacks. Their reliable operation is tightly related to the system's real-time information.
- Resilient estimation and control of power systems modeled by a dynamical state-space model are intensively studied. The load frequency control issues are investigated for multiarea power systems subject to energy-limited DoS attacks.
- A hierarchical control framework of power systems is commonly established to ensure power quality and frequency/voltage stability. To mitigate an attack impact, a finite-time control scheme is established to realize frequency regulation and active power-sharing.

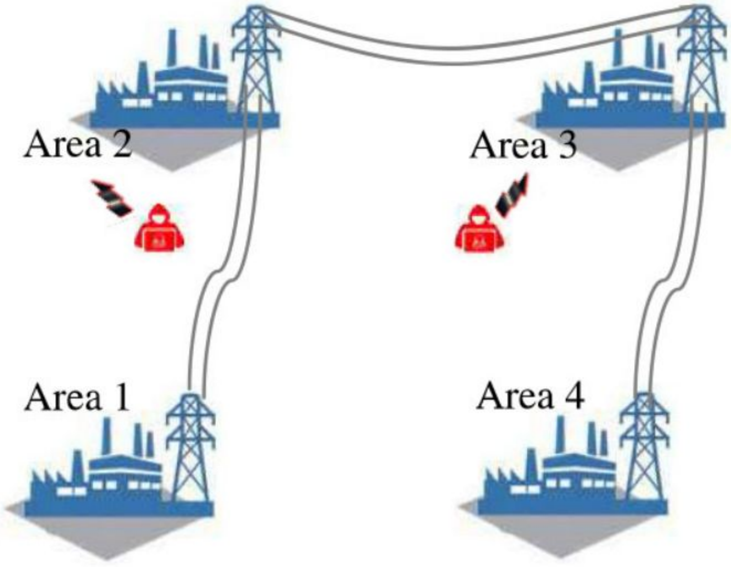
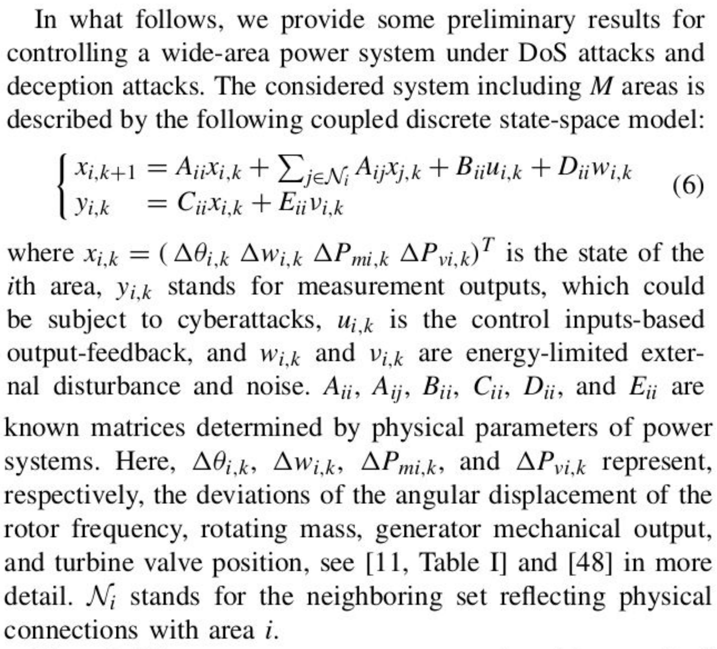


Fig. 3. Four area power system under attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems



In what follows, we provide some preliminary results for controlling a wide-area power system under DoS attacks and deception attacks. The considered system including M areas is described by the following coupled discrete state-space model:

$$\begin{cases} x_{i,k+1} = A_{ii}x_{i,k} + \sum_{j\in\mathcal{N}_i} A_{ij}x_{j,k} + B_{ii}u_{i,k} + D_{ii}w_{i,k} \\ y_{i,k} \quad = C_{ii}x_{i,k} + E_{ii}v_{i,k} \end{cases} \qquad (6)$$

where $x_{i,k} = (\,\Delta\theta_{i,k}\ \Delta w_{i,k}\ \Delta P_{mi,k}\ \Delta P_{vi,k})^T$ is the state of the ith area, $y_{i,k}$ stands for measurement outputs, which could be subject to cyberattacks, $u_{i,k}$ is the control inputs-based output-feedback, and $w_{i,k}$ and $v_{i,k}$ are energy-limited external disturbance and noise. A_{ii}, A_{ij}, B_{ii}, C_{ii}, D_{ii}, and E_{ii} are known matrices determined by physical parameters of power systems. Here, $\Delta\theta_{i,k}$, $\Delta w_{i,k}$, $\Delta P_{mi,k}$, and $\Delta P_{vi,k}$ represent, respectively, the deviations of the angular displacement of the rotor frequency, rotating mass, generator mechanical output, and turbine valve position, see [11, Table I] and [48] in more detail. $\mathcal{N}_i$ stands for the neighboring set reflecting physical connections with area i.

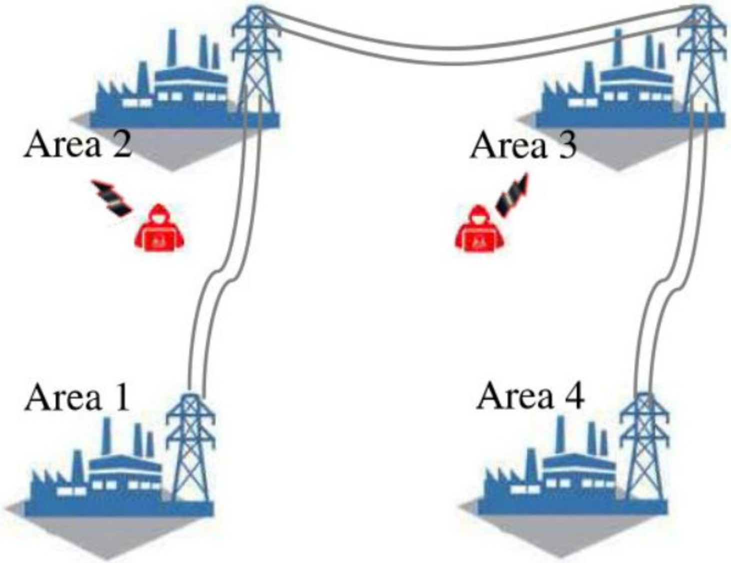
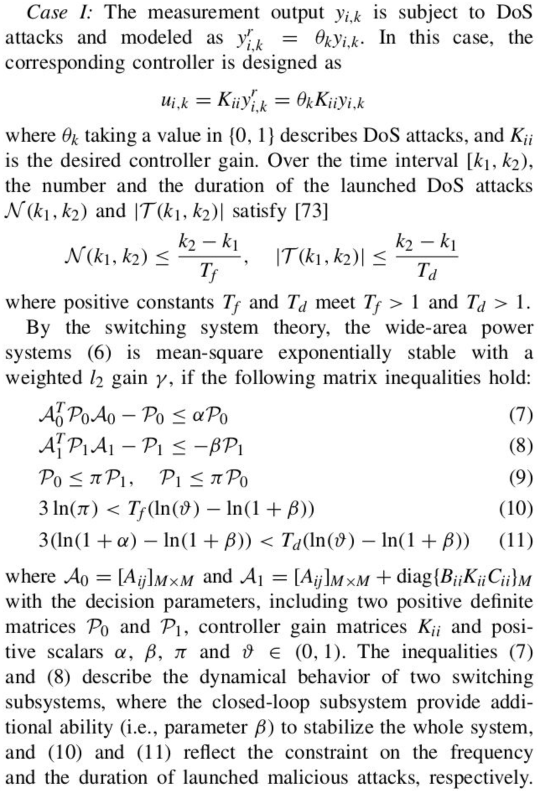


Fig. 3. Four area power system under attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems



Case I: The measurement output $y_{i,k}$ is subject to DoS attacks and modeled as $y^r_{i,k} = \theta_k y_{i,k}$. In this case, the corresponding controller is designed as

$$u_{i,k} = K_{ii} y^r_{i,k} = \theta_k K_{ii} y_{i,k}$$

where θ_k taking a value in $\{0, 1\}$ describes DoS attacks, and K_{ii} is the desired controller gain. Over the time interval $[k_1, k_2)$, the number and the duration of the launched DoS attacks $\mathcal{N}(k_1, k_2)$ and $|\mathcal{T}(k_1, k_2)|$ satisfy [73]

$$\mathcal{N}(k_1, k_2) \leq \frac{k_2 - k_1}{T_f}, \quad |\mathcal{T}(k_1, k_2)| \leq \frac{k_2 - k_1}{T_d}$$

where positive constants T_f and T_d meet $T_f > 1$ and $T_d > 1$.

By the switching system theory, the wide-area power systems (6) is mean-square exponentially stable with a weighted l_2 gain γ, if the following matrix inequalities hold:

$$\mathcal{A}_0^T \mathcal{P}_0 \mathcal{A}_0 - \mathcal{P}_0 \leq \alpha \mathcal{P}_0 \quad (7)$$

$$\mathcal{A}_1^T \mathcal{P}_1 \mathcal{A}_1 - \mathcal{P}_1 \leq -\beta \mathcal{P}_1 \quad (8)$$

$$\mathcal{P}_0 \leq \pi \mathcal{P}_1, \quad \mathcal{P}_1 \leq \pi \mathcal{P}_0 \quad (9)$$

$$3\ln(\pi) < T_f(\ln(\vartheta) - \ln(1+\beta)) \quad (10)$$

$$3(\ln(1+\alpha) - \ln(1+\beta)) < T_d(\ln(\vartheta) - \ln(1+\beta)) \quad (11)$$

where $\mathcal{A}_0 = [A_{ij}]_{M \times M}$ and $\mathcal{A}_1 = [A_{ij}]_{M \times M} + \text{diag}\{B_{ii} K_{ii} C_{ii}\}_M$ with the decision parameters, including two positive definite matrices $\mathcal{P}_0$ and $\mathcal{P}_1$, controller gain matrices K_{ii} and positive scalars α, β, π and $\vartheta \in (0, 1)$. The inequalities (7) and (8) describe the dynamical behavior of two switching subsystems, where the closed-loop subsystem provide additional ability (i.e., parameter β) to stabilize the whole system, and (10) and (11) reflect the constraint on the frequency and the duration of launched malicious attacks, respectively.

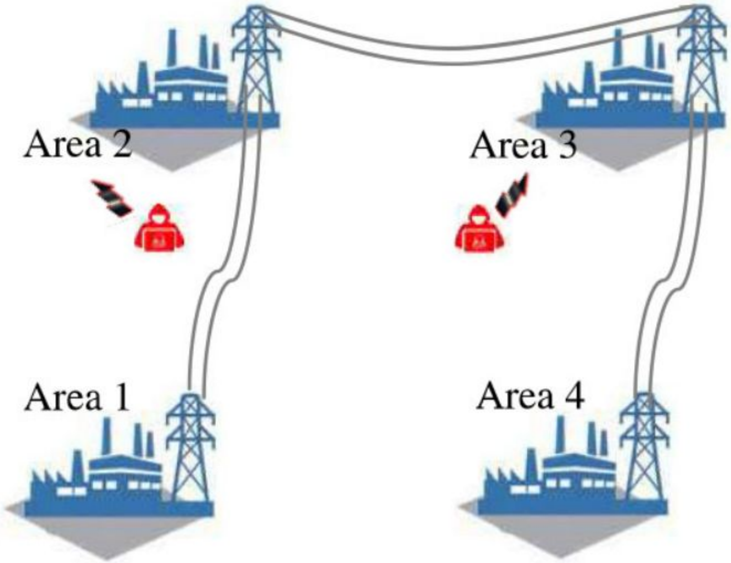
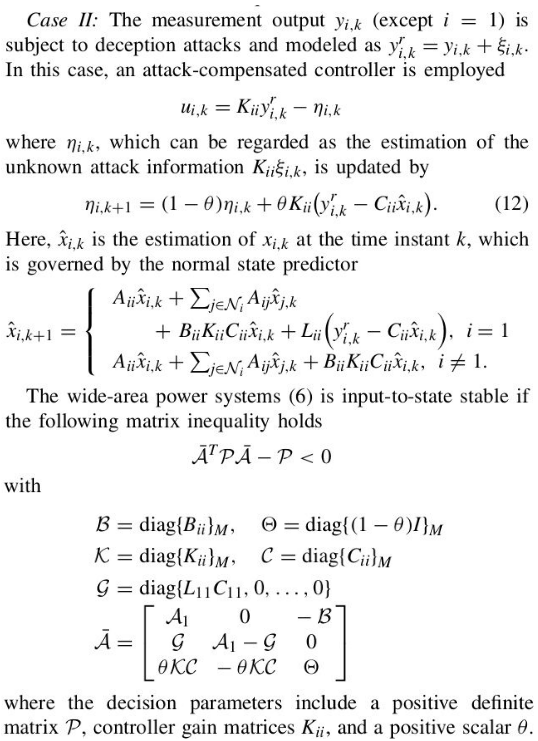


Fig. 3. Four area power system under attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems



Case II: The measurement output $y_{i,k}$ (except $i = 1$) is subject to deception attacks and modeled as $y^r_{i,k} = y_{i,k} + \xi_{i,k}$. In this case, an attack-compensated controller is employed

$$u_{i,k} = K_{ii} y^r_{i,k} - \eta_{i,k}$$

where $\eta_{i,k}$, which can be regarded as the estimation of the unknown attack information $K_{ii}\xi_{i,k}$, is updated by

$$\eta_{i,k+1} = (1-\theta)\eta_{i,k} + \theta K_{ii}\big(y^r_{i,k} - C_{ii}\hat{x}_{i,k}\big). \tag{12}$$

Here, $\hat{x}_{i,k}$ is the estimation of $x_{i,k}$ at the time instant k, which is governed by the normal state predictor

$$\hat{x}_{i,k+1} = \begin{cases} A_{ii}\hat{x}_{i,k} + \sum_{j\in\mathcal{N}_i} A_{ij}\hat{x}_{j,k} \\ \qquad + B_{ii}K_{ii}C_{ii}\hat{x}_{i,k} + L_{ii}\left(y^r_{i,k} - C_{ii}\hat{x}_{i,k}\right), & i = 1 \\ A_{ii}\hat{x}_{i,k} + \sum_{j\in\mathcal{N}_i} A_{ij}\hat{x}_{j,k} + B_{ii}K_{ii}C_{ii}\hat{x}_{i,k}, & i \neq 1. \end{cases}$$

The wide-area power systems (6) is input-to-state stable if the following matrix inequality holds

$$\bar{\mathcal{A}}^T \mathcal{P} \bar{\mathcal{A}} - \mathcal{P} < 0$$

with

$$\begin{aligned} &\mathcal{B} = \mathrm{diag}\{B_{ii}\}_M, \quad \Theta = \mathrm{diag}\{(1-\theta)I\}_M \\ &\mathcal{K} = \mathrm{diag}\{K_{ii}\}_M, \quad \mathcal{C} = \mathrm{diag}\{C_{ii}\}_M \\ &\mathcal{G} = \mathrm{diag}\{L_{11}C_{11}, 0, \ldots, 0\} \\ &\bar{\mathcal{A}} = \begin{bmatrix} \mathcal{A}_1 & 0 & -\mathcal{B} \\ \mathcal{G} & \mathcal{A}_1 - \mathcal{G} & 0 \\ \theta\mathcal{K}\mathcal{C} & -\theta\mathcal{K}\mathcal{C} & \Theta \end{bmatrix} \end{aligned}$$

where the decision parameters include a positive definite matrix $\mathcal{P}$, controller gain matrices K_{ii}, and a positive scalar θ.

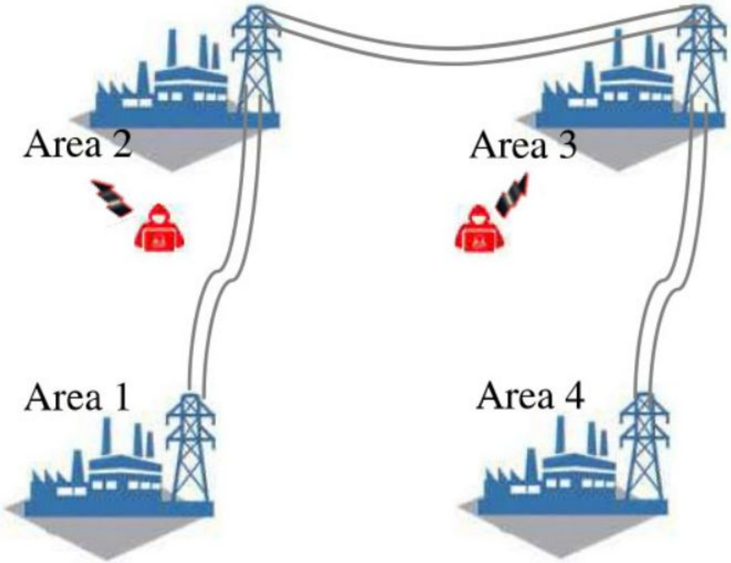


Fig. 3. Four area power system under attacks.

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems

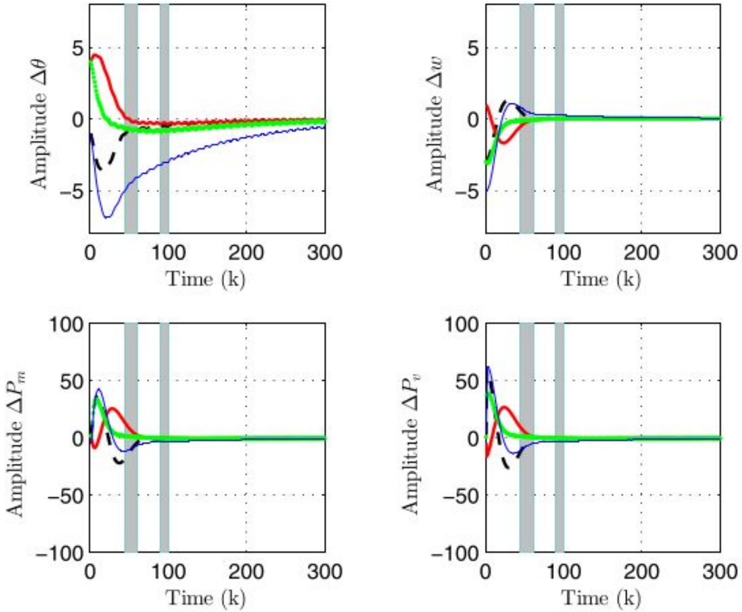


Fig. 4. Responses of the controlled power system under DoS attacks: (a) frequency deviation $\Delta\theta$; (b) tie-lie active power deviation Δw; (c) generator mechanical output deviation ΔP_m; and (d) valve position deviation ΔP_v, where the gray rectangles depict the intervals occurred attacks.

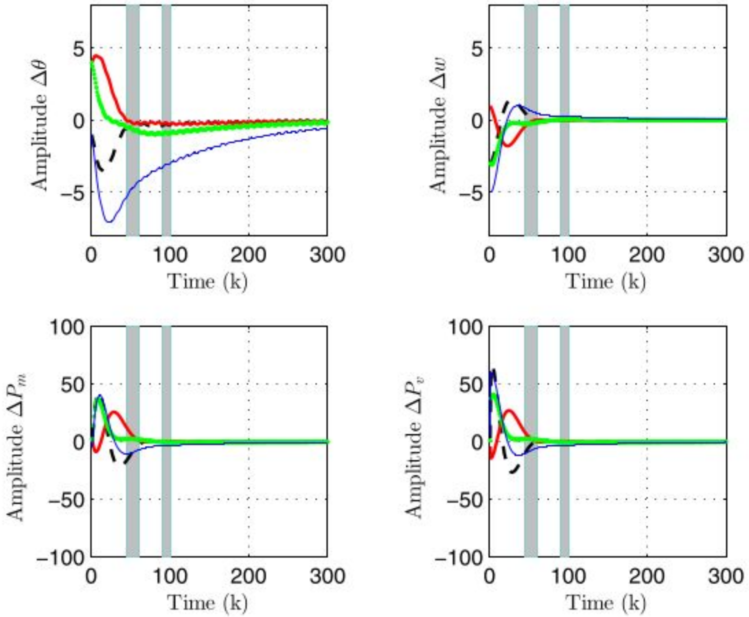


Fig. 5. Responses of the controlled power system with compensation $\eta_{i,k}$ under deception attacks.

- **Fig. 4 and Fig.5:** The presented secure control strategies based on passive defense or active compensation perform well and preserve satisfactory stable behavior of the controlled power system.

SEOULTECH
SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

V. TWO TYPICAL APPLICATION SCENARIOS OF SECURE STATE ESTIMATION AND CONTROL

B. Security Control of Wide-Area Power Systems

- However, in the case of deception attacks, it is observed from Fig. 6 that the system performance without attack compensation is seriously degraded, and the degraded performance cannot be easily recovered even if attacks disappear. This further confirms that active compensation plays a vital role in maintaining system stability and safety.

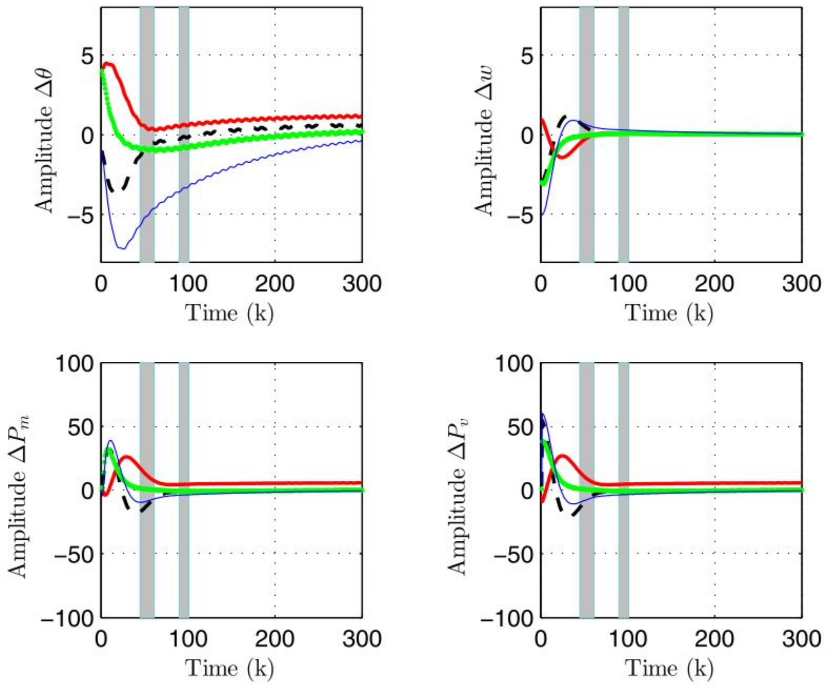


Fig. 6. Responses of the controlled power system without compensation $\eta_{i,k}$ under deception attacks.

VI. CONCLUSION AND CHALLENGING ISSUES

- An overview of secure state estimation and control has been carried out for CPSs of differential dynamical models.
- Water distribution systems and wide-area power systems have been exemplified to enable an elementary analysis framework for securing modern infrastructure.

Further research points:

1) Efficient Location and Isolation Mechanisms of Attacks Across Cyber and Physical Domains: Any corrupted data packet can be propagated over communication topology and affect the dynamical behavior of the whole physical system

2) Complicated Time Series Analysis Subject to Simultaneous Cyberattacks and Communication Scheduling and Network-Induced Phenomena: The limited cyber resources of practical CPSs are required to be properly scheduled.

3) Scalable Secure State Estimation and Control Solutions: The scale or structure of a practical CPS could suffer from connection changes due to plug-and-play components. centralized analysis and design approach necessitates the global information of the CPS.

4) Data-Driven Secure State Estimation and Control: Cyber resources in CPSs pose inherent challenges to model physical systems. Data-driven state estimation and control approaches offer a great potential.

5) Artificial Intelligence (AI)-Based Secure State: Estimation and Control Approaches:. When CPSs encounter sophisticated cyberattacks, the developed secure estimation and detection algorithms should possess certain intellectualization.