Supplementary File

RUI TAN, Advanced Digital Sciences Center, Illinois at Singapore
VARUN BADRINATH KRISHNA, University of Illinois at Urbana-Champaign
DAVID K. Y. YAU, Advanced Digital Sciences Center, Illinois at Singapore; Singapore University of Technology and Design
ZBIGNIEW KALBARCZYK, University of Illinois at Urbana-Champaign

This document includes the supplemental materials for the paper titled "Integrity Attacks on Real-Time Pricing in Electric Power Grids."

APPENDIX

A. SUMMARY OF NOTATION

Table S-I. Summary of Notation

	Definition	Unit		Definition	Unit
T	pricing period	hour	k	index of pricing period	n/a
λ_k	true price	\$/MWh	λ'_k	compromised price	\$/MWh
λ^*_k	clearing price	\$/MWh	b_k	baseline demand	MW
w	price-responsive demand	MW	d	total demand	MW
D	a constant in CEO model	MW	ϵ	price elasticity	n/a
s	scheduled total supply	MW	p	linear supply slope	MW/(\$/MWh)
h	marginal demand-supply ratio	n/a	q	linear supply intercept	MW
e_k	generation scheduling error	MW	η	price stabilization gain	n/a
λ_o	stabilization operating point	\$/MWh	C	all consumers	n/a
C'	consumers under attack	n/a	S	all suppliers	n/a
S'	suppliers under attack	n/a	ρ	$\simeq \lvert C'\rvert/\lvert C\rvert$ or $\lvert S'\rvert/\lvert S\rvert$	n/a
γ	price scaling factor	n/a	τ	time delay for price	T
F_m	branch power flow	MW	ω	social welfare	\$/hour

Note: We omit the physical unit of a quantity in the paper if it has been specified in this table.

B. STABILITY OF DIRECT FEEDBACK APPROACH

B.1. An Analysis

PROPOSITION B.1. *When the total supply is given by $s(\lambda_k) = p \cdot \lambda_k + q$ and the total demand is given by $d(k, \lambda_k) = b_k + D \cdot \lambda_k^{\epsilon}$, where $\epsilon \in (-1, 0)$ and b_k is a non-negative constant b, the system $\lambda_k = s^{-1}(d(k-1, \lambda_{k-1}))$ is not globally stable.*

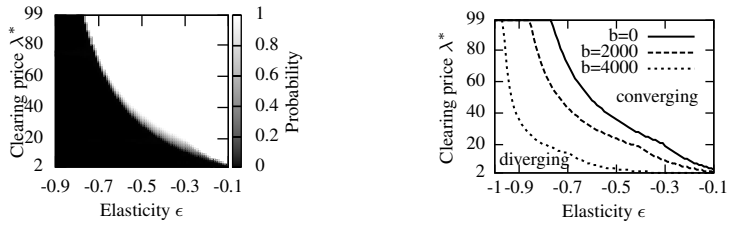
PROOF. From [Roozbehani et al. 2012], the Market's Maximal Relative Price Elasticity is $\theta^*(l) = \frac{-\epsilon D}{p} \sup_{\lambda>0} f(\lambda, l)$, where $f(\lambda, l) = \lambda^{\epsilon-1} \left(\frac{p\lambda+q}{D\lambda^{\epsilon}+b}\right)^l$. From Corollary 3 in [Roozbehani et al. 2012], the system is not globally stable if $\forall l \geq 0$, $\theta^*(l) \geq 1$. We now examine the value of $\theta^*(l)$:

Case 1. If $l = 0$, $\theta^*(0) = \frac{-\epsilon D}{p} \sup_{\lambda>0} \lambda^{\epsilon-1} = +\infty$.

Case 2. If $l > 0$ and $b = 0$,

$$f(\lambda, l) = \frac{1}{D^l} \left(p\lambda^{\frac{(1-\epsilon)(l-1)}{l}} + q\lambda^{\frac{\epsilon(1-l)-1}{l}}\right)^l.$$

For $0 < l \leq 1$, $\lim_{\lambda\to 0^+} f(\lambda, l) = +\infty$; for $l > 1$, $\lim_{\lambda\to+\infty} f(\lambda, l) = +\infty$. Hence, $\forall l > 0$, $\theta^*(l) = +\infty$.



(a) Map of convergence probability ($b = 0$).

(b) Stability boundary under various settings of b.

Fig. S-1. Stability of direct feedback approach under the linear supply and CEO demand models.

Case 3. If $l > 0$ and $b > 0$,

$$\lim_{\lambda \to 0^+} f(\lambda, l) \overset{z=1/\lambda}{=} \left(\frac{q}{D}\right)^l \lim_{z \to +\infty} z^{1-\epsilon(1-l)}.$$

For $l \in (0, 1 - 1/\epsilon)$, the above limit is positive infinity and hence $\theta^*(l) = +\infty$.

$$\lim_{\lambda \to +\infty} f(\lambda, l) = \frac{1}{b^l} \lim_{\lambda \to +\infty} \left(p\lambda^{\frac{\epsilon-1}{l}+1} + q\lambda^{\frac{\epsilon-1}{l}}\right)^l.$$

For $l \in (1 - \epsilon, +\infty)$, the above limit is positive infinity and hence $\theta^*(l) = +\infty$. As $\epsilon \in (-1, 0)$, $(0, 1 - 1/\epsilon) \cup (1 - \epsilon, +\infty) = (0, +\infty)$. Hence, $\forall l > 0$, $\theta^*(l) = +\infty$.

As a result, $\forall l \geq 0$, $\theta^*(l) = +\infty$ and the system is not globally stable. □

B.2. Numerical Experiments

As the direct feedback approach is not globally stable, its convergence highly depends on the system state. If b_k is time-varying, it can push the system to a state that eventually leads to divergence. A few realistic constraints may affect the system stability. For instance, even if the system is not globally stable, the system may converge when the initial price is within the allowed range $[\lambda_{\min}, \lambda_{\max}]$. Moreover, if a tentative price is out of the range $[\lambda_{\min}, \lambda_{\max}]$, it will be rounded to $\lambda_{\min}$ or $\lambda_{\max}$. Hence, we conduct numerical experiments that account for these realistic constraints for better understanding. We focus on the case where b_k is constant over time, i.e., $b_k = b$. We extensively evaluate the convergence of the direct feedback approach under a wide range of settings for D, ϵ, and b. Specifically, we run a large number of time-domain simulations with different settings for D, ϵ, and b. In each single time-domain simulation, the settings for D, ϵ, and b are fixed. The settings of the supply model are $p = 152$ and $q = 4503$, which are obtained in Fig. 1 in the paper. Given any settings for ϵ and b, the setting for D needs to ensure that the resulting clearing price λ^* is within $[\lambda_{\min}, \lambda_{\max}]$. For ease of evaluation, instead of setting D directly, we set λ^* to be a value within $[\lambda_{\min}, \lambda_{\max}]$ and calculate the corresponding D by solving $s(\lambda^*) = d(\lambda^*)$. The solution is $D = \frac{p\lambda^* + q - b}{\lambda^{*\epsilon}}$, where $b \in [0, p\lambda_{\min} + q)$ to ensure $D > 0$ for any valid λ^*. Fig. S-1(a) shows a map of the probability that the system is converging when $b = 0$. To calculate the probability, the initial price sweeps the range $[\lambda_{\min}, \lambda_{\max}]$ and the probability is calculated as the fraction of the initial prices that lead to system convergence. Fig. S-1(a) shows that the probability is mostly either 0 or 1 and the transition region with the probability within $(0, 1)$ is sharp. Fig. S-1(b) plots the boundaries between the converging and diverging regions under various settings of b, where its valid range is $[0, 4503)$. For instance, when $b = 4000$, the system can be diverging if $\epsilon = -0.8$ and $\lambda^* < 20$. For the data shown in Fig. S-1, about 20% of the prices are lower than 20. Therefore, the direct feedback approach can be unstable with significant probabilities.

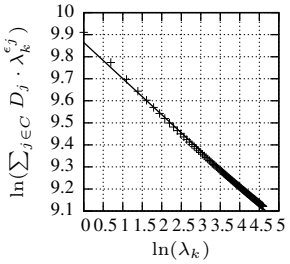


Fig. S-2. Linear fitting of aggregated demand.

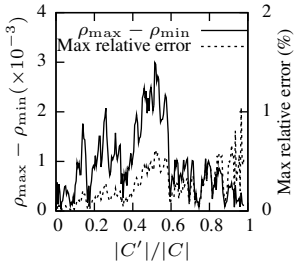


Fig. S-3. Constancy of ρ and error of Eq. (S2).

C. IMPACT OF INACCURACY IN ESTIMATING $\dot{W}(\lambda_O)$

As the price-dependent demand model $w(\cdot)$ is unknown to the ISO, we derive an upper bound for the error in estimating $\dot{w}(\lambda_o)$, to ensure the stability of the algorithm in Proposition 4.1. Let $\widetilde{\dot{w}(\lambda_o)}$ denote the estimated $\dot{w}(\lambda_o)$, and $E_w = \frac{\dot{w}(\lambda_o) - \widetilde{\dot{w}(\lambda_o)}}{\dot{w}(\lambda_o)}$ denote the relative estimation error. The stability condition $0 < \eta < 1$ can be rewritten as $0 < \frac{2\eta}{\dot{s}(\lambda_o) - \dot{w}(\lambda_o)} < \frac{2}{\dot{s}(\lambda_o) - \dot{w}(\lambda_o)}$. As long as $0 < \frac{2\eta}{\dot{s}(\lambda_o) - \widetilde{\dot{w}(\lambda_o)}} < \frac{2}{\dot{s}(\lambda_o) - \dot{w}(\lambda_o)}$, the system is stable. This condition can be derived as $E_w < (1-\eta)\left(1 - \frac{\dot{s}(\lambda_o)}{\dot{w}(\lambda_o)}\right)$. As $1 - \frac{\dot{s}(\lambda_o)}{\dot{w}(\lambda_o)} > 1$, $E_w < (1-\eta)$ is a sufficient condition for stability.

We now discuss the impact of inaccurate $\widetilde{\dot{w}(\lambda_o)}$ on the security analysis results in Section 5. From the definition of E_w, we have $\widetilde{\dot{w}(\lambda_o)} = (1 - E_w)\dot{w}(\lambda_o)$. Note that $E_w < 1$ since $\widetilde{\dot{w}(\lambda_o)} > 0$. By replacing h with $|1 - E_w| \cdot h$ in Proposition 5.6, we have a new result in the presence of the estimation error E_w. From the proofs of Propositions 5.7, 5.8, and 5.9, they are independent of h. Therefore, these propositions still hold in the presence of estimation errors.

D. PROPERTIES OF CEO DEMAND MODEL

Assume $w_j(\lambda_k) = D_j \cdot \lambda_k^{\epsilon_j}$ and hence $w(\lambda_k) = \sum_{j\in C} D_j \cdot \lambda_k^{\epsilon_j}$. The hypothesis that $w(\lambda_k)$ follows $w(\lambda_k) = D \cdot \lambda_k^{\epsilon}$ is equivalent to $\ln D + \epsilon \cdot \ln \lambda_k = \ln\left(\sum_{j\in C} D_j \cdot \lambda_k^{\epsilon_j}\right)$. We now evaluate this linear relationship by numerical study. We simulate 20,000 consumers with uniformly distributed parameters $D_j \sim \mathcal{U}(0.2, 1.8)$ and $e_j \sim \mathcal{U}(-0.4, 0)$. Fig. S-2 plots $\ln\left(\sum_{j\in C} D_j \cdot \lambda_k^{\epsilon_j}\right)$ versus $\ln(\lambda_k)$ and the linear fitting, where the Pearson correlation between them is -0.9987. Therefore, $w(\lambda_k)$ well conforms to the CEO model. When we vary the number of consumers from 1,000 to 100,000, the Pearson correlation keeps below -0.998. Hence, the linear relationship well scales with the number of consumers. From the Y-intercept of the linear fitting (i.e., $\ln(D)$) shown in Fig. S-2, the estimated D deviates only 4.5% from $\sum_{j\in C} D_j$. From the slope of the linear fitting, the estimated ϵ is -0.164, while the average value of ϵ_j is -0.201. Two important observations include: (i) the CEO model is a nearly aggregable model, and (ii) the D highly depends on the number of customers while the ϵ does not.

We also use this numerical example to evaluate the constancy of ρ defined by

$$\rho = \frac{\sum_{j\in C'} w_j(\lambda'_k)}{\sum_{j\in C} w_j(\lambda'_k)} = \frac{\sum_{j\in C'} w_j(\lambda'_k)}{w(\lambda'_k)} \tag{S1}$$

in Section 5.1.1 and the approximation accuracy of the following equation in Section 5.1.1:

$$\sum_{j\in C\setminus C'} w_j(\lambda_k) \simeq (1-\rho)\sum_{j\in C} w_j(\lambda_k) = (1-\rho)w(\lambda_k). \quad \text{(S2)}$$

We randomly choose a subset C' and calculate ρ using Eq. (S1) by iterating λ'_k from 1 to 100. The solid curve in Fig. S-3 is the difference between the maximum and minimum of ρ. We can see that the variation of ρ is smaller than 0.003. Note that ρ is centered at $|C'|/|C|$. For each λ'_k and the associated ρ, we calculate the range of the relative approximation error of Eq. (S2) by iterating λ_k from 1 to 100. The dashed curve in Fig. S-3 plots the maximum relative error, which is generally below 1%.

We have also run numerical experiments when D_j and ϵ_j are drawn from the normal and gamma distributions. We obtained similar results, which, however, are omitted in this paper due to limited space.

E. PROOF OF PROPOSITION 4.1

PROOF. By denoting $a = \frac{2\eta}{\dot{s}(\lambda_o)-\dot{w}(\lambda_o)}$ and applying the z-transform to the RTP algorithm, we can derive $\Lambda(z) = \frac{a}{1-z}\cdot E(z)$, where $\Lambda(z)$ and $E(z)$ are the z-transforms of λ_k and e_k. According to Fig. 3, we have $G_c(z) = \frac{\Lambda(z)}{0-H(z)E(z)} = \frac{a}{1-z^{-1}}$. The closed-loop transfer function, denoted by $T_c(z)$, is $T_c(z) = \frac{G_c(z)G_p(z)}{1+G_c(z)G_p(z)H(z)} = \frac{2\eta z}{z-1+2\eta}$. The closed-loop system has a single pole (i.e., the root of the denominator of $T_c(z)$) at $z = 1-2\eta$. As $\eta \in (0,1)$, this pole is within the unit circle centered at the origin in the z-plane. Therefore, the system is stable. Moreover, as $T_c(z)|_{z=1} = 1$, the controlled variable e must converge to zero if the disturbance b_k is a constant. □

F. PROOFS FOR SECTION 5

F.1. Proof of Proposition 5.6

PROOF. As $\dot{w}(\cdot)$ is decomposable, $G_w(z) = \rho\gamma\mu\dot{w}(\lambda_o) + (1-\rho)\dot{w}(\lambda_o)$. Thus, $G_p(z) = G_s(z) - G_w(z) = \dot{s}(\lambda_o) - \rho\gamma\mu\dot{w}(\lambda_o) - (1-\rho)\dot{w}(\lambda_o)$. The closed-loop transfer function [Ogata 1995] under the attack is $T_c(z) = \frac{G_c(z)G_p(z)}{1+G_c(z)G_p(z)H(z)} = \frac{2\eta(1+\rho\gamma\mu h+h-\rho h)z}{P(z)}$, where the *system characteristic function* $P(z) = (h+1)(z-1) + 2\eta(1+\rho\gamma\mu h + h - \rho h)$. If all the poles of $T_c(z)$ (i.e., roots of $P(z)$) are within the unit circle centered at the origin of the z-plane, the system is stable [Ogata 1995]. If $\eta < \bar{\eta}$, the pole is within the circle. As $\eta \in (0,1)$, η takes the minimum of 1 and $\bar{\eta}$. □

F.2. Proof of Proposition 5.7

PROOF. When $\gamma\mu \in (0,1]$, $\bar{\eta} \geq 1$. From Proposition 5.6, if $0 < \eta < 1$, the system is stable regardless of h. When $\gamma\mu > 1$, $\bar{\eta}$ is a bounded decreasing function of h. Its infimum $\inf_{h>0}\bar{\eta} = \lim_{h\to+\infty}\bar{\eta} = \frac{1}{1+\rho(\gamma\mu-1)}$. Therefore, if $0 < \eta < \inf_{h>0}\bar{\eta}$, the system is stable regardless of h. □

F.3. Proof of Proposition 5.8

PROOF. In the Jury test, the following four conditions are necessary for stability: (i) $(h+1) > 0$, (ii) $P(z)|_{z=1} = 2\eta(h+1) > 0$, (iii) $(-1)^{\tau+1}\cdot P(z)|_{z=-1} = 2(h+1) - 2\eta(1+h-\rho h) + 2\eta\rho h(-1)^{\tau+1} > 0$, and (iv) $2\eta\rho h < (h+1)$. It is easy to verify that the first three inequalities always hold for $h > 0$, $0 < \eta < 1$, and $0 < \rho \leq 1$. Therefore, the ROS is given by the intersection of the fourth condition and conditions derived from the odd-numbered rows of the Jury stability table [Ogata 1995, p. 185]. To make the presentation concise, we remove the even-numbered auxiliary rows from the Jury

stability table. When the delay is τ, it is easy to verify that the ith ($i \in [2, \tau]$) row of the Jury stability table is $R_i^\tau = [J_{i,1}, J_{i,2}, 0, 0, \cdots, 0, J_{i,3}]$, where $J_{i,1}$, $J_{i,2}$, and $J_{i,3}$ are expressed with ρ, η, and h, and there are $(\tau - i)$ zeros between $J_{i,2}$ and $J_{i,3}$. When the delay is $\tau + 1$, it is easy to verify that the ith ($i \in [2, \tau]$) row of the Jury stability table, i.e., $R_i^{(\tau+1)}$, is given by inserting a zero in R_i^τ before $J_{i,3}$. Therefore, the stability conditions derived from the ith ($i \in [2, \tau]$) row for different delays are exactly the same, i.e., $|J_{i,1}| > |J_{i,3}|$. The last row of the Jury stability table for the system with delay $\tau + 1$ is not included in that for the system with delay τ. As a result, $\mathrm{ROS}(\rho, \tau + 1) \subseteq \mathrm{ROS}(\rho, \tau)$. □

F.4. Proof for Proposition 5.9

PROOF. Denote $u_1 = h+1$, $u_2 = 2\eta+2\eta(1-\rho)h-h-1$, $u_3 = 2\eta\rho h$, and $P(z) = u_1 z^{\tau+1} + u_2 z^\tau + u_3$, where $u_1 > 0$ and $u_3 > 0$. Express any system pole (i.e., root of $P(z) = 0$) in polar coordinates: $z = A(\cos\theta + i\sin\theta)$, where $A > 0$. $P(z) = 0$ can be rewritten as two equations: $A^\tau (u_1 A\cos(\tau+1)\theta + u_2\cos\tau\theta) = -u_3$ and $A^\tau(u_1 A\sin(\tau+1)\theta + u_2\sin\tau\theta) = 0$. Adding the squares of the two equations yields $g(A) = 0$, where $g(A) = u_1^2 A^{2\tau+2} + 2u_1u_2\cos\theta A^{2\tau+1} + u_2^2 A^{2\tau} - u_3^2$. Thus, any pole satisfies $g(A) = 0$. We can verify $g(1) > 0$ when $\rho \in (0, 0.5]$. Moreover, $\dot{g}(A) = A^{2\tau} m(A)$, where $m(A) = u_1^2(2\tau+2)A + 2u_1u_2(2\tau+1)\cos\theta + \frac{2\tau u_2^2}{A}$ is a convex function with its minimum at $A^* = \left|\frac{u_2}{u_1}\right| \sqrt{\frac{\tau}{\tau+1}}$. We can verify that $\left|\frac{u_2}{u_1}\right| < 1$ if $\rho \in (0, 0.5]$. Thus, $A^* < 1$ and the minimum of $m(A)$ for $A \geq 1$ is $m(1)$, which satisfies $m(1) \geq u_1^2(2\tau+2) - 2u_1|u_2|(2\tau+1) + 2\tau u_2^2 = 2(u_1 - |u_2|)(\tau(u_1 - |u_2|) + u_1)$. If $u_2 < 0$, $u_1 - |u_2| = 2\eta + 2\eta(1-\rho)h > 0$; if $u_2 \geq 0$, $u_1 - |u_2| = 2(1-\eta) + 2h(1-\eta(1-\rho)) > 0$. Hence, $m(A) > 0$ and $\dot{g}(A) > 0$ for $A \geq 1$. Recalling $g(1) > 0$, we have $g(A) > 0$ for $A \geq 1$. Hence, $A < 1$ for all poles and the system is stable. □

Algorithm 1 Compute $\mathrm{ROS}(\rho, \tau)$ when $\rho \in (0.5, 1]$

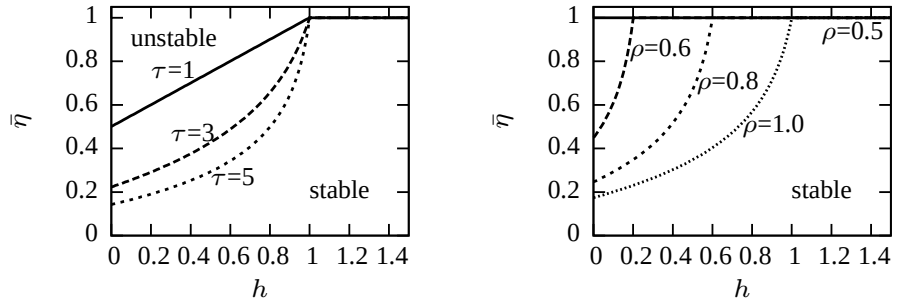
Input: ρ and τ
Output: $\lim_{h\to+\infty} \bar{\eta}(h|\rho, \tau)$
1: **if** $\tau = 1$ **then**
2: **return** $1/(2 \cdot \rho)$
3: **end if**
4: $\mathbf{X} = 1$, $\mathbf{Y} = 2\eta\rho$, $\mathbf{Z} = 2\eta\rho(1 - 2\eta(1-\rho))$
5: **for** $i = 1$ to τ **do**
6: $\mathbf{U} = \mathbf{X} \cdot \mathbf{X} - \mathbf{Y} \cdot \mathbf{Y}$, $\mathbf{V} = \mathbf{Z}$, $\mathbf{W} = (\mathbf{X} \cdot \mathbf{Z} \cdot \mathbf{Z})/\mathbf{Y}$
7: $\mathbf{X} = \mathbf{U}$, $\mathbf{Y} = \mathbf{V}$, $\mathbf{Z} = \mathbf{W}$
8: **end for**
9: $\mathbf{Q}(\eta|\rho) = \mathbf{X} \cdot \mathbf{X} - \mathbf{Y} \cdot \mathbf{Y} - \mathbf{Z}$
10: **return** minimum root of $\mathbf{Q}(\eta|\rho) = 0$ over $\eta \in (0, 1)$

Note: Line 4 to Line 9 are symbolic calculation, where the bold capitals are symbolic expressions of η and ρ.

G. INTEGRITY ATTACKS ON REAL-TIME PRICES FOR SUPPLIERS

This section studies the impact of the two integrity attacks on the real-time prices for suppliers. Although the price signals sent to the suppliers are often well protected, they may become the targets of the adversary because she needs to focus on a limited number of centralized suppliers only, in contrast to a large number of geographically distributed consumers. As this section follows the analysis approach in Section 5, we will keep the analysis procedures concise and focus on presenting the results.

Similar to Section 5.1.1, we define the following notation. Let S' denote the set of suppliers whose price signals are compromised, where $S' \subseteq S$, and $s'(\lambda_k)$ denote the total supply in the presence of an attack. Thus, $s'(\lambda_k) = \sum_{i\in S'} s_i(\lambda'_k) + \sum_{i\in S\setminus S'} s_i(\lambda_k)$.



(a) $\rho = 1$ (b) $\tau = 4$

Fig. S-4. Stability boundaries under delay attack on prices for suppliers.

The ρ is re-defined as $\rho = \frac{\sum_{i\in S'} s_i(\lambda'_k)}{\sum_{i\in S} s_i(\lambda'_k)} = \frac{\sum_{i\in S'} s_i(\lambda'_k)}{s(\lambda'_k)}$. We also make the following approximation: $\sum_{i\in S\setminus S'} s_i(\lambda_k) \simeq (1-\rho)\sum_{i\in S} s_i(\lambda_k) = (1-\rho)s(\lambda_k)$. Therefore, we have

$$s'(\lambda_k) \simeq \rho s(\lambda'_k) + (1-\rho)s(\lambda_k). \tag{S3}$$

The results in this section require that the total supply model satisfies the following property:

Definition G.1. The first derivative of the total supply model, i.e., $\dot{s}(x)$, is said to be *decomposable*, if $\dot{s}(x)|_{x=\gamma\lambda} = \dot{s}(x)|_{x=\lambda} \cdot \nu(\gamma|\Xi)$, where Ξ is the set of model parameters of $s(x)$, γ and $\nu(\gamma|\Xi)$ are independent of λ. For simplicity of exposition, we denote $\nu(\gamma|\Xi)$ as ν in the rest of this paper.

G.1. Impact of Scaling Attacks on Prices for Suppliers

The transfer function of the local linearization of Eq. (S3) with $\lambda'_k = \gamma\lambda_k$ is $G_s(z) = \rho\gamma\dot{s}(x)|_{x=\gamma\lambda_o} + (1-\rho)\dot{s}(\lambda_o)$. We have the following proposition, which is a counterpart of Proposition 5.6.

PROPOSITION 6.2. *For the scaling attacks on the prices for suppliers and the linearized system based on a fixed operating point λ_o and a decomposable $\dot{s}(\cdot)$, $\mathrm{ROS}_{\lambda_o}(\rho,\gamma) = \{(h,\eta)|0 < \eta < \min\{1,\bar{\eta}\}, \forall h > 0\}$, where $\bar{\eta} = \frac{h+1}{h+1+\rho(\gamma\nu-1)}$ and ν is defined in Definition G.1.*

PROOF. As $\dot{s}(\cdot)$ is decomposable, $G_p(z)$ can be further derived as $G_p(z) = G_s(z) - G_w(z) = \rho\gamma\nu\dot{s}(\lambda_o) + (1-\rho)\dot{s}(\lambda_o) - \dot{w}(\lambda_o)$. The system characteristic function can be derived as $P(z) = (h+1)(z-1) + 2\eta(1+\rho\gamma\nu+h-\rho)$. If $\eta < \bar{\eta}$, the sole pole of $P(z)$ is within the unit circle centered at the origin of z-plane and the system is stable. As $\eta \in (0,1)$, η takes the minimum of 1 and $\bar{\eta}$. □

The following proposition is a counterpart of Proposition 5.7.

PROPOSITION 6.3. *For the scaling attacks on the prices for suppliers and the linearized system based on a decomposable $\dot{s}(\cdot)$, when $\gamma\nu \in (0,1]$, $\mathrm{ROS}(\rho,\gamma) = \{\eta|0 < \eta < 1\}$; when $\gamma\nu > 1$, $\mathrm{ROS}(\rho,\gamma) = \{\eta|0 < \eta < \inf_{h>0}\bar{\eta}\}$, where $\inf_{h>0}\bar{\eta} = \frac{1}{1+\rho(\gamma\nu-1)}$. Note that ν is defined in Definition G.1.*

PROOF. When $\gamma\nu \in (0,1]$, $\bar{\eta} \geq 1$. From Proposition 6.2, if $0 < \eta < 1$, the system is stable regardless of h. When $\gamma\nu > 1$, $\bar{\eta}$ is a bounded increasing function of h. Its infimum $\inf_{h>0}\bar{\eta} = \lim_{h\to 0^+}\bar{\eta} = \frac{1}{1+\rho(\gamma\nu-1)}$. Therefore, if $0 < \eta < \inf_{h>0}\bar{\eta}$, the system is stable regardless of h. □

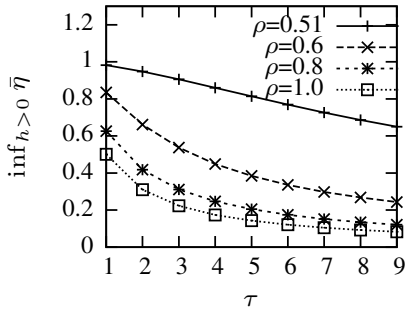


Fig. S-5. Upper bound of ROS under delay attacks on prices for suppliers.

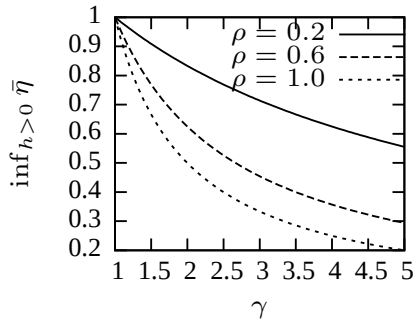
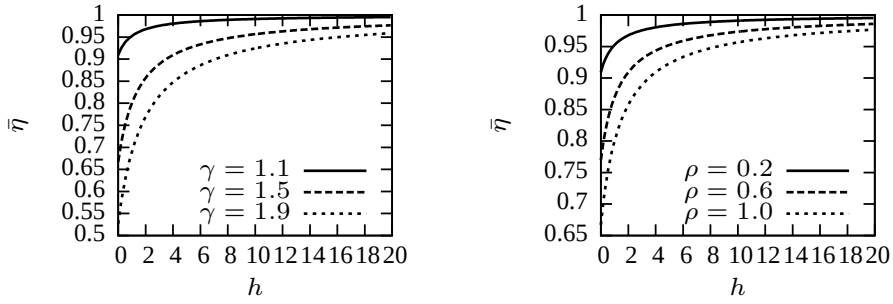


Fig. S-6. Upper bound of ROS under scaling attacks on prices for suppliers and the linear supply model.



(a) $\rho = 1$ (b) $\gamma = 1.5$

Fig. S-7. Stability boundaries under scaling attack on prices for suppliers and linear supply model (ROS_{λ_o} are the regions below the boundaries).

G.2. Impact of Delay Attacks on Prices for Suppliers

The transfer function of the local linearization of Eq. (S3) with $\lambda'_k = \lambda_{k-\tau}$ is $G_s(z) = z^{-\tau}\rho\dot{s}(\lambda_o) + (1-\rho)\dot{s}(\lambda_o)$. Therefore, $G_p(z) = G_s(z) - G_w(z) = z^{-\tau}\rho\dot{s}(\lambda_o) + (1-\rho)\dot{s}(\lambda_o) - \dot{w}(\lambda_o)$. The system characteristic function can be derived as $P(z) = (h+1)z^{\tau+1} + ((2\eta - 1)(h+1) - 2\eta\rho)z^{\tau} + 2\eta\rho$. Similar to Section 5.3, we can use the Jury test to compute the ROS_{λ_o}. Fig. S-4 plots the stability boundaries, where the ROS_{λ_o} are the regions below the boundaries. Similar to Proposition 5.9, we have the following proposition.

PROPOSITION 6.4. *For the delay attacks on the prices for suppliers and the linearized system, if* $\rho \in (0, 0.5]$, $\forall \tau \in \mathbb{Z}^+$, $\mathrm{ROS}(\rho, \tau) = \{\eta | 0 < \eta < 1\}$.

PROOF. The proof is same as the proof for Proposition 5.9 in Appendix F.4, except that: (1) u_2 and u_3 are defined as $u_2 = (2\eta - 1)(h+1) - 2\eta\rho$ and $u_3 = 2\eta\rho$; (2) if $u_2 < 0$, $u_1 - |u_2| = 2\eta(h + 1 - \rho)$, otherwise, $u_1 - |u_2| = 2(h+1)(1-\eta) + 2\eta\rho$. □

Proposition 6.4 suggests that the adversary has to compromise no less than a half of the suppliers to successfully destabilize the system. Fig. S-5 plots the upper bound of ROS versus τ when $\rho \in (0.5, 1]$. This result is close to Fig. 5, i.e., the counterpart for the delay attack on the prices for consumers.

G.3. Numerical Results based on Specific Demand and Supply Models

As a counterpart to Section 5.4, this section presents numerical results obtained under the CEO demand and linear supply models. Note that, under the linear supply model, $\dot{s}(\cdot)$ is decomposable and $\nu = 1$. The settings are same as in Section 5.4.

Under the linear supply model, by replacing $\nu = 1$ in Proposition 6.2, we have $\bar{\eta} = \frac{h+1}{h+1+\rho(\gamma-1)}$. Fig. S-7 plots the stability boundaries, where the ROS_{λ_o} are the regions below the boundaries. We can see that the ROS_{λ_o} shrinks with increased ρ, which is consistent with intuition. Moreover, ROS_{λ_o} shrinks with increased γ, which is in contrast to the observation in Section 5.4.1 for scaling attacks on prices for consumers. This is because the supply and demand models have inverse monotonicity.

Moreover, replacing $\nu = 1$ in Proposition 6.3 yields the following result. When $\gamma \in (0, 1]$, $\mathrm{ROS}(\rho, \gamma) = \{\eta | 0 < \eta < 1\}$; when $\gamma > 1$, $\mathrm{ROS}(\rho, \gamma) = \{\eta | 0 < \eta < \inf_{h>0} \bar{\eta}\}$, where $\inf_{h>0} \bar{\eta} = \frac{1}{1+\rho(\gamma-1)}$. Therefore, under the linear supply model, if the adversary scales down the price, the system remains stable. This result is in contrast to the result in Section 5.4.1, which, however, is consistent with intuition because of the inverse monotonicity of supply and demand models. Fig. S-6 plots $\lim_{h\to 0^+} \bar{\eta}$. We can see that ROS shrinks with increased γ and ρ.

H. PROOFS FOR SECTION 6

H.1. Proof for Proposition 6.1

PROOF. By following the procedure in the proof of Proposition 4.1, the system characteristic function is derived as $P(z) = (h+1)z^2 + ((2\eta - \alpha - 1)h + (2 - 2\alpha)\eta - \alpha - 1)z + (\alpha - 2\alpha\eta)h + \alpha$. The Jury test conditions are: (1) $h + 1 > |(\alpha - 2\alpha\eta)h + \alpha|$; (2) $P(1) > 0$; and (3) $P(-1) > 0$. These conditions always hold. Thus, the system is stable. □

H.2. Proof for Proposition 6.2

PROOF. By following the analysis approach in Section 5.2, the system characteristic function under the scaling attack is given by

$$P(z)=(h+1)z^2+(2\eta\rho h(\gamma\mu-1)+(2\eta-\alpha-1)h+2(1-\alpha)\eta-\alpha-1)z+\alpha((2\eta\rho(1-\gamma\mu)-2\eta+1)h+1).$$

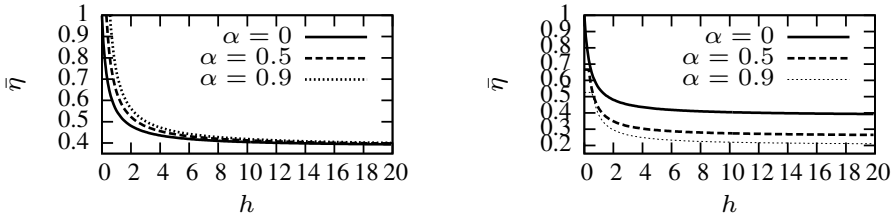
The Jury test conditions are: (1) $h + 1 > \alpha|(2\eta\rho(1 - \gamma\mu) - 2\eta + 1)h + 1|$; (2) $P(1) = 2(1 - \alpha)\eta(h + 1 + \rho h(\gamma\mu - 1)) > 0$; (3) $P(-1) > 0$, where the third condition can be derived as $\eta < \bar{\eta}$. The second condition always holds. Moreover, if $\eta < \bar{\eta}$, the first condition also holds. As $\eta \in (0, 1)$, η takes the minimum of 1 and $\bar{\eta}$. □

H.3. Proof for Proposition 6.4

PROOF. The system characteristic function is derived as $P(z) = (h + 1)z^2 + ((2\eta - 1)h + (2 - 2\alpha)\eta - 1)z - 2\alpha\eta h$. Jury test conditions are: (1) $h + 1 > 2\alpha\eta h$; (2) $P(1) = 2(1 - \alpha)(h+1)\eta > 0$; (3) $P(-1) = 2(h + \alpha\eta - \alpha\eta h - \eta h - \eta + 1) > 0$. The second condition always holds. If the third condition holds, the first condition holds. The third condition is derived as $\eta < \frac{h+1}{\alpha(h-1)+h+1}$. This upper bound for η decreases with h and its limit is $1/(1 + \alpha)$ when $h \to +\infty$. Thus, if $\eta \in (0, \frac{1}{1+\alpha})$, the system is stable. □

H.4. Proof for Proposition 6.5

PROOF. Under the scaling attack, the scheduled total supply is $\mathcal{S}_k = \alpha \cdot (b_{k-1} + w'(\lambda_{k-1})) + (1 - \alpha) \cdot s(\lambda_k)$, where $w'(\lambda_{k-1})$ is the total price-responsive demand in the presence of an attack. The $G_p(z)$ and $P(z)$ can be derived as $G_p(z) = (\alpha z^{-1} - 1)(\rho\gamma\mu\dot{w}(\lambda_o)+(1-\rho)\dot{w}(\lambda_o))+(1-\alpha)s$ and $P(z) = (h+1)z^2+(2\eta h\mu\rho\gamma-2\eta h\rho+2\eta h-h-2\alpha\eta+2\eta-1)z-2\alpha\eta h(\mu\rho\gamma-\rho+1)$. The Jury test conditions are: (1) $h+1 > 2\alpha\eta h|(\mu\gamma-1)\rho+1|$; (2) $P(1) = 2(1 - \alpha)\eta(h\mu\rho\gamma - h\rho + h + 1) > 0$; (3) $P(-1) > 0$. The third condition can be derived as $\eta < \bar{\eta}$. The second condition always holds. If the third condition holds, the first condition holds. From Proposition 6.4, η takes the minimum of $\frac{1}{1+\alpha}$ and $\bar{\eta}$. □



(a) Case 1: Consumers fully handle generation scheduling errors

(b) Case 2: Suppliers fully handle generation scheduling errors

Fig. S-8. Stability boundaries under scaling attack on prices for consumers and CEO demand model ($\epsilon = -0.8$, $\rho = 1$, $\gamma = 0.3$, ROS_{λ_o} are the regions below the boundaries).

I. NUMERICAL RESULTS FOR SECTION 6

As a counterpart to Section 5.4, this section presents numerical results obtained under the CEO demand and linear supply models. The settings are the same as in Section 5.4.

When the consumers fully handle the generation scheduling errors, Fig. S-8(a) plots the stability boundaries under the scaling attacks and different settings for α. From the figure, we can see that the ROS_{λ_o} expands with α. This is consistent with the intuition that the system becomes more resilient when the suppliers are more price-inelastic because of a larger α.

When the suppliers fully handle the generation scheduling errors, Fig. S-8(b) plots the stability boundaries under the scaling attacks and different settings for α. From the figure, we can see that the ROS_{λ_o} shrinks with α. This result is contrary to Fig. S-8(a) for Case 1. It is because in Case 2, the stateful supply model is a composite of the stateless supply and demand models. Therefore, a larger α increases the price-elasticity of supply, thereby making the system less resilient.

J. LMP UNDER GENERAL COST FUNCTION AND PRICE-RESPONSIVE DEMAND

This section describes how the LMPs are computed, where the demand is price-responsive. Let N and M denote the numbers of buses and branches in the transmission system, respectively. Let λ_n^B, d_n^B, b_n^B, s_n^B, $v_n^B(\cdot)$, and $c_n^B(\cdot)$ denote the LMP, demand, baseline demand, supply, value function, and cost function, respectively, at the nth bus. We assume that the demand and supply are determined by the value and cost functions as follows: $d_n^B = (\dot{v}_n^B)^{-1}(\lambda_n^B) + b_n^B$ and $s_n^B = (\dot{c}_n^B)^{-1}(\lambda_n^B)$ [Roozbehani et al. 2012]. We extend an LMP formulation based on the dc optimal power flow (DCOPF) in [Li and Bo 2007] to address a general cost function and price-responsive demand:

$$\text{minimize} \quad \omega = \sum\nolimits_{n=1}^{N} v_n^B(d_n^B - b_n^B) - c_n^B(s_n^B), \tag{S4}$$

$$\text{subject to} \quad \sum\nolimits_{n=1}^{N} \delta_n \cdot s_n^B - \sum\nolimits_{n=1}^{N} \delta_n \cdot d_n^B + \sum\nolimits_{m=1}^{M} (F_m/V)^2 R_m = 0, \tag{S5}$$

$$\delta_n = 1 - \sum\nolimits_{m=1}^{M} \frac{2R_m F_m H_{mn}}{V^2}, \quad \forall n \in [1, N], \tag{S6}$$

$$F_m = \sum\nolimits_{n=1}^{N} H_{mn}(s_n^B - d_n^B), \quad \forall m \in [1, M], \tag{S7}$$

$$-L_m \le F_m \le L_m, \quad \forall m \in [1, M], \tag{S8}$$

$$s_n^{\min} \le s_n \le s_n^{\max}, \quad \forall n \in [1, N], \tag{S9}$$

where ω in Eq. (S4) is the *social welfare*; Eq. (S5) is the power balance equation; δ_n in Eq. (S6) is the *delivery factor* for the nth bus; F_m in Eq. (S7) is the power flow over the mth branch; Eq. (S8) is the transmission line capacity constraint; Eq. (S9) is the generation capacity constraint; V is the voltage magnitude; H_{mn} is the *power trans-*

fer distribution factor to the mth branch from the nth bus; L_m, R_m, and $(F_m/V)^2 R_m$ are the capacity, resistance, and power loss of the mth branch, respectively. Note that $\{H_{mn} | n \in [1, N], m \in [1, M]\}$ can be calculated from the reactances of the branches and the incidence matrix (i.e., topology) of the transmission system, using various tools such as MATPOWER.

REFERENCES

Fangxing Li and Rui Bo. 2007. DCOPF-based LMP Simulation: Algorithm, Comparison with ACOPF, and Sensitivity. *IEEE Transactions on Power Systems* 22, 4 (2007), 1475–1485.

Katsuhiko Ogata. 1995. *Discrete-Time Control Systems* (2 ed.). Prentice-Hall, Englewood Cliffs, New Jersey.

Mardavij Roozbehani, Munther A. Dahleh, and Sanjoy K. Mitter. 2012. Volatility of Power Grids under Real-Time Pricing. *IEEE Transactions on Power Systems* 27, 4 (2012), 1926–1940.