Letters

Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution

Xuan Liu, *Member, IEEE*, Zuyi Li, *Senior Member, IEEE*, Zhikang Shuai, *Member, IEEE*, and Yunfeng Wen

***Abstract*—Today's smart power networks are exposed to an increasing number of cyber-attack events due to the highly integration of information techniques. It was revealed that an attacker can significantly increase the operation cost of a power system by launching undetectable false data injection attacks. However, the attack vector is determined by solving a bi-level linear programing (LP) problem, which is intractable for large systems. In this letter, we present a simple approach to determine an effective attack vector that can cause a significant increase in the operation cost. This is achieved by solving one LP. The simulation results on the IEEE testing systems verify the effectiveness of the proposed model and reveal that large-scale power systems are under high risk of cyber-attacks.**

***Index Terms*—Cyber-attacks, false data injection attacks, security constrained economic dispatch, power systems.**

NOMENCLATURE

$\boldsymbol{c_g}$, $\boldsymbol{c_d}$	Generation cost/load shedding cost vector.
$\boldsymbol{D}$	Load vector.
$\Delta\boldsymbol{D}$	Injected false data vector into $\boldsymbol{D}$.
$\boldsymbol{F}$	Calculated line flow vector with false data.
$\boldsymbol{f_{max}}$	Line flow limit vector.
F_l	Calculated power flow of line l.
f_l, f_l^{max}	True power flow/flow limit of line l.
$\boldsymbol{P}$	Generator output power vector.
$\boldsymbol{J}$	Load shedding vector.
$\boldsymbol{S}, \boldsymbol{S_l}$	Shifter factor matrix/ l-th row of $\boldsymbol{S}$.
$\boldsymbol{P_{min}}, \boldsymbol{P_{max}}$	Lower and upper bounds for generators' output.
$\boldsymbol{U}, \boldsymbol{V}$	Bus-generator/bus-load incidence matrices.
τ	Given maximum percentage of change for load measurement attack.
α	Threshold value for lines whose flows are closed to the limits.

Manuscript received March 28, 2016; revised June 20, 2016, August 17, 2016, and October 6, 2016; accepted October 18, 2016. Date of publication November 2, 2016; date of current version February 16, 2017. Paper no. PESL-00056-2016.

X. Liu and Z. Li are with the Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: xliu108@hawk.iit.edu; lizu@iit.edu).

Z. Shuai is with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: shuaizhikang-001@163.com).

Y. Wen is with the State Key Laboratory of Power Transmission Equipment and System Security and New Technology, Chongqing University, Chongqing 400044, China (e-mail: wenyunfeng@cqu.edu.cn).

Digital Object Identifier 10.1109/TSG.2016.2623983

I. PROBLEM FORMULATION

IN THE operation of power systems, the generators will be redispatched every 5-15 minutes to minimize the operation cost for supplying the current loads. This is achieved by solving a security constrained economic dispatch (SCED) problem. Due to the close association with communication networks, an attacker has a chance to interrupt the process of SCED by injecting false data to change the load data sent to the control center [1]–[3]. The optimal attack vector that maximizes the operation cost can be obtained by solving a bilevel linear programming (BLP) problem (1)-(9):

$$c_1 = \max_{\Delta \boldsymbol{D}} \ \boldsymbol{c_g^T P} + \boldsymbol{c_d^T J} \tag{1}$$

$$\text{subject to } \ \boldsymbol{1^T} \Delta \boldsymbol{D} = 0 \tag{2}$$

$$-\tau \boldsymbol{D} \le \Delta \boldsymbol{D} \le \tau \boldsymbol{D} \ (0 < \tau < 1) \tag{3}$$

$$\min_{\boldsymbol{P},\boldsymbol{J}} \ \boldsymbol{c_g^T P} + \boldsymbol{c_d^T J} \tag{4}$$

$$\text{subject to } \ \boldsymbol{1^T P} = \boldsymbol{1^T} (\boldsymbol{D} - \boldsymbol{J}) \tag{5}$$

$$\boldsymbol{F} = \boldsymbol{S} \cdot \boldsymbol{U} \cdot \boldsymbol{P} - \boldsymbol{S} \cdot \boldsymbol{V} \cdot (\boldsymbol{D} + \Delta \boldsymbol{D} - \boldsymbol{J}) \tag{6}$$

$$\boldsymbol{P_{min}} \le \boldsymbol{P} \le \boldsymbol{P_{max}} \tag{7}$$

$$-\boldsymbol{f_{max}} \le \boldsymbol{F} \le \boldsymbol{f_{max}} \tag{8}$$

$$\boldsymbol{0} \le \boldsymbol{J} \le \boldsymbol{D} + \Delta \boldsymbol{D} \tag{9}$$

In the upper level (1)-(3), an injected false data $\Delta\boldsymbol{D}$ vector is determined to maximize the load shedding after SCED. Constraints (2) and (3) indicate that the attacking amount is summed to zero and limited with a certain range. In the lower level (4)-(9), the operator minimizes the operation cost based on the corrupted load data $\boldsymbol{D} + \Delta\boldsymbol{D}$ considering the generator output power limits (7), transmission line flow limits (8) and load shedding limits (9).

The most popular methods to solve a bilevel optimization problem are the Karush-Kuhn-Tucker (KKT) based approach and dual based approach. For the KKT based approach, additional binary variables will be introduced to form the so called big-M constraints, which will slow down the algorithm greatly. For the duality based method, the bilinear terms of dual variables and corresponding primal variables make the whole problem hard to solve. Although there are several heuristic or approximation algorithms, such as Mountain Climbing (MC), to solve a bilevel optimization problem, it is

still time-consuming to get the solution for a large-size system. Please refer to [5] for detailed descriptions of the MC algorithm.

Does this mean that large-scales power systems have a natural immunity to these cyber-attacks due to the difficulty of constructing an effective attack vector?

Does an attacker have a fast approach to construct an effective attack vector that can significantly increase the operation cost of a power system?

The answer to these questions is very helpful for the operator to understand the vulnerability of power systems to cyber-attacks.

When false data $\boldsymbol{\Delta D}$ is injected, it was proved in [4] that the true line flow f_l and the calculated line flow F_l satisfy

$$F_l = f_l + \boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \boldsymbol{\Delta D} \quad \forall l \tag{10}$$

At the economic operating point, suppose the flows of the lines in set Ω are closed to their flow limits. That is,

$$|f_l| \geq \alpha f_l^{max} \ (0 < \alpha < 1) \quad \forall l \in \Omega \tag{11}$$

If an attacker injects false data $\boldsymbol{\Delta D}$ to make

$$\begin{cases} \boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \boldsymbol{\Delta D} > (1-\alpha) f_l^{max} & f_l \geq 0 \\ \boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \boldsymbol{\Delta D} > -(1-\alpha) f_l^{max} & f_l < 0 \end{cases} \quad \forall l \in \Omega \tag{12}$$

Then, constraint (13) holds,

$$|f_l + \boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \boldsymbol{\Delta D}| > f_l^{max} \quad \forall l \in \Omega \tag{13}$$

Constraint (13) indicates that the original optimal operating point is not feasible any more after the false data $\boldsymbol{\Delta D}$ is injected. As a result, the operation cost will be increased.

Thus, one strategy to increase the operation cost is to maximize the loading levels of the lines in set Ω by injecting false data. The optimization problem of determining the optimal false data $\boldsymbol{\Delta D}$ can be formulated as (14):

$$\begin{aligned} &\max_{\Delta \boldsymbol{D}} \sum_{l \in \Omega} \delta_l \frac{-\boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \Delta \boldsymbol{D}}{f_l^{max}} \\ &\text{subject to} \quad \text{Constraints (2)–(3)} \end{aligned} \tag{14}$$

It should be clarified that (14) is not mathematically equivalent to the bilevel model (1)-(9). The goal of (14) is only to provide an alternative method to construct an effective attack vector that can cause significant increase in the operation cost.

The objective is to maximize the loading levels of the lines in set Ω. Where $\delta_l = 1$, if the flow of line l is positive; $\delta_l = -1$ otherwise. The term $-\boldsymbol{S_l} \cdot \boldsymbol{V} \cdot \Delta \boldsymbol{D}$ represents the incremental power flow of line l due to the injected false data $\Delta \boldsymbol{D}$. Once $\boldsymbol{\Delta D}$ is determined, it will be introduced into (5)-(9) to calculate the operation cost.

To validate the effectiveness of the proposed method, the operation cost c_1 is compared with that of the case without false data $\Delta \boldsymbol{D}$, which is determined by solving the optimization problem (15):

$$\begin{aligned} &\min_{\boldsymbol{P}, \boldsymbol{J}} \boldsymbol{c_g^T P} + \boldsymbol{c_d^T J} \\ &\text{subject to} \quad \text{Constraints (5)–(9)} \end{aligned} \tag{15}$$

TABLE I
COMPARISONS OF OPERATION COSTS AND RUN TIMES FOR THE SIMPLE AND BILEVEL MODELS

Power Grid	Operation Cost($/h)		Run times(s)	
	Bilevel	Simple	Bilevel	Simple
IEEE 14-bus	9482.0(14.2%)	9400.6(13.3%)	0.19	0.001
IEEE 30-bus	5806.2(12.1%)	5659.8(9.2%)	0.41	0.002

TABLE II
PERFORMANCE COMPARISONS FOR THE SIMPLE MODEL AND MC ALGORITHM

Power Grid	MC		Simple Model	
	$c(10^6\$/h)$	$t(s)$	$c(10^6\$/h)$	$t(s)$
IEEE 2383	2.75(2.56)	(12.98)	2.67	0.002
IEEE 2736	1.74(1.57)	(10.74)	1.73	0.002
IEEE 3120	2.75(2.66)	(20.91)	2.74	0.007
IEEE 6240	5.55(5.35)	(116.23)	5.52	0.009

*c: operation cost; t: run times in one iteration

We can see that the optimization attack vector can be determined by solving one LP (14) with only one equality constraint. Thus, the run time will be reduced greatly compared to the KKT or other heuristic algorithms.

II. CASE STUDY

In this section, we test the proposed model using the IEEE 14-bus, IEEE 30-bus, IEEE 2383-bus, IEEE 2736-bus, IEEE 3120-bus and two-area IEEE 3120-bus(IEEE 6240-bus) systems. The data for the system is available at http://motor.ece.iit.edu/data/SCEDA_data.xlsx. Simulations are carried out on a 2.4GHz personal computer with 4GB of RAM. For the illustrative purpose, we use the simple model to represent the proposed model in this letter.

The operation costs for the 14-bus, IEEE 30-bus, IEEE 2383-bus, IEEE 2736-bus, IEEE 3120-bus and IEEE 6240-bus systems without false data are 8299.6 \$/h, 5180.6 \$/h,2.48×10^6 \$/h, 1.57×10^6 \$/h, 2.60×10^6 \$/h and 5.20×10^6 \$/h respectively. Table I compares the operation costs and run times of the bilevel and simple models for the IEEE 14-bus and IEEE 30-bus systems. The values of τ and α are set to 0.5, 0.99, respectively. The data in the parentheses represent the percentage of the incremental operation cost to the original operation cost without false data. It can be observed that the attack vector determined by the simple model can cause a significant increase in the operation cost. However, the optimal attack vector determined using the bilevel model will lead to a higher operation cost. This is because that the bilevel model can obtain the global optimal solution for the attack vector. It can be also observed that the simple model can determine an attacker vector much faster compared to the bilevel one. For example, it only takes 0.002 seconds to construct the attack vector, much less than that of the bilevel model.

Table II compares the performance of the proposed simple model with the MC algorithm, which is the most popular heuristic algorithm to solve a max-min bilevel optimization problem. The convergence tolerance for the heuristic algorithm is set to 10^{-3}. The numbers in the parentheses represent the operation costs and run times in one iteration for the

MC algorithm. It can be observed that our proposed model can determine a good attack vector that causes an equivalent increase in the operation cost compared to the MC algorithm. For example, the operation costs of the IEEE 3120-bus system under the optimal attack vector constructed by our model and the MC algorithm are 2.74×10^6 \$/h, 2.75×10^6 \$/h, which are very close. In addition, the proposed simple model provides a better attack vector that leads to a higher operation cost than the MC algorithm in one iteration. It is also verified that the simple model has a dominate advantage of run times over the MC algorithm. Consider the IEEE 6240-bus as an example. It only takes less than 0.01s to get the optimal attack vector if an attacker adopts the simple model, much less than that of the MC algorithm (116s, one iteration).

III. Conclusion

In this letter, we present a simple yet effective approach to determine an optimal attack vector that can lead to a significant increase in the operation cost. This is achieved by solving one LP. Our work highlights the vulnerability of power systems to cyber-attacks since an attacker can construct an effective attack vector in real time against large-scale power networks. In future work, we will develop corresponding countermeasures to defend these cyber-attacks.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.

[2] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[3] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016, doi: 10.1109/TPWRS.2015.2504950.

[4] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2015.2475701.

[5] H. Konno, "A cutting plane algorithm for solving bilinear programs," *Math. Program.*, vol. 11, no. 1, pp. 14–27, 1976.