Appendix: A Verifiable Framework for Cyber-Physical Attacks and Countermeasures in a Resilient Electric Power Grid

Zhigang Chu[1], Andrea Pinceti[1], Ramin Kaviani[1], Roozbeh Khodadadeh[1], Xingpeng Li[2], Jiazi Zhang[3], Karthik Saikumar[1], Mostafa Sahraei-Ardakani[4], Christopher Mosier[5], Robin Podmore[6], Kory Hedman[1], Oliver Kosut[1], and Lalitha Sankar[1]

1. Arizona State University 2. University of Houston 3. National Renewable Energy Laboratory
4. University of Utah 5. PowerData 6. IncSys

***Abstract*—This paper investigates the feasibility and physical consequences of cyber attacks against energy management systems (EMS). Within this framework, we have designed a complete simulation platform to emulate realistic EMS operations: it includes state estimation (SE), real-time contingency analysis (RTCA), and security constrained economic dispatch (SCED). This software platform allowed us to achieve two main objectives: 1) to study cyber vulnerabilities of an EMS and understand their consequences on the system, and 2) to formulate and implement countermeasures against these cyber-attacks. Our results show that the false data injection attacks against state estimation described in the literature do not easily cause base-case overflows because of the conservatism introduced by RTCA. For a successful attack, a more sophisticated model that includes all of the EMS blocks is needed; even in this scenario, only post-contingency violations can be achieved. Nonetheless, we propose several countermeasures that can detect changes due to cyber-attacks and limit their impact on the system.**

Appendix A
Observability analysis (OA) algorithm

Observability analysis determines whether the system is fully observable using topology and available measurements. Consider a single branch with reactance $X_{k,m} = 1.0p.u.$ connected between buses k and m. Assuming the voltage magnitude at each terminal to be 1.0 p.u., the first order approximation around $\theta_k^0 = \theta_m^0 = 0$ of the real power flowing through this branch can be written as:

$$P = \frac{V_k V_m}{X_{k,m}} \cos(\theta_k^0 - \theta_m^0)(\theta_k - \theta_m) = \theta_k - \theta_m \qquad (1)$$

If a tree can be formed such that each branch of this tree contains a power flow measurement, then the phase angles at all buses can be determined, i.e. the system will be fully observable. The topological method hence starts out by assigning power flow measurements to their respective branches and tries to form a spanning tree, i.e. a tree that reaches each and every bus in the system, using these branches. If this procedure is not successful, then it will yield a forest where there are several smaller size trees. In that case, the remaining measurements which are of injection type, will be used in order to merge these trees and reduce the size of the forest as described in [1]. If successful, this reduction process will result in a single tree, in which case the system will be declared as observable.

Appendix B
Weighted least-square state estimation algorithm using Givens rotation

The WLS state estimator minimizes the following objective function (weighted sum-squared error):

$$J(\mathbf{x}) = \sum_{i=1}^{n} (z_i - h_i(\mathbf{x}))^2 / R_{ii} = [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{R} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \qquad (2)$$

where $\mathbf{x}$ is the $p \times 1$ state vector, $\mathbf{z} = \mathbf{h}(\mathbf{x})$ is the $n \times 1$ measurement vector, and $\mathbf{R}$ is the covariance matrix of the measurements. The derivative of $J(x)$ with respect to $\mathbf{x}$ must vanish at the minimum:

$$\mathbf{g}(\mathbf{x}) = \frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = -\mathbf{H}^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] = 0 \qquad (3)$$

where $\mathbf{H}(\mathbf{x}) = \frac{\partial \mathbf{h}(\mathbf{x})}{\partial \mathbf{x}}$.

An iterative solution scheme can be derived by expanding $\mathbf{g}(\mathbf{x})$ into its Taylor series around the state vector at the k^{th} iteration $\mathbf{x}^k$ and neglecting the high order terms:

$$\mathbf{x}^{k+1} = \mathbf{x}^k - [\mathbf{G}(\mathbf{x}^k)]^{-1} \mathbf{g}(\mathbf{x}^k) \qquad (4)$$

where the gain matrix

$$\mathbf{G}(\mathbf{x}) = \frac{\partial \mathbf{g}(\mathbf{x})}{\partial \mathbf{x}} = \mathbf{H}^T(\mathbf{x}) \mathbf{R}^{-1} \mathbf{H}(\mathbf{x}). \qquad (5)$$

Eqs. (4) and (5) yield the normal equation

$$[\mathbf{G}(\mathbf{x}^k)] \Delta \mathbf{x}^k = \mathbf{H}^T(\mathbf{x}^k) \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x}^k)]. \qquad (6)$$

When the gain matrix $\mathbf{G}$ is singular or close to singular, it is very difficult to solve for Δx using standard normal equation (6). Orthogonal factorization can be used to solve this problem. Let

$$\mathbf{H}' = \mathbf{R}^{-\frac{1}{2}} \mathbf{H}, \qquad (7)$$

then

$$\mathbf{G} = \mathbf{H'}^T\mathbf{H'}. \tag{8}$$

An orthogonal factorization on matrix $\mathbf{H'}$ yields

$$\mathbf{H'} = \mathbf{QU}. \tag{9}$$

One way to perform orthogonal factorization is to use Givens rotation [2]. For a fixed coordinates pair (i, j) where $i > j$, The non-zero elements in the corresponding Givens rotation matrix are given by

$$GR_{kk} = 1, \forall k \neq i, j \tag{10}$$

$$GR_{kk} = c, \forall k = i, j \tag{11}$$

$$GR_{ij} = -GR_{ji} = s. \tag{12}$$

When a Givens rotation matrix multiplies another matrix from the left, only rows i and j of that matrix are affected. Thus, given a and b, c and s can be calculated using

$$\begin{bmatrix} c & -s \\ s & c \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} r \\ 0 \end{bmatrix}, \tag{13}$$

where $r = \sqrt{a^2 + b^2}$ is the length of vector $[a, b]^T$. An obvious solution would be $c = a/r$ and $s = -b/r$. Each Givens rotation matrix introduces a zero at a specific entry of $\mathbf{H'}$. Eventually the $\mathbf{Q}$ matrix is an orthogonal matrix that is the product of all the Givens rotation matrices, and the $\mathbf{U}$ matrix will become $\begin{bmatrix} \mathbf{U_1} \\ \mathbf{0} \end{bmatrix}$, where $\mathbf{U_1}$ is an upper triangular matrix. Let

$$\Delta\mathbf{z'} = \mathbf{R}^{-\frac{1}{2}}[\mathbf{z} - \mathbf{h}(\mathbf{x})]. \tag{14}$$

Substituting (7), (8), (9), and (14) into the normal equation (6) yields

$$\mathbf{U^T Q^T Q U} \Delta\mathbf{x}^k = \mathbf{U^T Q^T} \Delta\mathbf{z'}. \tag{15}$$

Since $\mathbf{Q}$ is orthogonal, multiplying both sides of (15) by $\mathbf{U}$ from the left leads to

$$\mathbf{U}\Delta\mathbf{x}^k = \mathbf{Q}^T\Delta\mathbf{z'}. \tag{16}$$

$\Delta\mathbf{x}^k$ in (16) can be efficiently solved using forward substitution method. The iteration is terminated when $\Delta\mathbf{x}^k < \epsilon$, where ϵ is the convergence tolerance. Note that the Givens rotation process involves massive amount of matrix multiplications in each iteration, and we use sparsity techniques (powered by SuiteSparse [3]) to accelerate the solving process.

Let $\hat{\mathbf{x}}$ be the estimated states. Measurements are re-calculated after the state estimation process using $\hat{\mathbf{z}} = \mathbf{h}(\hat{\mathbf{x}})$, and a χ^2-test is performed to determine if there exists any bad data. Recall the objective function of WLS state estimator (2), a χ^2-test is performed by comparing $J(\hat{\mathbf{x}})$ and the χ^2-test threshold χ^2_{th}. This threshold is determined by looking up the value from the χ^2 distribution table corresponding to the detection confidence probability P (typically 95%) with $(n-p)$ degrees of freedom. If $J(\hat{\mathbf{x}}) < \chi^2_{th}$, the measurements are determined as free of bad data and the SE block terminates. Otherwise, the measurements contain bad data, and the largest normalized residual method is used to identify and remove the bad measurement. The normalized residual is given by

$$r_i^N = \frac{|z_i - h_i(\mathbf{x})|}{\sqrt{\Omega_{ii}}}, \quad i = 1, 2, ..., n \tag{17}$$

where Ω is the covariance matrix of the residual. The measurement with the largest normalized residual is then removed from the available measurements list, and the remaining measurements are sent for OA-SE-BDD-BDE again. This process is performed until there are no bad data.

APPENDIX C
COMPLETE SCED FORMULATION

Nomenclature for SCED

Sets:

D	Loads
D(n)	Loads at bus n
N	Buses
C	Contingencies
K	Branches
K(if)	Branches that form the interface if.
KM	Base case monitored branches
KM(c)	Monitored branches under contingency c
G	Generators
G(n)	Generators located at bus n
GC	Dispatchable units that have available cost curve data.

Parameters:

T_{ED}	Look-ahead time for one period SCED
T_{SR}	Time for spinning reserve requirements
P_d	Active power of load d
St_g	Status of generator g
St_d	Status of load d
St_k	Status of branch k
P_{g0}	Initial output of generator g
P_{k0}	Initial from side active flow on branch k
NS_g	Number of cost segments of generator g
$BS_{g,i}$	Breadth of segment i of generator g
MRR_g	Energy ramp rate of generator g
SRR_g	Spinning ramp rate of generator g
$C_{g,i}$	Cost for segment i of generator g
CSR_g	Spinning reserve cost of generator g
$S_{k,\text{max}}$	Base case flow limit of branch k
$S_{kc,\text{max}}$	Contingency case flow limit of branch k
$P_{g,\text{max}}$	Maximum output of generator g
$P_{g,\text{min}}$	Minimum output of generator g
$\text{PTDF}_{n,k}$	PTDF from bus n to branch k
$\text{LODF}_{k,c}$	Line c outage distribution factor on branch k
$\text{OTDF}_{n,k,c}$	Outage transfer distribution factor from bus n to branch k when branch c is out
Rate_i	Total flow limit of interface i
RateA_k	Normal thermal limit of branch k
RateC_k	Emergency thermal limit of branch k

Variables:

p_k	Power flow on branch k
$p_{k,c}$	Power flow on branch k under contingency c
p_g	Total output of generator g
$p_{g,i}$	Output of segment i of generator g
$p_{g,c}$	Total output of generator g under contingency c
$p_{d,\text{serve}}$	Served active power of load d
$p_{d,\text{shed}}$	Shedded active power of load d

$p_{d,\text{serve},c}$ Served active power of load d under contingency c

$p_{d,\text{shed},c}$ Shedded active power of load d under contingency c

sr_g Spinning reserve provided by generator g

p_{if} Total power flow for interface if

$p_{if,c}$ Total power flow for interface if under contingency c

$s_{g,\text{LB}}$ Slack variable for lower bound of output of generator g

Penalty factors:

PF_{shed} A fixed penalty factor for $p_{d,\text{shed}}$ and $p_{d,\text{shed}.c}$

PF_{LB} A fixed penalty factor for $s_{g,\text{LB}}$

The SCED formulation is given by

Objective function:

$$\begin{aligned}\text{minimize} \quad & \sum_{g\in G}\sum_{i=1}^{NS_g} p_{g,i}C_{g,i} + \sum_{g\in G} sr_g \text{CSR}_g \\ & + \text{PF}_{\text{shed}}\Big(\sum_{d\in D} p_{d,\text{shed}} + \sum_{c\in C}\sum_{d\in D} p_{d,\text{shed},c}\Big) \\ & + \text{PF}_{\text{LB}} \sum_{g\in G} s_{g,\text{LB}} \end{aligned} \tag{18}$$

Constraints:

- Power balance equations:

Base case:

$$\sum_{g\in G} p_g = \sum_{d\in D} p_{d,\text{serve}} \tag{19}$$

Contingency case:

$$\sum_{g\in G} p_{g,c} = \sum_{d\in D} p_{d,\text{serve},c} \tag{20}$$

- Load equations:

Base case:

$$p_{d,\text{serve}} + p_{d,\text{shed}} = P_d \cdot St_d \tag{21}$$

if $Std = 0$ or $Pd \le 0$,

$$p_{d,\text{shed}} = 0 \tag{22}$$

else,

$$p_{d,\text{serve}} \ge 0 \tag{23}$$

Contingency case:

$$p_{d,\text{serve},c} + p_{d,\text{shed},c} = P_d \cdot St_d \tag{24}$$

if $Std = 0$ or $Pd \le 0$,

$$p_{d,\text{shed},c} = 0 \tag{25}$$

else,

$$p_{d,\text{serve},c} \ge 0 \tag{26}$$

- Branch flow calculation:

Base case:

$$p_k = St_k \cdot (P_{k0} + \sum_{n\in N} \text{PTDF}_{n,k} \cdot (\sum_{g\in G(n)} (p_g - P_{g0}) + \sum_{d\in D(n)} p_{d,\text{shed}})), k \in \text{KM or K}(if) \tag{27}$$

Contingency case:

if $St_k = 0$ or $k = c$,

$$p_{k,c} = 0 \tag{28}$$

else

$$p_{k,c} = P_{k,c,0} + \sum_{n\in N} \text{OTDF}_{n,k,c} \cdot (\sum_{g\in G(n)} (p_{g,c} - P_{g0}) + \sum_{d\in D(n)} p_{d,\text{shed},c}), k \in \text{KM}(c) \text{ or K}(if) \tag{29}$$

- Branch flow limit:

Base case:

$$-\text{RateA}_k \le p_k \le \text{RateA}_k \ , \ \text{k} \in \text{KM} \tag{30}$$

Contingency case:

$$-\text{RateC}_k \le p_{k,c} \le \text{RateC}_k \ , \ \text{k} \in \text{KM} \tag{31}$$

- Unit generation equations:

Base case:

If St_g == 0, then p_g = 0.

If St_g == 0, and $g \in$ GC, then p_{gi} = 0.

If St_g == 1, and $g \in$ (G-GC), then $p_g = P_{g0}$.

If St_g == 1, and $g \in$ GC and $P_{g0} \le 0$, then p_{gi} = 0.

If St_g == 0, and $g \in$ GC, then:

$$p_g = \sum_{i=1}^{NS_g} p_{g,i} \ , \ \text{g} \in \text{GD} \tag{32}$$

$$0 \le p_{g,i} \le BS_{g,i} \ , \ \text{g} \in \text{GD} \tag{33}$$

Contingency case:

If St_g ==0, then, $p_{g,c}$ = 0.

If St_g ==1 and $g \in$ (G-GC), then: $p_{g,c} = P_{g0}$.

If St_g ==1, then,

$$p_{g,c} \le P_{g,max} \tag{34}$$

$$p_{g,c} \ge P_{g,min} - s_{g,\text{LB}} \tag{35}$$

- Ramp rate limit:

Base case:

$$p_g \le \min\{P_{g0} + MRR_g.T_{ED}.P_{g,max}\} \tag{36}$$

$$p_g \ge \max\{P_{g0} - MRR_g.T_{ED}.P_{g,min}\} - s_{g,\text{LB}} \tag{37}$$

Contingency case:

$$p_{g,c} - p_g \le SRR_g.T_{SR} \tag{38}$$

$$p_{g,c} - p_g \ge -SRR_g.T_{SR} \tag{39}$$

- Reserve limit:

$$0 \le sr_g \le SRR_g.T_{SR}.St_g \tag{40}$$

- Generation limits:

$$p_g + sr_g \leq P_{g,max} \tag{41}$$

- Reserve requirements:

$$\sum_{g \in G} sr_g \geq p_g + sr_g \tag{42}$$

- Interface limit:

Base case:

$$\sum_{k \in k(if)} p_k \leq Rate_i \tag{43}$$

Contingency case:

$$\sum_{k \in k(if)} p_{k,c} \leq Rate_i \tag{44}$$

- Additional constraints:

$$s_{g,\text{LB}} \geq 0 \tag{45}$$

$$p_{d,shed} \geq 0 \tag{46}$$

$$p_{d,shed,c} \geq 0 \tag{47}$$

If preventive control strategy is used, then,

$$p_{g,c} = p_g \tag{48}$$

The objective function (18) minimizes the total system operating cost. The total system operating cost consists of various parts:

- The linear generating cost of generators producing energy
- The cost of procuring system wide spinning reserves from generators
- The penalty for shedding load in the system when generation and reserves in the system cannot be scheduled in a manner that respects all physical system limitations.

The power balance constraints (19) and (20) are included for the base case and each contingency case. The base case is the system as it is with all the transmission elements in service. Each contingency case represents a system scenario in which a specific transmission contingency is modeled. Power balance requires the net real power generation from all sources to meet the real power load and real power losses in the system. Power balance is to be satisfied in the base case as well as every contingency case. However, consistent with industry practices on application of constraint relaxations to SCED models, the designed SCED allows for load shedding in both the base case and the contingency cases. The high penalty factor applied as the coefficient to the load shedding variable in the objective function ensures that the SCED model will resort to load shedding only when there is a true infeasibility in the system. Equations (21) - (26) ensure that any load which is in service will be served, potentially with some load shedding. Two different sets of variables are used to define load serve and load shed during the base case and the contingency cases. The branch flows on transmission lines (27) - (31) are calculated for the base case and for various contingency cases. The branch flows for the base case and contingency cases are calculated based on network shift factors, such as PTDFs and OTDFs. The base case flows on branches must respect the normal line ratings (Rate A) and the post contingency flows on lines must respect the emergency ratings (Rate B). In order to accelerate the calculation process, flows on the lines obtained from AC power flow are used along with a combination of the product of the incremental generation change from the SCED and the associated shift factor. The post transmission contingency generation dispatch must be within the upper limit on the physical generation of the unit for each generating unit in the system as shown in (34). The post transmission contingency generation dispatch must be above the lower limit on the physical generation of the unit for each generating unit in the system as shown in (35). The ramp rate limits are shown in (36) - (39). The spinning reserve constraint (40) ensures that reserve allocated to a unit must be below the spinning ramp rate of the unit. The sum of the generation dispatch and spinning reserve allocated to a unit must be within the total capacity of the unit. The system reserve requirement (42) states that the total spinning reserve acquired in the system must be greater than or equal to the dispatch of the highest dispatched generator, so that the total reserve capacity is sufficient to cover loss of any generator. Constraints (43) and (44) are additional flow limits known as the interface limits, which further limit the total flow from one area to another due to other reasons (*e.g.*, voltage stability). The last constraint (48) depends on the system operating mode. The model consist of a variable $p_{g,c}$, which denotes the generation of a generator in a post transmission contingency state. Usually, system operators do not re-dispatch generators in response to transmission contingencies, however, this model includes this variable to allow this flexibility. This is typically considered as a preventive approach in transmission contingency modeling. The model allows for a corrective approach or a preventive approach. In the corrective approach, the SCED solves for a post transmission contingency dispatch variable. If a preventive approach is selected, the model forces the post contingency dispatch of a generating unit to be equal to its base case generation dispatch.

REFERENCES

[1] G. K. K. A. Clements and P. Davis, "Power system state estimation with measurement deficiency: An observability/measurement placement algorithm," *IEEE Transactions on Power Apparatus and Systems*, vol. 102, pp. 2012–2020, 1983.

[2] "Givens rotation," Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Givens_rotation

[3] T. A. Davis, "Algorithm 9xx: SuiteSparse:GraphBLAS: graph algorithms in the lanuage of sparse linear algebra," *ACM Transactions on Mathematical Software*, 2018.