Supplementary file for “Defending Against Unidentifiable Attacks in Electric Power Grids”

Zhengrui Qin, *Student Member, IEEE,* Qun Li, *Member, IEEE,* Mooi-Choo Chuah, *Senior Member, IEEE*

Appendix A
Best attack regions for unidentifiable attacks

Therefore, we first need to find the regions that require fewest compromised meters for an undetectable attack. In [6], Liu *et al*. proposed a heuristic algorithm for desirable attack region in DC model, where $\mathbf{z} = \mathbf{Hx} + \mathbf{e}$ and $\mathbf{H}$ is fixed; with column transformation of $\mathbf{H}$ matrix, they aimed to find a column vector with the greatest number of zero elements. However, in our AC model case, there is no such fixed $\mathbf{H}$ matrix and the relations between measurements and state variables are non-linear. Instead, we examine the Jacobian matrix $\partial\mathbf{h}/\partial\mathbf{x}$, denoted by $\mathbf{J}$. Similar to [6], we apply column transformations on the Jacobian matrix to find a column vector with the greatest number of zero elements, say vector $\mathbf{u}$. Then, we figure out the rows with non-zero elements in $\mathbf{u}$. Finally the attack region is the region containing meters i such that $u_i \neq 0$. The algorithm is summarized as follows.

```
Alg. 1: Finding the best attack region
1: Calculate $\mathbf{J}$ at the pre-attack point;
2: $\mathbf{u}$ =the column vector in $\mathbf{J}$ with most zeros;
3: For each column vector $\mathbf{j} \in \mathbf{J}$, $\mathbf{j} \neq \mathbf{u}$,
4:       Find $\mathbf{u}' = \mathbf{u} + c\cdot \mathbf{j}$ that results in most zero
         elements, where $c$ can be any scalar;
5: Endfor
6: If $\mathbf{u}'$ has more zero elements than $\mathbf{u}$, go to line 3;
7: Find the set of meters with indices $\{i|u_i \neq 0\}$; the
   attack region is the region where these meters are.
```

Different from $\mathbf{H}$, which is fixed, our Jacobian matrix is different at different starting points. Here, we assume a simple starting scenario that all voltages are 1 and all phases are 0, which is a feasible solution to power systems. We examine three IEEE bus systems: 9-bus system, 14-bus system, and 30-bus system. The results are shown in Table 1. As we can see, these attack regions usually are the regions with a leaf node or with fewer connections to the rest area of a bus system.

TABLE 1: The best attack regions with the metric d'.

bus system	d'	attack region
9-bus	2	bus 1 and bus 4
	2	bus 2 and bus 8
	2	bus 3 and bus 6
14-bus	2	bus 7 and bus 8
	5	bus 4,7,8 and 9
30-bus	2	bus 9 and bus 11
	2	bus 12 and bus 13
	4	bus 25 and bus 26

Appendix B

CLAIM: By eliminating the measurement with the largest residual until the remaining ones are consistent, the attack region defined above is not guaranteed to include all bad data.

Proof: Suppose the whole system has n buses with m measurements, then the system has $2n-1$ state variables. The adversary has modified $m-2n+1$ measurements, and the remaining $2n-1$ measurements are all critical and can make the system observable (and hence satisfy *Assumption 1*). Now the $2n-1$ measurements can give a deterministic solution for the state variables, but any $2n-2$ measurements of the same set cannot. Now let us select $2n-2$ measurements out of the set of $2n-1$ measurements, and refer to the remaining one measurement as R. The $2n-2$ measurements yield many feasible solutions of state variables for that particular power system. We select one of the feasible solutions, which is different from the one obtained using the set of $2n-1$ measurements. The adversary then modify the $m-2n+1$ measurements based on this selected feasible solution. Obviously, the largest residual will then occur on the meter that measures R. After eliminating R, the rest of the measurements are consistent. *Step 2* only identifies the attack region as a small neighborhood around R and hence does not include all bad data in the set which contains the $m-2n+1$ readings. □

- *Z. Qin and Q. Li are with the Department of Computer Science, College of William and Mary, VA, 23187.*
E-mail: {zhengrui, liqun}@cs.wm.edu.
- *M. Chuah is with the Department of Computer Science and Engineering, Lehigh University, Bethlehem, PA, 18015.*
E-mail: chuah@cse.lehigh.edu.

Appendix C
Direct Meter Verification to Eliminate Feasible Cases

The problem is formulated as follows. Suppose there are m meters in the power system. For each feasible case, we have a set of all meter values; we call them feasible values. Of course, some of these feasible values may be exactly the same as the readings collected from the meters. Therefore, for case k, $k \in [1, l]$, we have a set of feasible values for all meters, $\{a_{k,1}, a_{k,2}, ..., a_{k,m}\}$; for each meter i, $i \in [1, m]$, we have a set of feasible values for l different cases, denoted as $\{a_{1,i}, a_{2,i}, ..., a_{l,i}\}$. Each meter i, $i \in [1, m]$ has a real measured value a^*_i, which can be obtained by checking its reading at its physical location. All these notations are shown in Table 2. At least one of $a_{k,i}$, $k \in [1, l]$, is equal to a^*_i.

TABLE 2: The notations in meter verifying formulation.

	meter 1	meter 2	meter 3	...	meter m
case 1	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	...	$a_{1,m}$
case 2	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	...	$a_{2,m}$
...	...	...	...	...	...
case l	$a_{l,1}$	$a_{l,2}$	$a_{l,3}$	...	$a_{l,m}$
real case	a^*_1	a^*_2	a^*_3	...	a^*_m

Given a verified value a^*_i, if $a_{k,i} \neq a^*_i$, then we know that case k is not the real case; that is, by verifying meter i, we can exclude case k from the feasible set of cases; if $a_{k,i} = a^*_i$, feasible case k is possible to be the real case, depending on whether there exists $a_{k',i} = a^*_i$, $k' \neq k$. However, from the perspective of the control center, it cannot know the value a^*_i before physically checking meter i. What the control center knows is just the top part of Table 2. For feasible case k and case k', if $a_{k,i} \neq a_{k',i}$ we can guarantee that at least one of them is not the real case by verifying meter i. That is, if $a_{k,i} = a^*_i$, then case k' is not the real case; if $a_{k',i} = a^*_i$, then case k is not the real case; otherwise, both of them are not the real case. However for the case where $a_{k,i} = a_{k',i}$, we still cannot rule out either case k or case k' by verifying meter i, since in the case of $a_{k,i} = a_{k',i} = a^*_i$, case k and k' are still both feasible. Following this reasoning, in order to guarantee that one can find the real case, the control center has to verify a set of meters such that for any pair of case k and case k' there exists a meter index i in the set satisfying $a_{k,i} \neq a_{k',i}$. Thus, the unequal relations, such as $a_{k,i} \neq a_{k',i}$, are the essential information that can help us decide which meters to verify.

For each set of l values of meter i, $\{a_{1,i}, a_{2,i}, ..., a_{l,i}\}$, $i \in [1, m]$, each pair has a relation which is either "equal" or "unequal". Thus, there are $l' = \binom{l}{2}$ relations. We denote these relations as follows: First, we list the l' relations in the following order: $O_i = [(a_{1,i}, a_{2,i})$, $(a_{1,i}, a_{3,i})$, ..., $(a_{1,i}, a_{l,i})$, $(a_{2,i}, a_{3,i})$, ..., $(a_{2,i}, a_{l,i})$, ..., $(a_{l-1,i}, a_{l,i})]$, and index them by 1, 2, ..., l' sequentially. Second, we define a set S_i for each meter i, $i \in [1, m]$, such that its elements have integer values in the range $[1, ..l']$. S_i is empty in the beginning; j is added into S_i when jth pair in O_i are not equal to each other. Alg. 6 is the pseudo-code that how S_i is populated. The complexity of Alg. 6 is $O(ml^2)$.

```
Alg. 6: Set $S_i$ for meter $i$
$S_i = \emptyset$;
For $j = 1, l'$
    If $j$th pair in $O_i$ are unequal to each other
        $S_i = S_i \cup j$;
    Endif
Endfor
```

For example, suppose $l = 4$ and $a_{1,1} = a_{2,1} \neq a_{3,1} = a_{4,1}$ for meter 1, we can get $S_1 = \{2, 3, 4, 5\}$, as illustrated in Table 3. By going through this process for all meters, we can get a set $S = \{S_1, S_2, ..., S_m\}$.

TABLE 3: Set S_1 for meter 1 in case of $l = 4$.

Index	Relation	True/False	Elements in S_1
1	$a_{1,1} \neq a_{2,1}$	F	
2	$a_{1,1} \neq a_{3,1}$	T	2
3	$a_{1,1} \neq a_{4,1}$	T	3
4	$a_{2,1} \neq a_{3,1}$	T	4
5	$a_{2,1} \neq a_{4,1}$	T	5
6	$a_{3,1} \neq a_{4,1}$	F	

Now let $U = \{1, 2, 3, ..., l'\}$, where $l' = \binom{l}{2}$, and C is a set of meter indices. Then we can formally formulate our problem for two different cases: (1) with limited resource, the control center can exclude $l - 1$ out of l feasible cases (reveal the real case); and (2) with limited resource, the control center cannot exclude $l - 1$ out of l feasible cases. The formulations are:

(1) the first case:

min: $|C|$, such that $\{\cup S_i | i \in C\} = U$.

(2) the second case:

max: $|\{\cup S_i | i \in C\}|$, such that: $|C| \leq s$.

Apparently this problem has the same formulation as the set cover problem, except that S_i has some restrictions; for example for $l = 4$, S_i cannot be $\{1, 2\}$, which is a set of impossible relations ($a_{1,i} \neq a_{2,i}$, $a_{1,i} \neq a_{3,i}$, $a_{1,i} = a_{4,i}$, $a_{2,i} = a_{3,i}$, $a_{2,i} = a_{4,i}$, $a_{3,i} = a_{4,i}$). The set cover problem has been well studied in the literature, and we can use a greedy algorithm to solve this problem, which selects the set that covers the greatest number of elements not yet covered each time. Though the formulations are different for the above two cases, we can use the same algorithm, Alg. 7, as follows:

```
Alg. 7: Finding meters to verify: greedy algorithm
$X = U$;
$C = \emptyset$;
While $X \neq \emptyset$ or $|C| < s$;
    Select $S_i$ that maximizes $|S_i \cap X|$;
    $X = X - S_i$;
    $C = C \cup i$;
Endwhile
Output $C$.
```

The greedy algorithm has an approximation ratio of $O(ln(l^2))$, and it cannot guarantee an optimal solution. Considering l and s are usually small, we can resort to brute-force search to find the optimal solution, as shown in Alg. 8. The complexity of Alg. 8 is $O(\sum_{i=1}^{s} \binom{m}{i})$.

```
Alg. 8: Finding meters to verify: brute-force search.
  1: $n_0 = 0$;
  2: For $j = 1$ to $s$
  3:     For each different set $C'$ with $j$ indices
  4:         Calculate $n_1 = |\cup\{S_i|i \in C'\}|$;
  5:         if $n_1 = l(l-1)/2$, go to line 9;
  6:         if $n_1 > n_0$, then $n_0 = n_1$ and $C = C'$;
  7:     Endfor
  8: Endfor
  9: Output $C$.
```

Appendix D
Evaluation on 9-bus and 30-bus systems

Here we detail the evaluation on IEEE 9-bus system and 30-bus system, whose topologies are shown in Fig. 1 and Fig. 2 respectively.

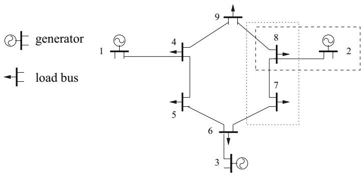

Fig. 1: The topology of 9-bus system in Matpower.

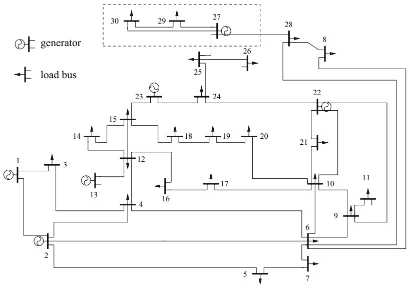

Fig. 2: The topology of 30-bus system in Matpower.

D.1 Generating unidentifiable attacks

We first generate two unidentifiable attacks using the 9-bus system in Matpower. For the Type I attack, the compromised meters are listed in Table 4, and the rest meters remain intact and their readings are omitted. The meter readings before the attack are based on the real power load vector $\{bus7, bus8\} = \{100, 0\}$, and the meter readings after the attack are based on the real power load vector $\{bus7, bus8\} = \{80, 20\}$; the loads in other buses have the same values as those in the Matpower distribution package. For the Type II attack, the compromised data are listed in Table 5. The meter readings before the attack are obtained when the load of bus 8 is 0, the meter readings after the attack are obtained when the load of bus 8 is 20; the remaining loads are the same as those in the Matpower distribution package.

TABLE 4: Type I attack in 9-bus system. The bold ones are the changed.

Meters	Before attack	After attack (Type I)
PI on bus7	-100	$\mathbf{-80}$
PL from bus7 to bus8	-75.95	$\mathbf{-58.03}$
PL from bus8 to bus7	76.51	**58.34**
PL from bus6 to bus7	24.18	**22.09**
QL from bus6 to bus7	22.64	**21.46**

TABLE 5: Type II attack in 9-bus system.

Meters	Before attack	After attack (Type II)
PL from bus2 to bus8	163.0	$\mathbf{-183.0}$
PL from bus8 to bus2	-163.0	**-183.0**

We then generate two unidentifiable attacks using the 30-bus system in Matpower. Both Type I and Type II attacks are shown in Table 6. Columns 3 show the changed meters for the Type I attack scenario. The meters in other region remain unchanged. The meter readings before the attack are based on the real power load vector $\{bus29, bus30\} = \{2.4, 10.6\}$, and the meter readings after the attack are based on the real power load vector $\{bus29\_1, bus30\_2\} = \{12.4, 0.6\}$; the loads in other buses have the same values as those in the Matpower distribution package. Column 4 shows the changed meters for the Type II attack scenario. The meter readings before the attack are obtained when the load of bus 30 is 10.6, the meter readings after the attack are obtained when the load of bus 30 is 20.6; the remaining loads are the same as those in the Matpower distribution package.

TABLE 6: Type I and II attacks in 30-bus system.

Meters	Before attack	After attack (Type I)	After attack (Type II)
PI on bus27	26.91	26.91	**37.63**
QI on bus27	11.39	11.39	**12.74**
PI on bus29	-2.4	$\mathbf{-12.4}$	-2.4
PL from bus27 to bus29	6.17	**9.32**	**10.56**
QL from bus27 to bus29	1.68	1.68	**2.27**
PL from bus29 to bus27	-6.08	$\mathbf{-9.12}$	-6.08
PL from bus27 to bus30	7.12	**3.96**	**13.46**
QL from bus27 to bus30	1.67	1.67	**2.45**
PL from bus30 to bus27	-6.95	$\mathbf{-3.91}$	-6.95
PL from bus29 to bus30	3.68	$\mathbf{-3.28}$	**7.90**
QL from bus29 to bus30	0.61	0.61	**0.88**
PL from bus30 to bus29	-3.65	**3.31**	-3.65

D.2 Locate the attack region and enumerate feasible cases

For the four attacks listed above, we first use Alg. 2 to get the deleted set D. The deleted set for each attack is listed in Table 7, where where $bsxx\_1/2$ means PI/QI on bus xx respectively, and $brxx\_1/2/3/4$ means the PL/QL on the from-bus and to-bus of branch xx respectively. In 9-bus power system, $br3 = \{bus5, bus6\}$, $br5 = \{bus6, bus7\}$,

$br6 = \{bus7, bus8\}$, $br7 = \{bus2, bus8\}$, and $br8 = \{bus8, bus9\}$. In 30-bus power system, $br37 = (bus27$, $bus29)$, $br38 = (bus27$, $bus30)$ and $br39 = (bus29$, $bus30)$. In order to show the effectiveness of IBE, we also list the real compromised set for each attack.

TABLE 7: The deleted sets and compromised set for four attacks.

Attack		Deleted set	Compromised set
9	Type I	$bs8\_1$, $br5\_3$, $br3\_3$ $br3\_1$, $bus5\_1$, $br5\_1$	$bs7\_1$, $br6\_1$, $br6\_3$ $br5\_1$, $br5\_2$
	Type II	$bs2\_1$, $bs8\_1$ $br7\_2$, $br8\_2$	$br7\_1$, $br7\_3$
30	Type I	$bs30\_1$, $br38\_2$, $br37\_2$ $br38\_4$, $br37\_4$, $br39\_2$ $br39\_4$	$bs29\_1$, $br37\_1$, $br37\_3$ $br38\_1$, $br38\_3$, $br39\_1$ $br39\_3$
	Type II	$bs30\_1$, $br38\_3$, $br37\_3$ $br39\_3$, $br37\_4$, $br39\_4$ $br38\_4$	$bs27\_1$, $bs27\_2$, $br37\_1$ $br37\_2$, $br38\_1$, $br38\_2$ $br39\_2$

Again we can see that the IBE method cannot identify the real compromised measurements, and there is even no common element between the deleted set and the compromised set.

Next we apply Alg. 3 on the deleted set listed in Table 7 to get the attack region. Though the deleted sets do not even contain one real compromised measurement, the attack regions obtained from Alg. 3 do contain all the compromised measurements. The attack regions are shown in the dashed rectangles in Fig. 1 and Fig. 2; in the 30-bus system, the two attacks have the same attack region.

Finally, we apply Alg. 4 directly to enumerate all feasible cases. For all four unidentifiable attacks, we are able to find out that there are only two feasible cases for each attack, just as same as described in Section D.1.

D.3 Cost optimization

D.3.1 Type I attack in 9-bus system

In this attack, we change five meters as shown in Table 4. Under this unidentifiable attack, the control center may either conclude that the power demands of bus 7 and bus 8 are 100 and 0 (case 1), or they are 80 and 20 (case 2). These two load vectors are fed together with the constraints into IPOPT to determine the optimal state variables, the voltage and phase on each bus, which can minimize the total cost. In the original Matpower packet, all line capacities are 250 MVA. In order to examine the impact of line capacities, we adjust the line capacity of line 6 (between bus 7 and bu 8) to 60 MVA. The cost comparison is listed in Table 8, in which solution 1 is the optimal solution based on case 1, and solution 2 is the optimal solution based on case 2. "Over-load" means that if the control center gets a solution based on case 2 but it is actually case 1, then some branches will exceed their line capacities. As we can see, our solution is better than solution 2. However, our solution is comparable to Solution 1. The reason is that even we limit the line capacity between bus 7 and bus 8, the power can go from generator 2 to bus 7 by circumventing the line between bus 7 and bus 8.

TABLE 8: The cost comparison for type I attack in 9-bus system.

	If case 1	If case 2	Average
Solution 1	5316.9	5316.9	5316.9
Solution 2	Over-loaded	5306.0	NA
Our solution	5317.0	5315.5	5316.2

D.3.2 Type II attack in 9-bus system

Table 5 shows the type II attack in the 9-bus system. The two feasible cases are: the real power demand on bus 7 is either 0 (case 1) or 20 (case 2). In this example, we do not change any line capacity. The cost comparison is listed in Table 9, where "Over-powered" means that if the control center gets a solution based on case 2 but it is actually case 1, then some buses will get more power than their demands. As we can see, our solution is still the best, given that the control center cannot favor one case over the other.

TABLE 9: The cost comparison for type II attack in 9-bus system.

	If case 1	If case 2	Average
Solution 1	5310.0	6055.0	5682.5
Solution 2	Over-powered	5805.2	NA
Our solution	5310.1	5863.4	5586.7

D.3.3 Two attacks in 30-bus system

The evaluation for the two attacks in 30-bus system is similar to that in 9-bus system and 14-bus system. Here we omit the details but only keep the main results. In the type I attack, the two feasible cases are: the power demands of bus 29 and 30 are 2.4 and 10.6 (case 1), or they are 12.4 and 0.6 (case 2). And we adjust the line capacities for the following branches: branch 37, branch 38, and branch 39 from the original value of 16 MVA to 4 MVA, 8 MVA and 3 MVA respectively. The cost comparison is listed in Table 10. In the type II attack, the two feasible cases are: the real power demand on bus 30 is either 10.6 (case 1) or 20.6 (case 2), and the cost comparison is shown in Table 11.

TABLE 10: The cost comparison for type I attack in 30-bus system.

	If case 1	If case 2	Average
Solution 1	635.0	Over-loaded	NA
Solution 2	693.1	693.1	693.1
Our solution	680.3	693.7	687.0

TABLE 11: The cost comparison for type II attack in 30-bus system.

	If case 1	If case 2	Average
Solution 1	581.2	775.0	678.1
Solution 2	Over-powered	623.6	NA
Our solution	581.3	750.7	666.0

Again, we can see that our solutions is the best on average among all the solutions, which shows that our optimization strategy is indeed viable and effective.