Robust Optimal Protection Strategy Against False Data Injection Attacks in Power Grids

Zeli Wang, Tong Han, Zifa Liu
School of Electrical and Electronic Engineering
North China Electric Power University
Beijing, China 102206
Email: hantong.eee@gmail.com

Shujun Wang
Mudanjiang Power
Industry School
Mudanjiang, China, 157011
Email: 2236200569@qq.com

***Abstract*—This paper addresses the issue of the optimal protection strategy with minimum protection cost against false data injection attacks, considering multiple power grid topologies. The model of robust optimal protection strategy, that can make power grids immune from false data injection attacks even if the grid topology changes, is first proposed. And then combining graph theory and recursive Bayesian estimation, we solve the model from the standpoint of pattern recognition. Finally, by testing on the IEEE 14-bus system, the correctness and effectiveness of our proposed robust optimal protection strategy model and its solving algorithm are demonstrated.**

***Index Terms*—Cyber-physical system, false data injection attack, optimal protection, topology change.**

I. Introduction

With extensively permeation of information technologies, modern power grids have developed into a complex cyber-physical system. Due to the strong interconnection between the cyber system and the physical system, faults in the cyber system will not only affect the normal operation of itself, but also the security, stability and economy of the physical system. This new security problem is called cyber-physical security problems. And among them, the false data injection attack is a imperative form [1], [2].

Briefly, false data injection attacks are the cyber attacks that adversaries tamper with measurements in order to change the results of power system state estimation stealthily, and potentially affect the security, stability and economy of power grids [1]–[3]. And there are mainly two kinds of countermeasures against false data injection attacks: detection-based countermeasures and protection-based countermeasures. In this paper, we focus on the later one, namely counteracting false data attacks by protecting specific measurements .

Recent studies have investigated some about the protection-based countermeasures against false data injection attacks. In [4], it is proved that it is necessary and sufficient to protect a basic measurement set for preventing power grids from false data injection attacks. To address the complexity issue of selecting a basic measurement set with minimum total protection cost, [5] and [6] both propose a fast greedy algorithm. And in [7], the optimal protection problem is characterized as a variant Steiner tree problem in a graph. Based on the graphical characterization, both exact and reduced-complexity algorithms are proposed. In [8] , a bilevel mixed integer linear programming model is proposed to determine the least number of measurements to be protected. A decomposition approach is adopted to obtain the suboptimal solution and a subnetwork-protection-based approach is proposed to further reduce the computation complexity.

However, a serious demerit of the existing protection-based countermeasures against false data injection attacks is that they all determine the protected measurements considering only one certain power grid topology. Since power grids are operated with topology changes, even if the obtained measurements are protected, adversaries can still successfully launch false data injection attacks by tampering the unprotected measurements.

In this paper, we address the issue of the optimal protection strategy with minimum protection cost considering multiple power grid topologies. Firstly, we give the problem formulation of the robust optimal protection strategy, i.e., a optimization model. And then, combining graph theory and recursive Bayesian estimation, the solving approach and algorithms for the optimization model are proposed from the standpoint of pattern recognition. Finally, the robust optimal protection strategy is tested on the IEEE 14-bus system.

II. Problem Formulation of Robust Optimal Protection Strategy

The basic idea of robust optimal protection strategy is that by protecting a specific set of measurements from being tampered with using the minimum protection cost, power grids can avoid false data injection attacks under any frequent topology change. Since for any frequent grid topology, there is always at least one basic measurement set is protected, attackers are incapable of launch successful false data injection attacks.

Let $\Gamma = \{\Gamma_i | i = 1, 2, \ldots, n_t\}$ denote the set of grid topologies, with Γ_i and n_t representing a frequent grid topology and the number of Γ_i respectively, and $\boldsymbol{z} = [z_1, z_2, \ldots, z_m]^T$ denote the measurement vector corresponding to all configured measurements. The vector $\boldsymbol{b} = [b_1, b_2, \ldots, b_m]^T$ consist of boolean variables, with $b_i = 1$ and $b_i = 0$ representing measurement z_i is and is not protected respectively, and $\boldsymbol{c} = [c_1, c_2, \ldots, c_m]^T$ is the vector of protection cost with c_i representing the protection cost of the measurement z_i.

Then the problem of robust optimal protection strategy can be formulated as the following optimization model:

$$\begin{aligned} \boldsymbol{b}_{\text{opt}} = \arg\min_{\boldsymbol{b}} \ & \boldsymbol{b}^T \boldsymbol{c} \\ \text{s.t. } & O\left(\Gamma_i, \boldsymbol{z}, \boldsymbol{b}\right) = 1 \quad i = 1, 2, \ldots, n_t. \end{aligned} \tag{1}$$

Here $\boldsymbol{b}^T \boldsymbol{c}$ is the total protection cost. And $O\left(\Gamma_i, \boldsymbol{z}, \boldsymbol{b}\right)$ is the function for network observability analysis, denoting that given grid topology Γ_i and available measurements, i.e., all z_i with $b_i = 1$, if the grid is fully observable, then $O\left(\Gamma_i, \boldsymbol{z}, \boldsymbol{b}\right) = 1$, otherwise $O\left(\Gamma_i, \boldsymbol{z}, \boldsymbol{b}\right) = 0$.

To simplify the problem, according to the practice, we give the following basic assumptions :

Assumption 1: active power measurements and reactive power measurements are configured and protected in pairs, and the cost of protecting a pair is same as that of protecting any one in the pair;

Assumption 2: there is a topology in Γ, assumed to be Γ_1, that can be transformed into any topology $\Gamma_i \in \Gamma$, $i \neq 1$ by removing branches;

Assumption 3: for $\forall \Gamma_i \in \Gamma$, the power grid is not disaggregated and is fully observable with all configured measurements.

Base on the above assumptions, the problem of robust optimal protection strategy only involve the active power measurements and observability analysis of voltage angles, and then (1) is rewritten as

$$\begin{aligned} \tilde{\boldsymbol{b}}_{\text{opt}} = \arg\min_{\tilde{\boldsymbol{b}}} \ & \tilde{\boldsymbol{b}}^T \tilde{\boldsymbol{c}} + c_{\text{u,min}} \\ \text{s.t. } & O\left(\Gamma_i, \tilde{\boldsymbol{z}}, \tilde{\boldsymbol{b}}\right) = 1 \quad i = 1, 2, \ldots, n_t \end{aligned} \tag{2}$$

with $\tilde{\boldsymbol{b}}$, $\tilde{\boldsymbol{c}}$ and $\tilde{\boldsymbol{z}}$ denoting vectors consisting of entries corresponding with active power measurements of $\boldsymbol{b}$, $\boldsymbol{c}$ and $\boldsymbol{z}$, respectively. And $\tilde{\boldsymbol{b}}^T \tilde{\boldsymbol{c}} + c_{\text{u,min}}$ is the total protection cost with $c_{\text{u,min}}$ representing the minimum protection cost of one voltage measurement.

It should be noted that given Assumption 1, the network observability is approximately equivalent to the observability of voltage angles, i.e., if voltage angles are fully observable, then the power grid is fully observable provided that there is any bus configured with voltage magnitude measurements. And the final protection strategy can be obtained by finding a magnitude measurement with minimum protection cost after getting $\tilde{\boldsymbol{b}}_{\text{optimal}}$ by solving (2).

III. Approach for Solving The Proposed Model

The proposed model of robust optimal protection strategy is a nonlinear integer optimization model with black-box functions. And for large-scale power grids, the dimension of optimization variables increase greatly. Thus it is hard to solve the proposed model efficiently and optimally from the standpoint of optimizing, such as using the branch and bound algorithm or evolutionary algorithms.

To cope with the proposed strategy model, we propose a solving approach combining graph theory and recursive Bayesian estimation. The main idea can be explained with two steps. The first step is to find all the possible basic measurement set for the power grid with topology Γ_1. And then the second step is to determine a specific one among all basic measurement sets found in the first step, considering minimizing the total protection cost and ensuring full observability of the power grids with topology changes by adding adequate measurements to the basic measurement sets.

The first step can be solved with graph theory. And for the second step, its essence is a pattern recognition problem, i.e., finding the optimal one among some measurement sets and adjusting measurements in the sets according to topology changes. The improved recursive Bayesian estimation proposed in our previous work [9] and [10] can be introduce to address the second step. And we explain our solving approach in detail in the following parts.

A. Enumeration of Basic Measurement Sets Based on Graph Theory

The necessary and sufficient condition of power grids being fully observable is that there is a spanning tree of the undirected graph of the power grid, and edges of the spanning tree satisfy specific mappings with measurements. Therefore, a feasible way to find all the possible basic measurement sets of power grids is that: firstly find all the possible spanning trees of the graph of the power grid, secondly find all the possible mappings for each spanning tree, and finally determine basic measurement sets corresponding with each spanning tree and thus all the possible basic measurement sets of power grids.

In this paper, the algorithm for finding all spanning trees of graphs proposed in [11] is used. Assuming that the undirected graph of the power gird with the topology Γ_1 is $G_1 = (V_1, E_1)$ with V_1 and E_1 denoting sets of vertices and edges of G_1 respectively, the algorithm flow can be illustrated as Fig. 1.

In Fig. 1, T is the current generated subtree, and F is the list to store all edges going from vertices in T to vertices outside T. The set $\{L\}$ is used to store all the found spanning trees, and FF is the list used to restore F. And for clarity, the algorithm shown in Fig. 1 is symbolized by $\{L\} = ST(G)$ with G and $\{L\}$ denoting the input graph and the output spanning tree set respectively in the following part. Readers interested in theoretical foundations of this algorithm should refer to [11].

After obtaining all the spanning trees of G_1, the next step is to determine basic measurement sets corresponding with each $L_i \in \{L\}$ and then all the basic measurement sets of the power grid. According to [12], given the graph of the power grid and the measurement configuration, the power grid is fully observable only if there is a spanning tree and a mapping satisfying two conditions:

Condition 1: the mapping is one-to-one between all edges of the spanning tree and partial configured measurements;

Condition 2: the measurement in 1) mapped to a edge is a active power flow measurement or a terminal bus's active power injection measurement both of the branch corresponding with this edge.

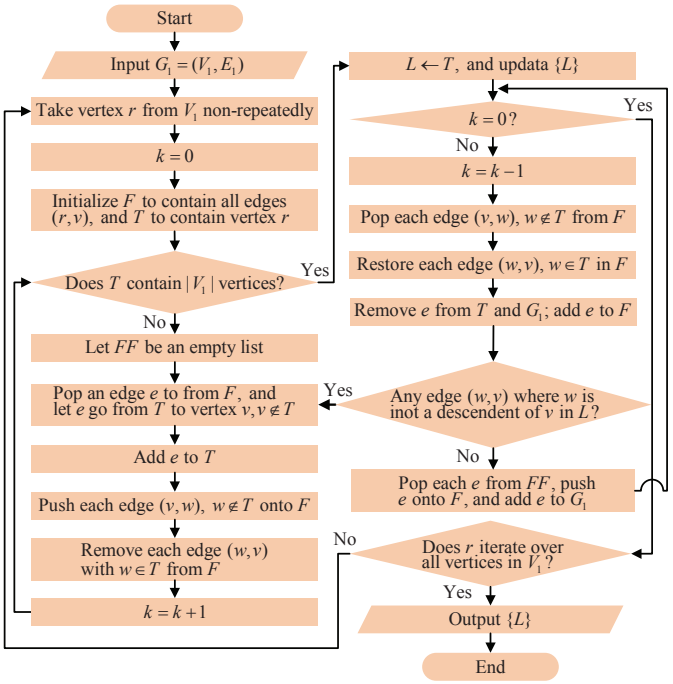

Fig. 1. Flowchart of the algorithm for finding all spanning trees.

Based on the above two requirements, we give the basic measurement sets enumeration algorithm as shown in Algorithm 1. The output $\mathbf{M}$ of Algorithm 1 is the set containing all basic measurement sets of power gird with the topology Γ_1.

Algorithm 1 Basic measurement sets enumeration algorithm

Input: G_1; $\tilde{\boldsymbol{z}}$

$L \leftarrow ST(G_1)$
repeat
  $L_i \leftarrow$ a spanning tree from $\{L\}$
  Let V_{L_i} and E_{L_i} be the vertex set and edge set of L_i respectively.
  repeat
    $s_j \leftarrow$ a edge from E_{L_i}
    Compute all measurement sets $\Upsilon_{ij} = \{\tilde{z}_k\}$that can form a mapping satisfying Condition 2 with e_j.
  until e_j has traversed E_{L_i}
  Compute all $\mathrm{M}_{ir} = \{\tilde{z}_j\}$ for L_i, satisfying $|\mathrm{M}_{ir}| = |E_{L_i}|$ and $\forall z \in \mathrm{M}_{ir}$, there is no $z' \in \mathrm{M}_{ir}$, $z' \neq z$ making $z \in \Upsilon_{ij}$ and $z' \in \Upsilon_{ij}$.
  $\mathbf{M}_i \leftarrow \{\mathrm{M}_{ik}\}$
until L_i has traversed $\{L\}$
$\mathbf{M} \leftarrow \bigcup\{\mathbf{M}_i | 1 \leq i \leq |\{L\}|\}$

Output: $\mathbf{M}$

B. Determination of Optimal Basic Measurement Set Based on Recursive Bayesian Estimation

To determine the optimal basic measurement set from $\mathbf{M}$, an approach based on recursive Bayesian estimation illustrated is proposed in this section. Fig. 2 give an illustration of one recursion of the proposed approach. In each recursion, one new gird topology $\Gamma_i \in \Gamma$ is considered, and then one recursion as shown in Fig. 2 is execute.

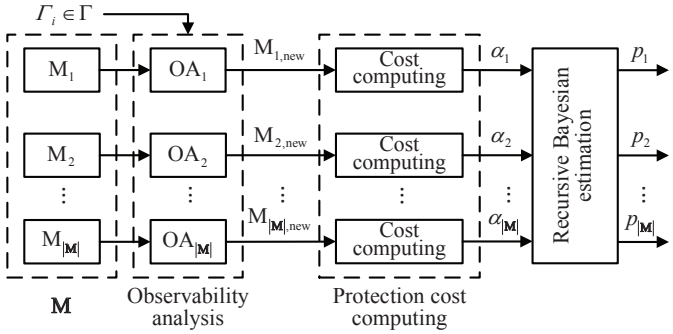

Fig. 2. Illustration of determination of optimal basic measurement set based on recursive Bayesian estimation (one recursion).

In Fig. 2, $\mathrm{M}_1 \sim \mathrm{M}_{|\mathbf{M}|}$ denote all the basic measurement sets in $\mathbf{M}$, and $\mathrm{OA}_1 \sim \mathrm{OA}_{|\mathbf{M}|}$ represent observability analysis for $\mathrm{M}_1 \sim \mathrm{M}_{|\mathbf{M}|}$ under topology Γ_i respectively. And $\mathrm{M}_{1,\mathrm{new}} \sim \mathrm{M}_{|\mathbf{M}|,\mathrm{new}}$ denote the updated basic measurement sets corresponding with $\mathrm{M}_1 \sim \mathrm{M}_{|\mathbf{M}|}$ respectively, after observability analysis. Each one in $\mathrm{M}_{1,\mathrm{new}} \sim \mathrm{M}_{|\mathbf{M}|,\mathrm{new}}$ represent a kind of protected measurement set, i.e., a protection strategy. And $\mathrm{M}_{1,\mathrm{new}} \sim \mathrm{M}_{|\mathbf{M}|,\mathrm{new}}$ are assigned to $\mathrm{M}_1 \sim \mathrm{M}_{|\mathbf{M}|}$ respectively in the next recursion. The step of protection cost computing is to compute the protection cost of $\mathrm{M}_{1,\mathrm{new}} \sim \mathrm{M}_{|\mathbf{M}|,\mathrm{new}}$, and $\alpha_1 \sim \alpha_{|\mathbf{M}|}$ are values of the likelihood function.

The step of observability analysis in Fig. 2 is executed using the numerical method proposed in [13] and [14]. To take observability analysis for M_i under topology Γ_i as an example, we give the observability analysis algorithm as illustrated in Algorithm 2. It should be noted that to ensure the protection cost of added measurements is minimum, in Gaussian elimination used in Algorithm 2, the protection cost of the measurement corresponding to the row containing the eliminated entry should not be lower than that of the measurement corresponding to the row containing the pivot used in current elimination. And this can be realized by elementary row operations.

The recursive Bayesian estimation in Fig. 2 is executed using the improved recursive Bayesian estimation proposed in our previous work [9] and [10], which is more efficient and robust compared with traditional one. The recursion formulas of the recursive Bayesian estimation are given as

$$\hat{p}_i^{(k)} = \frac{\alpha_i^{(k)} p_i^{(k-1)}}{\sum_{j<i} \alpha_j^{(k)} \hat{p}_j^{(k)} + \sum_{j \geq i} \alpha_j^{(k)} \hat{p}_j^{(k-1)}} \tag{3}$$

$$p_i^{(k)} = \frac{\hat{p}_i^{(k)}}{\sum_{j=1}^{|\mathbf{M}|} \hat{p}_j^{(k)}}. \tag{4}$$

Here k is the current recursion time. And $p_i^{(k)}$ is the posterior probability that M_i is the optimal basic measurement set after

Algorithm 2 Observability analysis algorithm

Input: Γ_i; M_i; $\tilde{\boldsymbol{z}}$; $\tilde{\boldsymbol{c}}$

Compute the Jacobian matrix $\mathbf{H}_{AA}$ of DC state estimation model according to Γ_i and M_i, and assuming branch impedance to be 1 p.u..
$\mathbf{G}_{AA} \leftarrow {\mathbf{H}_{AA}}^T \mathbf{H}_{AA}$
Decomposed $\mathbf{G}_{AA}$ into its Cholesky factors $\mathbf{L}\mathbf{D}\mathbf{L}^T$.
if $\mathbf{D}$ has only one zero pivot **then**
  $\mathrm{M}_{i,\mathrm{new}} \leftarrow \mathrm{M}_i$
else
  $\mathbf{W} \leftarrow$ rows in $\mathbf{L}^{-1}$ corresponding to zero pivots of $\mathbf{D}$
  $\mathbf{C} \leftarrow \mathbf{A}\mathbf{W}^T$, with $\mathbf{A}$ denoting branch-bus incidence matrix
  Find all unobservable branches, which are branches corresponding to rows in $\mathbf{C}$ with at least one nonzero entry.
  Get all observable islands by removing all unobservable branches.
  Let $\mathrm{M}_\mathrm{c} = \{\tilde{z}_i\}$, where $\tilde{z}_i \in \tilde{\boldsymbol{z}}$, $\tilde{z}_i \notin \mathrm{M}_i$ and $\tilde{z}_i$ connects at least two different observable islands.
  $\mathbf{B} \leftarrow \mathbf{H}_\mathrm{c}\mathbf{W}^T$, where $\mathbf{H}_\mathrm{c}$ is the block of $\mathbf{H}_{AA}$ corresponding to measurements in M_c
  Get $\mathbf{E}$, row echelon form of $\mathbf{B}$, by Gaussian elimination.
  Let M_a be the set of measurements in M_c corresponding to rows in $\mathbf{E}$ with a nonzero pivot.
  $\mathrm{M}_{i,\mathrm{new}} \leftarrow \mathrm{M}_i \cup \mathrm{M}_\mathrm{a}$
end if

Output: $\mathrm{M}_{i,\mathrm{new}}$

the kth recursion. $p_i^{(k-1)}$ is the prior probability that M_i is the optimal basic measurement set before the kth recursion, and also the posterior probability that M_i is the optimal basic measurement set after the $(k-1)$th recursion. $\hat{p}_i^{(k)}$ is the auxiliary probability in the kth recursion. And $\alpha_i^{(k)}$ denotes the likelihood function given by

$$\alpha_i^{(k)} = \exp(-0.5(\boldsymbol{c}_i^{(k)})^T \mathbf{C}_i^{(k)} \boldsymbol{c}_i^{(k)}) \tag{5}$$

with $\boldsymbol{c}_i^{(k)}$ representing the protection cost vector corresponding with measurements in $\mathrm{M}_{i,\mathrm{new}}$, and $\mathbf{C}_i^{(k)}$ representing the diagonal weight coefficient matrix. In theory, as k increases, the posterior probability of the measurement sets corresponding to the robust optimal protection strategy will progressively approach 1 while the posterior probability of other measurement sets will progressively approach 0 [13], [14].

Since the number of basic measurement sets, i.e., $|\mathbf{M}|$, is generally large, it is essential to progressively reduce the set $\mathbf{M}$ during recursion for lessening computation burden. After each recursion in Fig. 2, e.g., the kth recursion, we execute the reduction algorithm as given in Algorithm 2. According to [14], the parameter $p_{\mathrm{m,sum}}$ in Algorithm 2 is set to 0.9 in our work.

C. The Overall Algorithm of the Solving Approach

Based on the above analysis and algorithms, we further illustrate our proposed approach to solve the robust optimal protection strategy model. The overall algorithm of the solving approach is given in Algorithm 4. The output M_opt of Algorithm 4 is the set of measurements whose corresponding entries in $\boldsymbol{b}_\mathrm{opt}$ are 0, i.e., the robust optimal protection strategy.

Algorithm 3 Reduction algorithm

Input: $\mathbf{M}$

Sort $\mathrm{M}_1 \sim \mathrm{M}_{|\mathbf{M}|}$ in descending order of the posterior probability $p_i^{(k)}$.
$m \leftarrow 1$
while $\sum_{j=1}^{m} p_j^{(k)} \leq p_{\mathrm{m,sum}}$ **do**
  $m \leftarrow m + 1$
end while
if $m = |\mathbf{M}| + 1$ **then**
  $\mathbf{M} \leftarrow \mathbf{M}$
else
  $\mathbf{M} \leftarrow$ the set of $\mathbf{M}$ with eliminating $\mathrm{M}_1 \sim \mathrm{M}_{m-1}$ from itself.
end if

Output: $\mathbf{M}$

Algorithm 4 Reduction algorithm

Input: Γ; $\boldsymbol{z}$; $\boldsymbol{c}$

Execute Algorithm 1 to compute $\mathbf{M}$.
$k \leftarrow 0$, $p_i^{(0)} \leftarrow \frac{1}{|\mathbf{M}|}$
repeat
  $\Gamma_i \leftarrow$ a non-repetitive topology from Γ
  $k \leftarrow k + 1$
  Execute one recursion as illustrated in Fig. 2.
  Reduce $\mathbf{M}$ using Algorithm 3.
until $k = |\mathbf{M}|$
$z_{\mathrm{u,min}} \leftarrow$ the voltage magnitude measurement with minimum protection cost.
$\mathrm{M}_\mathrm{opt} \leftarrow \arg\max_{\mathrm{M}_{i,\mathrm{new}}} p_i^{(k)} \cup \{z_{\mathrm{u,min}}\}$

Output: M_opt

IV. Case Study

The proposed model of robust optimal protection strategy and its solving algorithm are tested in the IEEE 14-bus system, to demonstrate their effectiveness.

A. Parameter Settings

The measurement configuration of the IEEE 14-bus system is given in Fig. 3. All branches are configured with power flow measurements in one terminal, all buses are configured with voltage magnitude measurements, and bus 2, 4, and 6 are configured with injection power measurements.

The protection cost of each injection power measurements and each voltage magnitude measurement is set to 1.5 and 1, respectively. The protection cost of each power flow measurements in the branch 1-2, 2-3, 2-5, 4-5, 4-9, 6-11, 6-13, 7-9, 9-14 and 12-13 is set to 1, and that in the branch 1-5, 2-4, 3-4, 4-7, 5-6, 6-12, 7-8, 9-10, 10-11 and 13-14 is set to 2. Note

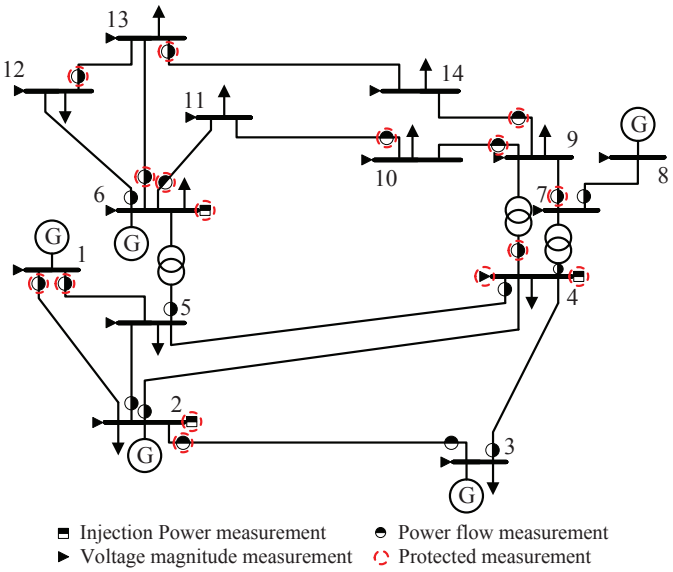

Fig. 3. Measurement configuration of the IEEE 14-bus system.

TABLE I
ALL BASIC MEASUREMENTS SETS UNDER TOPOLOGY Γ_1

Number of basic measurement sets	Measurements	
	Power flow measurements	Injection power measurements
1	4-9,6-11,9-14,9-10,1-5,2-3,6-13,6-12,7-8	2,6,4
2	4-9,5-6,9-14,9-10,1-5,2-3,6-13,6-12,7-8	2,6,4
3	4-9,5-6,9-14,6-11,9-10,1-5,2-3,6-13,7-8	2,6,4
4	4-9,5-6,9-14,6-11,9-10,1-5,2-3,6-12,7-8	2,6,4
5	4-9,5-6,9-14,6-11,9-10,1-5,2-3,6-13,6-12,7-8	2,4
⋮	⋮	⋮
1586	1-2,4-9,12-13,9-14,9-10,13-14,6-13,10-11,3-4,2-4,7-9	4
1587	1-2,4-9,12-13,7-8,9-14,9-10,13-14,6-13,10-11,3-4,2-4	4
1588	1-2,4-9,12-13,7-8,9-14,9-10,13-14,6-13,10-11,3-4,2-4,7-9	4
1589	1-2,4-9,4-5,9-10,12-13,13-14,6-13,9-14,10-11,3-4,2-4,7-9	–
1590	1-2,4-9,4-5,7-8,9-10,12-13,13-14,6-13,9-14,10-11,3-4,2-4	–

that the protection cost here represents relative values instead of the actual protection cost.

And Γ consists of 51 grid topologies, in which Γ_1 is the topology as shown in Fig. 3, and the other 50 topologies are obtained by removing branches from Γ_1. Due to the limit of space, details of these topologies are not given.

B. Results and Analysis

By executing Algorithm 1, we obtain a total of 1590 basic measurement sets of power gird under the topology Γ_1, i.e., the set $\mathbf{M}$, as given in TABLE I. It should be noted that for each basic measurement set, it also contain the injection power measurement at bus 7, which is a virtual measurement.

Fig. 4 and Fig. 5 give the change curves of posterior probability $p_i^{(k)}$ of different basic measurement sets in $\mathbf{M}$ without and with reduction for $\mathbf{M}$ in recursion, respectively. And Fig. 6 is the scatter plot illustrating the relationship between total protection cost and posterior probability after last recursion of different basic measurement sets.

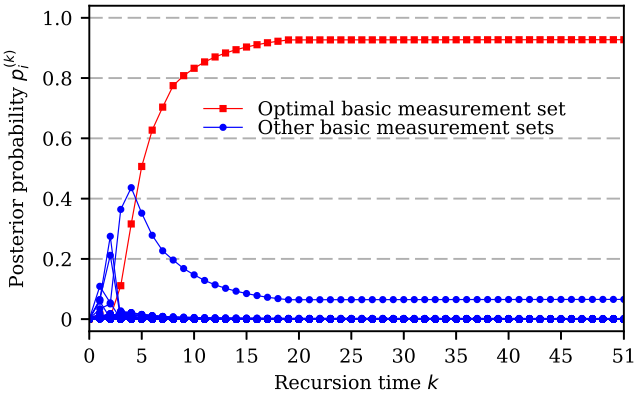

Fig. 4. Change curve of posterior probability of different basic measurement sets without reduction for $\mathbf{M}$ in recursion.

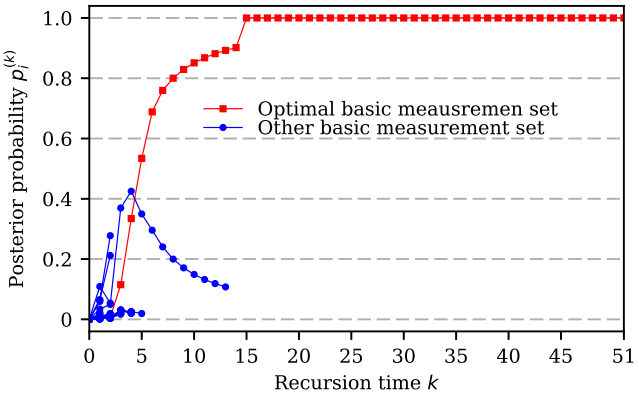

Fig. 5. Change curves of posterior probability of different basic measurement sets with reduction for $\mathbf{M}$ in recursion.

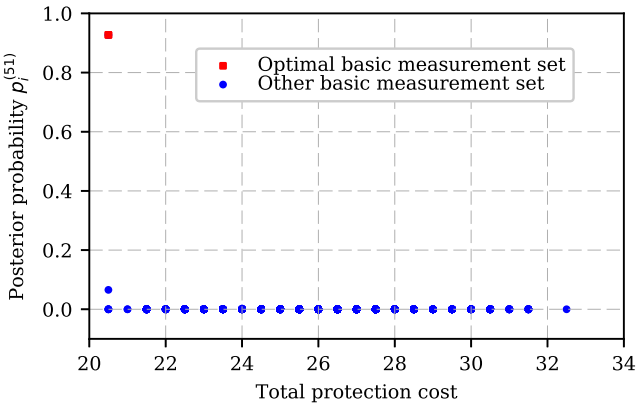

Fig. 6. Relationship between total protection cost and posterior probability after last recursion of different basic measurement sets.

According to Fig. 4 and Fig. 6, the basic measurement set whose posterior probability approaches 1 after several time of recursion has the minimum total protection cost, while posterior probability of the other basic measurement sets with

higher or equal total protection cost approach 0. Besides, the optimal basic measurement set whose posterior probability progressively approaches 1 in Fig. 4 and that in Fig. 5 are the same, illustrating the correctness of the Reduction algorithm. And with Fig. 5, it can be found that computation burden can be effectively slashed by the reduction of $\mathbf{M}$ in recursion. After 5 times of recursion, there are only two basic measurement sets retained for further recursion, and after approximately 15 times of recursion, only one basic measurement sets, i.e., the optimal basic measurement set, is retained for further recursion.

Finally, by adding a voltage magnitude measurement with minimum protection cost, e.g., the voltage magnitude measurement at bus 4 to the identified optimal basic measurement set, the measurement set corresponding to the robust optimal protection strategy can be obtained. And the measurements need to be protected against false data injection attacks are marked in Fig. 3.

V. Conclusion

This paper proposes a robust optimal protection strategy model that minimizes the total protection cost and considers multiple power grid topologies, making power grids immune from false data injection attacks even if the grid topology changes. For solving the proposed model, graph theory is first used to enumerate all basic measurement sets of power grids. And then from the standpoint of pattern recognition, the optimal basic measurement set is determined using recursive Bayesian estimation. For lessening computation burden in recursion, a reduction algorithm is also proposed. Finally, by testing on the IEEE 14-bus system, it is demonstrated that the robust optimal protection strategy model and its solving algorithm are correct and effective.

References

[1] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[2] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[4] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[5] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[6] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1–12, 2015.

[7] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[8] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–9, 2016.

[9] Y. Chen, F. Liu, G. He, and S. Mei, "A seidel-type recursive bayesian approach and its applications to power systems," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1710–1711, 2012.

[10] Y. Chen, F. Liu, S. Mei, G. He, Q. Lu, and Y. Fu, "An improved recursive bayesian approach for transformer tap position estimation," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2830–2841, 2013.

[11] H. N. Gabow and E. W. Myers, "Finding all spanning trees of directed and undirected graphs," *SIAM Journal on Computing*, vol. 7, no. 3, pp. 280–287, 1978.

[12] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[13] B. Gou and A. Abur, "A direct numerical method for observability analysis," *IEEE Transactions on Power Systems*, vol. 15, no. 2, pp. 625–630, 2000.

[14] B. Gou and A. Abur, "An improved measurement placement algorithm for network observability," *IEEE Transactions on Power Systems*, vol. 16, no. 4, pp. 819–824, 2001.