Chapter 8
Bi-level Adversary-Operator Cyberattack Framework and Algorithms for Transmission Networks in Smart Grids

M. Hadi Amini, Javad Khazaei, Darius Khezrimotlagh, and Arash Asrari

Abstract Transmission system is one of the most important assets in secure power delivery. Recent advancements toward automation of smart grids and application of supervisory control and data acquisition (SCADA) systems have increased vulnerability of power grids to cyberattacks. Cyberattacks on transmission network, specifically the power transmission lines, are among crucial emerging challenges for the operators. If not identified properly and in a timely fashion, they can cause cascading failures leading to blackouts. This chapter tackles false data injection modeling from the attacker's perspective. It further develops an algorithm for detection of false data injections in transmission lines. To this end, first, a bi-level mixed integer programming problem is introduced to model the attack scenario, where the attacker can target a transmission line in the system and inject false data in load measurements on targeted buses in the system to overflow the targeted line. Second, the problem is analyzed from the operator's viewpoint and a detection

M. H. Amini (✉)
School of Computing and Information Sciences, Florida International University, Miami, FL, USA

Sustainability, Optimization, and Learning for InterDependent Networks Laboratory (solid lab), Florida International University, Miami, FL, USA
e-mail: moamini@fiu.edu; hadi.amini@ieee.org; www.solidlab.network

J. Khazaei
Electrical Engineering, Architectural Engineering, Penn State University Park, State College, PA, USA
e-mail: jxk792@psu.edu

D. Khezrimotlagh
Mathematics, Penn State Harrisburg, Middletown, PA, USA
e-mail: dzk349@psu.edu

A. Asrari
Electrical and Computer Engineering, Southern Illinois University, Carbondale, IL, USA
e-mail: arash.asrari@siu.edu

M. H. Amini (ed.), *Optimization, Learning, and Control for Interdependent Complex Networks*, Advances in Intelligent Systems and Computing 1123,
https://doi.org/10.1007/978-3-030-34094-0_8

algorithm is proposed using l_1 norm minimization approach to identify the bad measurement vector in data readings. In order to evaluate the effectiveness of the proposed attack model, case studies have been conducted on IEEE 57-bus test system.

Keywords Cyberphysical security · Optimal attacker strategy · Attack detection · Sparsity-based decomposition · Energy systems · Smart grid

8.1 Introduction

8.1.1 Overview

Transmission system is one of the most important assets in secure power delivery. Recent advancements toward automation of smart grids and application of supervisory control and data acquisition (SCADA) systems have increased vulnerability of power grids to cyberattacks. Cyberattacks on transmission network, specifically the power transmission lines, are among crucial emerging challenges for the operators. If not identified properly and in a timely fashion, they can cause cascading failures leading to blackouts. This chapter tackles false data injection modeling from the attacker's perspective. It further develops an algorithm for detection of false data injections in transmission lines. To this end, first, a bi-level mixed integer programming problem is introduced to model the attack scenario, where the attacker can target a transmission line in the system and inject false data in load measurements on targeted buses in the system to overflow the targeted line. Second, the problem is analyzed from the operator's viewpoint and a detection algorithm is proposed using l_1 norm minimization approach to identify the bad measurement vector in data readings. In order to evaluate the effectiveness of the proposed attack model, case studies have been conducted on IEEE 57-bus test system.

In recent years, as online monitoring devices have widely being developed and implemented in smart grids, cybersecurity has also become a more serious issue to be tackled. In addition, interconnection of power systems in different areas and development of advanced communication technologies to automate smart grid assets have made the grid more vulnerable to cyber-physical attacks. A cyberattacker can therefore inject computer viruses or anomalies to endanger the security and resiliency of the smart grid system [1–4]. Example of such attach includes Russian's cyberattack on obtaining detailed data on nuclear power plants and water facilities in the USA in 2018 [6]. Another real-world example is the successful cyberattack by Russian hackers in December 2015 on the Ukraine power grid. In this cyberattack, 30 substations were switched off by hackers which resulted in a power outage of 1–6 h for almost 230,000 people [7].

Transmission lines are the most important assets in power delivery in smart grids, and if failed, can cause serious cascading problems leading to blackouts. One example of such cascading failure was a blackout in Italy that happened in 2004

[8]. Cyberattacks on transmission lines are normally designed to overflow a line or series of lines with the aim of cascading failures. Such transmission line congestion can be achieved if an attacker injects false data on load measurements without being detected by bad data detection algorithms in state estimation process. Recent studies show that by having information on the topology of the system, these false data injections can be designed in a way to bypass state estimation methods without being detected [9–11]. Thus, to protect the smart grid against these vulnerabilities and increase the resiliency of the system, it is crucial to understand the problem from attacker's point of view and develop models that account for various attack scenarios in transmission line congestion.

A few studies developed models for false data injection attacks with the aim of bypassing state estimation in smart grids [12–17]. For instance, [12] extensively modeled false data injection attacks which could not be detected by DC state estimation algorithms. It was shown that if the injected false values in load buses follow system's admittance matrix (B), the attack can be successful. To identify the worst attacking strategy in false data injection attacks, a heuristic algorithm was developed in [14]. Furthermore, an attack model was formulated in [16] that would allow the attacker to make profits in real-time markets. Moreover, a comparison between few bad data detection algorithms were reported in [17]. Although these studies provided a full insight to false data injection problems in smart grids, they did not focus on transmission line congestion and also would require the attacker to have complete access to the system, which was not realistic.

There are also several studies which aimed to generalize false load data injection attacks by focusing on incomplete power system models and limited access by the attackers [18–22]. For example, a practical model on false data injection attack was introduced in [19]. Physical constraints of the smart grid system were considered to formulate the model. The model was developed based on the fact that the attackers could not alter the generator output powers. As a result, the power balance needed to be met continuously. Furthermore, an attack model was developed in [18], which only relied on the data and the topology of a local targeted region that could bypass the bad data detection algorithm. Recent studies showed that mixed integer linear programming (MILPs) modeling of the cyberattacks is the most suitable and practical modeling procedures for false data injection attacks [19, 21]. Several studies introduced MILP attack models to initially maximize the system costs [20, 22]. Nevertheless, the main focus of these studies were on attacks which maximized the system costs, and attacks on transmission lines' congestion were not considered.

In [23], in order to overflow transmission lines, a tri-level MILP solution was developed. This model took into account the security constrained economic dispatch problem to find an optimal strategy to overflow multiple targeted transmissions lines through data falsification. Although this model is effective for the scenario in which attacker has access to all lines, in realistic scenarios attacker does not have access to all buses. Due to complexity of tri-level model, it increases the complexity of protection schemes as well. In order to tackle the complexity issues regarding the

model in [23], a bi-level MILP model was proposed in [24]. This model also ignored some practical limits. Optimal injection on load buses was not modeled in this study, i.e., there is no specific strategy to choose the most vulnerable bus from attacker's perspective. In practice, this may not be possible due to limited access to a part of network.

This study addresses two cybersecurity problems from two completely different perspectives: (1) optimal attack strategy from the attacker's viewpoint, (2) state estimation to identify bad data injection considering presence of cyberattacks from operator's viewpoint. The main advantages of the presented MILP approach for the attacker are:

- Optimizing false data injections rather than number of target buses to achieve a more realistic attack model to overflow the transmission lines.
- Restricting transmission line overflow to a certain upper limit to prevent unrealistic spike in line flow, e.g., two times as compared with normal operating scenario in some cases [24].
- Making the realistic assumption that all lines/buses may not be accessible to the attacker. To this end, our model assumes attacking to a target load bus without being detected by the operator.
- Developing a bi-level MILP model as an alliterative to tri-level methods. This simplifies protection scheme in resilient power system studies. Further, we have included load injection limits to outperform the bi-level model in [24].

More importantly, this chapter proposes a detection framework that identifies the false data injections in smart grids, this has never been studied in the existing literature.

The organization of this chapter is as follows. Section 8.2 provides the preliminaries regarding DC power flow model. Section 8.3 explains the false data injection attacks and their effect on smart grid state estimation. Section 8.4 explores a bi-level MILP model to find the optimal strategy of an attacker in transmission networks. Section 8.5 is devoted to the operator's strategy for bad data injection identification using sparsity-based decomposition. Section 8.6 includes the case studies on IEEE 57-bus benchmark model, followed by Sect. 8.7 that concludes the paper. The overall structure of this study is provided in Fig. 8.1.

8.2 DC Power Flow Model

Here, we provide the preliminaries for DC power flow formulation. This notation is used both for finding the optimal cyberattack strategy for the attacker and developing a bad data detection method for the operator.

The following assumptions are made due to the physical characteristics of transmission networks to obtain linear DC power flow formulation as opposed to nonlinear AC power flow model:

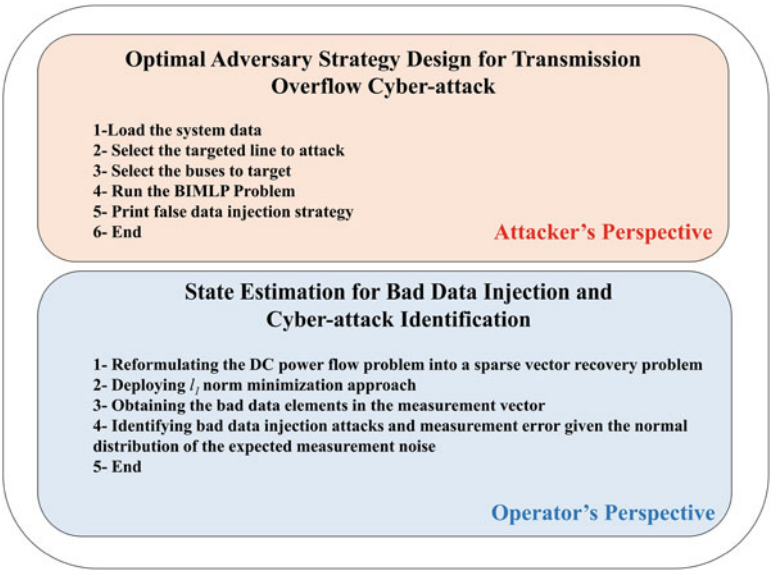

Fig. 8.1 Overall structure of this study: exploring the cyberattack from attacker's and operator's perspectives

1. Due to the high X/R ratio in transmission networks, only the inductive component of impedance is considered [25], i.e., $R_{ij} = 0$ for all lines.
2. Voltage mismatch among neighboring (connected) buses is negligible, i.e., $\delta_i - \delta_j \approx 0$; hence, we can make the following approximations $\cos(\delta_i - \delta_j) \approx 1$ and $\sin(\delta_i - \delta_j) \approx 0$.
3. Due to the low voltage deviation in transmission networks, all voltage magnitudes are set to 1 p.u.

Newton–Raphson power flow method is the most suitable approach to solve the power flow equations due to its quadratic convergence. DC power flow is a simplified version of decoupled power flow by further dropping the $Q - |V|$ equations and assuming a constant voltage profile for all the buses in the system. Therefore, it is assumed that $|V_i| = 1$ p.u. for all the buses. Assuming the system has N buses and bus number 1 is the slack bus (e.g., $V_1 = 1\angle 0$ p.u.), the decoupled power flow can be modeled by

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} J_1 & 0 \\ 0 & J_4 \end{bmatrix} \begin{bmatrix} \Delta\theta \\ \Delta|V| \end{bmatrix} \tag{8.1}$$

where $\Delta P = [\Delta P_2, \Delta P_3, \ldots, \Delta P_N]$ and $\Delta Q = [\Delta Q_2, \Delta Q_3, \ldots, \Delta Q_N]$ are vectors representing the mismatch between the scheduled and calculated active/reactive powers (e.g., $\Delta P_i = P_i^{\text{sch}} - P_i^{(k)}$, $\Delta Q_i = Q_i^{\text{sch}} - Q_i^{(k)}$), J_1 and J_4 are elements of Jacobean matrix represented by

$$J_1 = \begin{bmatrix} \frac{\partial P_2}{\partial \theta_2} & \cdots & \frac{\partial P_2}{\partial \theta_N} \\ \vdots & \ddots & \vdots \\ \frac{\partial P_N}{\partial \theta_2} & \cdots & \frac{\partial P_N}{\partial \theta_N} \end{bmatrix}, \quad J_4 = \begin{bmatrix} \frac{\partial Q_2}{\partial |V|_2} & \cdots & \frac{\partial Q_2}{\partial |V|_N} \\ \vdots & \ddots & \vdots \\ \frac{\partial Q_N}{\partial |V|_2} & \cdots & \frac{\partial Q_N}{\partial |V|_N} \end{bmatrix} \tag{8.2}$$

Disregarding the resistance of transmission lines, this model can be further simplified to the DC power flow formulation as,

$$\begin{bmatrix} \Delta P_2 \\ \vdots \\ \Delta P_N \end{bmatrix} = \begin{bmatrix} B_{11} & B_{12} & B_{13} & \ldots & B_{1N} \\ B_{21} & B_{22} & B_{23} & \ldots & B_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ B_{N1} & B_{N2} & B_{N3} & \ldots & B_{NN} \end{bmatrix} \begin{bmatrix} \Delta \theta_2 \\ \vdots \\ \Delta \theta_N \end{bmatrix} \tag{8.3}$$

where $B_{ik} = -\frac{1}{x_{ik}}$ and $B_{ii} = \sum_{i=1}^{N} \frac{1}{x_{ik}}$, and x_{ik} is the reactance of the transmission line between bus i and bus k. In a matrix form, the DC power flow is formulated as

$$P - D = B\theta \tag{8.4}$$

where P is the vector of generated active powers and D is the demand vector in the system. The power flow in transmission lines between bus i and k using DC power flow is formulated by

$$P_{ik} = \frac{1}{x_{ik}}(\theta_i - \theta_k) \tag{8.5}$$

8.3 False Data Injection Attacks Based on DC State Estimation

In smart grids, the supervisory control and data acquisition is in charge of estimating the parameters of the system based on received phasor measurement unit (PMU) measurements. This is mainly to ensure an error-free measurement by running a bad data detection algorithm in state estimation process. State estimation is the process of using sample measurements to calculate the values of state variables in power systems. In DC power flow, since the only variables are bus voltage angles, the objective of state estimation is to estimate the bus voltage angles using measured values. The maximum likelihood criterion is normally used to estimate the parameters of the system in this case. The objective of maximum likelihood criterion is to maximize the probability that estimated value ($\hat{x}$) is the true value of the state variable x. This can be formulated as

$$P(\hat{x}) = x \tag{8.6}$$

In the maximum likelihood criterion, it is assumed that the probability density function (PDF) of the random measurement errors is known. However, if the PDF of sample measurements is assumed to follow a normal (Gaussian) distribution function, the least square estimates can be used to estimate the states of the system [26]. Therefore, if a single parameter, θ, is to be estimated using N_m measurements, the objective is to [26]

$$\min \sum_{i=1}^{N_m} \frac{\left[\theta_i^{\text{meas}} - f_i(\theta)\right]^2}{\sigma_i^2} \tag{8.7}$$

where $f_i(\theta)$ is the function used to calculate the bus voltage angles, which is equal to $H\theta$ in DC power flow. It is noted that H is an $N_m \times N_s$ matrix of the coefficients of linear function $f_i(\theta)$ and is related to transmission line reactances. Furthermore, σ_i^2 is the variance of ith measurement, θ_i^{meas} is the measured bus voltage angle, and N_m is the total number of measurements in the system. By converting (8.7) to matrix form, the problem can be written as [26]

$$\min J(\theta) = [\theta^{\text{meas}} - H\theta]^T W^{-1} [\theta^{\text{meas}} - H\theta] \tag{8.8}$$

where $J(\theta)$ is the measurement residual, and θ^{meas} and W are defined as

$$\theta^{\text{meas}} = \begin{bmatrix} \theta_1^{\text{meas}} \\ \theta_2^{\text{meas}} \\ \vdots \\ \theta_{N_m}^{\text{meas}} \end{bmatrix}, W = \begin{bmatrix} \sigma_1^2 & & & \\ & \sigma_2^2 & & \\ & & \ddots & \\ & & & \sigma_{N_m}^2 \end{bmatrix} \tag{8.9}$$

To find the minimum of $J(\theta)$ in (8.8), the gradient of measurement residual must be zero (e.g., $\nabla J(\theta) = 0$), this will result in a solution of estimated values

$$\hat{\theta} = [H^T W^{-1} H]^{-1} H^T W^{-1} \theta^{\text{meas}} \tag{8.10}$$

After deriving the estimated values, the SCADA system normally runs a bad data check to calculate the two-norm value of the mismatch between the estimated values and measured values. If the error is greater than the threshold, the bad data is detected. It was proved in [23] that an attacker can bypass the bad data detection algorithm if the false data is designed to satisfy

$$\Delta z = H \Delta\theta \tag{8.11}$$

where $\Delta\theta$ is the change in the bus voltage angles, and Δz is the change in the measurement vector due to the false data injection.

It should be noted that the successful attack might not be guaranteed, this is because of the fact that after the false data injections, the control center should adjust the generation powers for an optimal power flow that results in a lower system cost. The economic dispatch problem will then be run in presence of false data injection, which results in a new transmission flow that deviates from normal load flow results. Since the economic dispatch might have multiple solutions, the success of attack cannot be guaranteed [23]. The main assumptions for false data injection attacks due to system limitations can be listed as [27]:

- The synchronous generator readings cannot be altered
- The measurement tampering on each load is limited within its nominal rating
- Power balance, which is a mismatch between the generation and load, should always be met

These limitations will mathematically be modeled and included in the cyberattack problem to be formulated in the next section. It is also assumed that the attacker has limited access to the system buses for false data injection. Therefore, a subset of all system buses (F) that the attacker can access is defined to highlight the fact that the attack can only be done on the subset. In addition, to avoid supply–demand violation, sum of injected powers by the attacker has to be zero, this can be formulated as

$$\sum_{i \in F} \Delta D_i = 0 \tag{8.12}$$

where ΔD_i is false active power injection at bus i. To account for limited injection on each measurement, a new constraint has to be defined,

$$-\tau D_i \leq \Delta D_i \leq \tau D_i \tag{8.13}$$

where τ is the limit on the maximum injection and is considered as 15% in this study, and D_i is the nominal load at bus i.

8.4 Attacker's Problem: Finding the Optimal Set of Target Transmission Lines using MILP

In this section, the attacker's problem is modeled as a bi-level mixed integer linear programming (MILP) optimization model, where an attacker can target a transmission line and overflow the targeted line by injecting false data on targeted buses. The assumption is that the attackers have enough information on topology of the system to conduct attacks; however, they might not have access to all buses in the system. The attacker's problem is designed in a way that the transmission flow of a targeted line always exceeds the maximum thermal limit of the line after running the security constraint economic dispatch problem. As a result, regardless

of the economic dispatch solution (it might have multiple solutions), the targeted line will always be overflowed. Another assumption of this problem is that all generating units are online in the period of false data injection. Thus, instead of unit commitment, economic dispatch is formulated.

$$\min \sum_{i \in F} \Delta D_i \tag{8.14}$$

$$s.t. \quad P_{ij}^t + U_i M \geq \alpha P_{ij}^{\max} \tag{8.15}$$

$$-P_{ij}^t + (1 - U_i) M \geq \alpha P_{ij}^{\max} \tag{8.16}$$

$$-1.2 \leq \frac{P_{ij}^t}{P_{ij}^{\max}} \leq 1.2 \tag{8.17}$$

$$\sum_{i \in F} \Delta D_i = 0 \tag{8.18}$$

$$-\tau D_i \leq \Delta D_i \leq \tau D_i \tag{8.19}$$

$$P - (D + \Delta D) = B\theta^t \tag{8.20}$$

$$P_{ij}^t = \frac{\theta_i^t - \theta_j^t}{x_{ij}} \tag{8.21}$$

$$-2\pi \leq \theta_i^t \leq 2\pi \tag{8.22}$$

$$\min \sum_{i=1}^{n_G} C_{g,i}(P_{G,i}) \tag{8.23}$$

$$s.t. \quad C_{g,i}(P_{G,i}) = a_i + b_i P_{G,i} + c_i P_{G,i}^2 \tag{8.24}$$

$$P - (D + \Delta D) = B\theta^f \tag{8.25}$$

$$P_{G,i}^{\min} \leq P_{G,i} \leq P_{G,i}^{\max} \tag{8.26}$$

$$-P_{ij}^{\max} \leq \frac{\theta_i^f - \theta_j^f}{x_{ij}} \leq P_{ij}^{\max} \tag{8.27}$$

The developed MILP problem is separated into two sub-problems known as upper level and lower level problems. The upper level problem formulates the attack using a given power flow results and outputs the injection vector on targeted lines to ensure bypassing the bad data detection method in DC optimal power flow. The lower level problem formulates the DC economic dispatch problem with false data injections to retain the operation of power system within the desired limits. The problem is shown in (8.14)–(8.27).

The upper level objective function (8.14) is designed to find the minimum injections needed in a subset of targeted buses (F). The main target of the attacker is to overflow a targeted transmission line, it is also noted that the transmission line flow can be bi-directional, this can be formulated as

$$|P_{ij}^{t}| \geq \alpha_l P_{ij}^{\max} \tag{8.28}$$

where $|P_{ij}^{t}|$ is the transmission flow between bus i and j, the absolute value is used to reflect the fact the flow can be bi-directional, $P_{ij}^{\max}$ is the maximum thermal limit of the line between bus i and j, and α is a number greater than 1 to ensure the transmission line flow will be greater than the limit. Due to the existence of absolute value in the constraint (8.28), the problem becomes nonlinear. To solver the issue, this constraint can be linearized by introducing a binary variable U_i and a large enough constant M. The linearization will result in two constraints shown in (8.15) and (8.16). The readers are encouraged to refer to [28] for more information on linearizing the constraints with absolute value using the big M method.

Constraint (8.17) enforces the overflow to be within 20% of maximum power flow, although the main target is to overflow a line, to avoid being detected by the operator, the max flow should be limited. Constraint (8.18) is designed to ensure the power balance is always met; therefore, summation of all the injections should be zero at any moment. Constraint (8.19) refers to the fact that an attacker cannot inject any amount of data at any load bus; therefore, the false injected power at any bus is limited to $\tau\%$ of the nominal load at that bus. Constraint (8.20) ensures bypassing the bad data detection. As it was mentioned in (8.11), the attacker can bypass the DC state estimation without being detected if the injected data is designed based on (8.11). By rearranging (8.20),

$$(P - D) + \Delta D = B\theta + B\Delta\theta \tag{8.29}$$

where $\Delta\theta$ is the change in the bus voltage angles due to false data injection. Knowing the fact that $P - D = B\theta$, (8.29) can be simplified to (8.11). Constraints (8.21) and (8.22) relate the transmission flow to maximum allowable limits of bus voltage angles. The lower level problem is the economic dispatch problem based on DC power flow, which is formulated through (8.23)–(8.27). In the lower level problem, the objective is to minimize the generation cost for all n_G generators in the system. It is assumed that the generating units do not contain several control valves. Hence, the "convex" cost function of the generators is represented by $a_i + b_i P_{G,i} + c_i P_{G,i}^2$, where $P_{G,i}$ is the active power generated by generator i, and a, b, and c are cost function constants (constraint (8.24)). Constraint (8.25) represents the power balance equation in presence of false data injection, constraints (8.26) and (8.27) ensure the generator powers and transmission line flows are within the limit after injection, where x_{ij} is the reactance of the transmission line between bus i and j.

8.4.1 *Identifying Feasible Attacks*

Realistically, physical limitations of power systems and solution of economic dispatch problem limit the feasibility of the attacks from attacker's point of view. In other words, it is impractical to target all the transmission lines in the system and only a few lines might be practically targeted at any moment. Therefore, the attacker's first step is to recognize the feasible attacks and then inject data on selected buses (targeted buses) to overflow those lines that can result in a feasible solution. An algorithm is defined to identify the feasible solution of overflowing transmission lines in the system. The model requires the power flow data from previous step to result in a successful subset of transmission line numbers that can be targeted without violating the bad data detection algorithm in state estimation procedure. The flowchart of the proposed algorithm that results in feasible solutions of the line overflows is shown in Fig. 8.2.

8.5 Operator's Problem: Bad Data Detection to Prevent Outages Caused by Cyberattack

In the previous section, we explained the algorithm for finding the optimal attack strategy from attacker's perspective. Successful attack will affect the result of DC power flow problem. Power system operator is responsible for maintaining situational awareness, as well as ensuring resilient and secure energy delivery by identifying these attacks and deploying preventive measures [29]. In this section, we focus on a specific algorithm to identify bad data injection attacks, i.e., attacks that manipulate the measurement vector to falsify the real values used for DC power flow calculation in transmission networks. The main idea is to design a state estimator which is robust to error/attack in the measurement vector while obtaining the power flows. This estimator leverages the structure of admittance matrix to efficiently identify bad data injection attacks.

The following section is devoted to the details of this state estimator. To this end, we build on the proposed sparsity-based error detection algorithm proposed in [30]. This algorithm leverages the singularity of B matrix due to the geographically dispersed transmission networks, as well as the sparse nature of estimation error vector. Sparsity-based cyberattack detection algorithm is based on the following steps:

1. Reformulating the DC power flow problem into a sparse vector recovery problem
2. Deploying l_1-norm minimization approach [31]
3. Obtaining the bad data elements in the measurement vector
4. Identifying bad data injection attacks and measurement error given the normal distribution of measurement noise

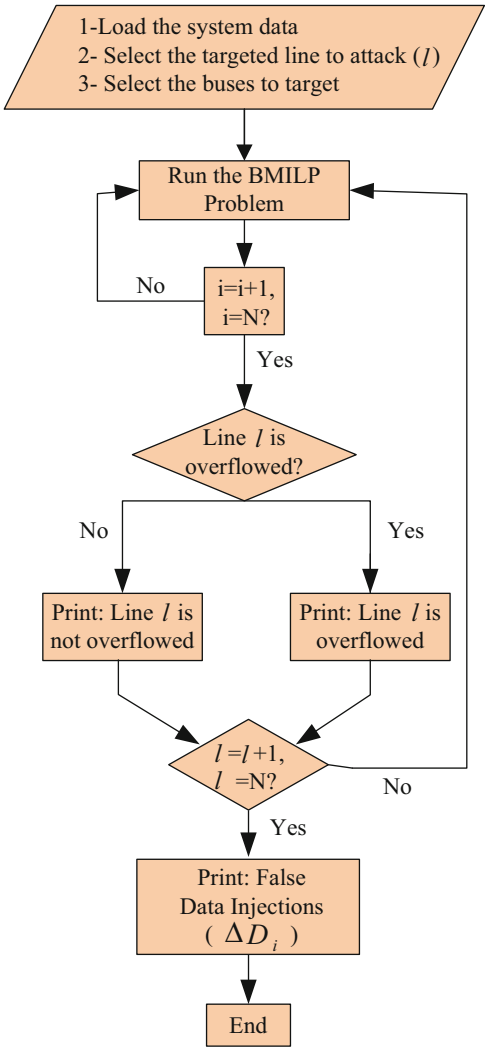

Fig. 8.2 Flowchart of the proposed BMILP program for line overflow feasibility in

There is a low dimensional structure in most of the collected data and measurements in real-world applications, including DC power flow problem. This has been leveraged by some of the prior studies to improve sparse vector recovery [31, 32], e.g., they have explored sparse vector recovery in case of having limited available measurements. In order to recover an N-dimensional sparse vector, these algorithms do not necessarily require N data points [32, 33].

Candes et al. [32] proposed a sparse vector recovery algorithm that only needs a minor portion of random orthogonal projection [30]. Let $\mathbf{v} \in \mathbb{R}^N$ denote an arbitrary sparse vector with its number of non-zero components defined as l_0-norm, i.e., $\|\mathbf{v}\|_0$. We define set of orthonormal basis matrix as $\mathbf{O} \in \mathbb{R}^{N \times N}$. We have

$$\mathbf{O}^T\mathbf{O} = \mathbf{I}, \tag{8.30}$$

where $\mathbf{I}$ represents identity matrix. We represent a set of random columns from $\mathbf{O}$ as $\mathbf{M} \in \mathbb{R}^{N\times m}$. We further let μ denote the lowest value that meets the following inequality:

$$\max_i \|\mathbf{M}^T\mathbf{e}_i\|_2 \leq \frac{\mu m}{N}, \tag{8.31}$$

where e_i denotes a standard basis. Note that the dimension of space is $N \times m$. Small values of μ refers to the fact that the subspace corresponding to columns of $\mathbf{M}$ is not in the same direction as standard basis. The orthogonal matrix $\mathbf{M}$ is used to measure the sparse vector. As we use this matrix to measure sparse vector, it should not be sparse.

According to [32], if

$$m \geq c\|\mathbf{v}\|_0 \mu \log\frac{N}{\delta} \tag{8.32}$$

where c is a constant, then, solution of following optimization problem

$$\begin{aligned} \min_{\hat{\mathbf{z}}} \quad & \|\hat{\mathbf{z}}\|_1 \\ \text{subjectto} \quad & \mathbf{M}^T\hat{\mathbf{z}} = \mathbf{M}^T\mathbf{v} \end{aligned} \tag{8.33}$$

is the same as $\mathbf{v}$ with a lower probability bound of $(1-\delta)$, i.e., we can reconstruct the N-dimensional vector given a limited set of random measurements [34].

Given the above-mentioned preliminaries on sparse vector recovery, we now explain the sparsity-based decomposition algorithm for bad data injection in DC power flow calculation [30]. In the B matrix, due to the row corresponding to slack bus, there is at least one row which can be obtained as linear combination of the other rows, i.e., B matrix is not full rank. Let r_B denote rank of B matrix. Hence, we can reformulate DC power flow problem as $\mathbf{p} = \mathbf{Q}\theta + \epsilon$, where $\mathbf{Q} \in \mathbb{R}^{\aleph\times r_B}$ represents orthonormal basis for column subspace of B matrix. Conventionally, in order to estimate the coefficient vector, which is equivalent to the voltage angles vector in DC power flow problem (i.e., θ) least square approach is used as follows:

$$\min_{\hat{\theta}} \|\mathbf{p} - \mathbf{Q}\hat{\theta}\|_2 \tag{8.34}$$

The optimization problem in (8.34) basically projects $\mathbf{p}$ on the columns subspace of $\mathbf{Q}$. Hence, the effectiveness of the estimator depends on the noise vector ϵ and its projection on column subspace of B matrix. Note that noise vector aims at modeling the natural measurement noise in normal situation. However, in presence of attackers (e.g., the attack scenario that has been introduced in previous section) or measurement anomalies (e.g., communication failure or defective equipment), some elements of this vector will have abnormal value.

We assume that the error/attack vector ϵ is a sparse vector, i.e., attackers cannot manipulate all measurements at the same time. As opposed to l_2-minimization, l_1-minimization methods are adaptive in presence of sparse error/attack vector [34, 35], i.e., if ϵ is sufficiently sparse and $\mathbf{Q}$ meets incoherency criterion [31, 35], solution of

$$\min_{\hat{\theta}} \|\mathbf{p} - \mathbf{Q}\hat{\theta}\|_1 \tag{8.35}$$

is θ.

In the proposed sparsity-based decomposition algorithm in [30], based on the sparsity assumption for B matrix, $r_B < \aleph$. If $\mathbf{Q}^{\perp} \in \mathbb{R}^{\aleph \times (\aleph - r_B)}$ represent the matrix that complements the column subspace of $\mathbf{Q}$, according to [31, 35], we can rewrite (8.35) as

$$\begin{aligned} &\min_{\hat{\epsilon}} && \|\hat{\epsilon}\|_1 \\ &\text{subjectto} && (\mathbf{Q}^{\perp})^T \hat{\epsilon} = (\mathbf{Q}^{\perp})^T \mathbf{p} \end{aligned} \tag{8.36}$$

If the following inequality holds,

$$(\aleph - r_B) \geq c\|\epsilon\|_0 \mu_B \log \frac{N}{\delta} \tag{8.37}$$

then, with a lower bound probability of $(1 - \delta)$, the optimal solution of (8.36) is θ, where μ_B is obtained using the following:

$$\max_i \|(\mathbf{Q}^{\perp})_i^T\|_2 \leq \frac{\mu_B(\aleph - r_B)}{\aleph} \tag{8.38}$$

Consequently, given the assumption regarding low rank of B matrix ($(\aleph - r_B)$ is fairly large), the optimization problem in (8.35) can find the exact estimation.

8.6 Case Studies

The proposed BMILP cyberattack model is validated in IEEE 57-bus benchmark model using MATLAB. The parameters of the system are derived from MATPOWER toolbox, which is an open access MATLAB toolbox used for load flow studies [36]. The maximum flow limits ($P_{ij}^{\max}$) for IEEE 57-bus system were not provided in the toolbox, and it was considered to be 120 MW for each transmission line. The structure of the system is illustrated in Fig. 8.3, the system is composed of 7 generators, 80 transmission lines, and 42 loads. The upper level problem for best scenario false data injection attacks represented in (8.14)–(8.22) is solved using ("intlinprog") function of MATLAB, which is designed to solve mixed integer linear

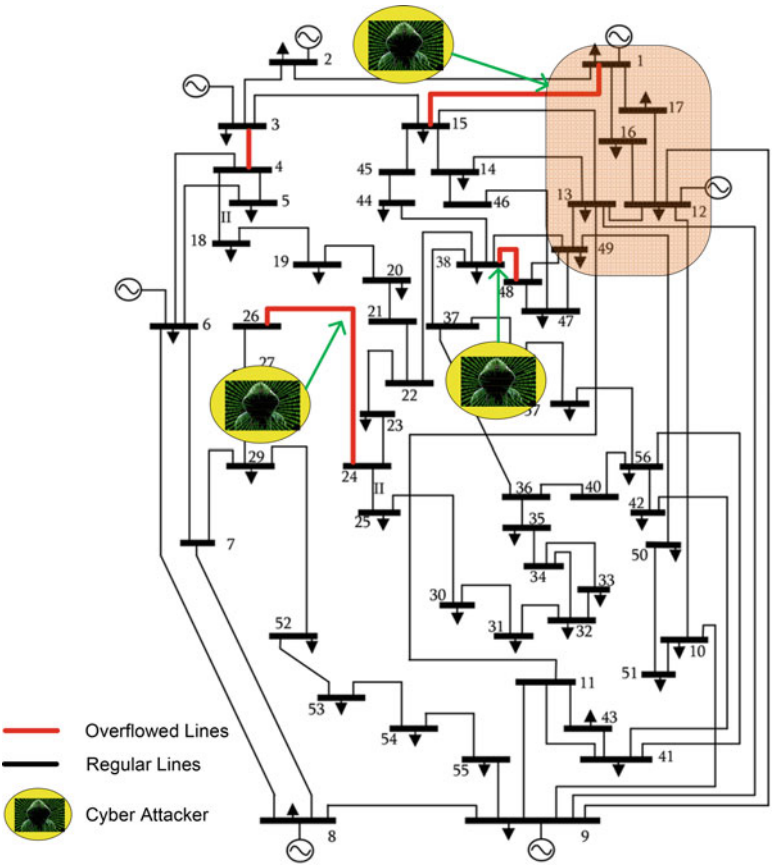

Fig. 8.3 Schematic of the IEEE 57-bus system studied in this work; transmission lines highlighted by red color indicate the potential lines that can be targeted by attackers. The highlighted area is used to illustrate the effect of gaining access to a complete area in the system

programming problems. The lower problem represented in (8.23)–(8.27) involves a nonlinear objective function and therefore, a nonlinear solver of MATLAB named ("fmincon") is used to solve the lower level problem. A few case studies are carried out in the following sections.

8.6.1 Feasibility of Line Overflow

Due to the physical limitations imposed on cyberattacks and false data injections, the attackers cannot target any transmission line in the system. For example, the factor τ limits the injection on each load to 15% in this study. Furthermore, the

Table 8.1 Feasibility of line overflow in IEEE 57 case

Line number	From bus	To bus	U_i
3	3	4	0
15	1	15	1
37	24	26	0
79	38	48	1

flow of a line cannot exceed 120% of the maximum limit (1.2×120 MW). These limitations will leave the attackers with few options to overflow. The proposed attack model in (8.14)–(8.27) can be run for all the buses in the system in order to identify a list of transmission lines that can be overflowed successfully. In this case study, the algorithm was run for all 80 transmission lines in the IEEE 57-bus system to identify a list of lines to be targeted for overflowing. To solve this problem, the objective function in (8.14) is run for all buses in the system instead of a subset F of system buses. This means, the subset F is considered as $i = 1, 2, \ldots, 57$.

Test results for the list of feasible attacks on targeted transmission lines to overflow in IEEE 57-bus system are illustrated in Table 8.1. It is seen that four transmission lines can be targeted in this system by attackers, which includes transmission lines number 3, 15, 37, and 79. The second and third column represent that each line number is assigned based on the MATPOWER data from one bus to another, and the last column shows the value of the binary variable for overflowing the line (U_i). These transmission lines are highlighted by red color in IEEE 57-bus system depicted in Fig. 8.3. It is worth mentioning that the results in Table 8.1 are only valid for the conditions considered in this case (e.g., $\tau = 15\%$, $\alpha = 1.01$). Therefore, the results might change if the security constraints in (8.15), (8.16), and (8.19) are relaxed.

8.6.2 Targeted Attack on Line 15

This case investigates targeted attacks to overflow transmission line number 15, which connects bus 1 to bus 15 in IEEE 57-bus system as shown in Fig. 8.3. Since the attacks are targeted, the attacker can target any set of buses to inject false data and overflow this line. Ideally, the attacker would access buses close to the targeted line and inject data. A few set of feasible solutions to overflow line number 15 is shown in Table 8.2. Three different combinations are considered to overflow line 15, in the first scenario, the attacker targets buses 12, 44, 47, and 49 that are very close to the targeted transmission line. In the second case, the attacker targets buses 8, 9, and 12, and finally, it is shown that if the attacker only targets buses 9 and 12, the attack can successfully be done. Table 8.2 shows the attack results for these three test scenarios. It is noted that the attackers target specific buses in the system that they can access and the program outputs the minimum injections needed to

Table 8.2 False data injection on buses to overflow line 15

(Case 1 buses)	ΔD	(Case 2 buses)	ΔD	(Case 3 buses)	ΔD
12	−11.94 MW	8	−5.62 MW	9	24.2 MW
44	2.4 MW	9	24.2 MW	12	−24.2 MW
47	5.94 MW	12	−18.58 MW		
49	3.6 MW				
P_{15}	121.49 MW	P_{15}	121.2 MW	P_{15}	121.5 MW
Cost (no attack)	$45,342	Cost (no attack)	$45,342	Cost (no attack)	$45,342
Cost (with attack)	$45,938	Cost (with attack)	$45,108	Cost (with attack)	$44,902

Table 8.3 False data injection on buses to overflow one area

Targeted buses	ΔD	Targeted buses	ΔD
1	−11 MW	12	28 MW
13	−3.6 MW	16	−8.4 MW
17	−8.6 MW	49	3.6 MW
P_{15} = 125.9 MW			
Cost (no attack) = $ 45,342			
Cost (with attack) = $ 45,685			

overflow the targeted transmission line. It is observed that the targeted line 15 is overflowed in all three cases as its power flow (P_{15}) is more than 120 MW limit. The last two columns show the cost of the system with no attack and after attack, it can be inferred from the Table 8.2 that in case 2 and 3, the system cost is less with data injections, compared to the no data injection case, which might trick the operator to choose this scenario as an acceptable economic dispatch case study.

8.6.3 Severe Attack on an Area

This case study considers a severe false data injection attack, where the attacker(s) can access an area in the power system and can inject false data in any bus within that area. This concept is illustrated in the highlighted area shown in Fig. 8.3. The attacker targets line 15 and injects data on buses 1, 12, 13, 16, 17, and 49 within the area. Results of false data injection on the whole area are illustrated in Table 8.3. The false data injections are also shown in second and fourth column for each bus. It is observed that the attack can successfully overflow line 15 and the cost of operation has also increased after the attack.

8.7 Conclusion

In this chapter, a framework was proposed to initially model the false data injection attacks on smart grids with the aim of transmission line congestion on targeted buses and eventually proposed a detection framework to detect such injections. A bi-level mixed integer programming problem was considered for the attacker's problem that would allow attackers to target a transmission line in the system and inject false data on targeted buses in vicinity of the targeted transmission line to cause congestion without being detected by DC state estimation algorithm. Through case studies, it was shown that the proposed attack model results in a list of available transmission lines to overflow. Furthermore, it was shown that the attacker can inject false data on selected buses or buses in a hacked area in the system to overflow a targeted

line. To detect these attacks, a detection framework from operator's point of view is also developed that uses l_1 norm minimization to identify the bad measurement vector. The proposed model can easily be integrated to the security constraint economic dispatch problem in order to protect the smart grid against transmission lines congestion cyberattacks. Future research will focus on (1) validating the detection algorithm in IEEE benchmarks, (2) proposing a framework that would protect the system against congestion attacks on multiple lines at the same time, and (3) introducing market frameworks in which market participants can gain profit by contributing to mitigation of system congestion caused by cyberattacks.

Acknowledgements This work was under support from Penn State's Center for Security Research and Education (CSRE) seed grant 2019.

References

1. X. Yu, Y. Xue, Smart grids: a cyberphysical systems perspective. Proc. IEEE **104**(5), 1058–1070 (2016)
2. M.H. Cintuglu, O.A. Mohammed, K. Akkaya, A.S. Uluagac, A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials **19**(1), 446–464 (2017)
3. H. Chung, W. Li, C. Yuen, W. Chung, Y. Zhang, C. Wen, Local cyber-physical attack for masking line outage and topology attack in smart grid. IEEE Trans. Smart Grid **10**, 4577–4588 (2019)
4. A. Imteaj, M.H. Amini, J. Mohammadi, Leveraging decentralized artificial intelligence to enhance resilience of energy networks (2019). arXiv preprint arXiv:1911.07690
5. Y. Tang, Q. Chen, M. Li, Q. Wang, M. Ni, and X. Fu, Challenge and evolution of cyber attacks in cyber physical power system, in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)* (IEEE, Xi'an, 2016), pp. 857–862
6. N. Perlroth, D.E. Sanger, Cyberattacks put Russian fingers on the switch at power plants, US says. New York Times **15** (2018)
7. T. Maurer, *Cyber Mercenaries* (Cambridge University Press, Cambridge, 2018)
8. Y. Cai, Y. Cao, Y. Li, T. Huang, B. Zhou, Cascading failure analysis considering interaction between power grids and communication networks. IEEE Trans. Smart Grid **7**(1), 530–538 (2015)
9. X. Liu, Z. Li, X. Liu, and Z. Li, Masking transmission line outages via false data injection attacks. IEEE Trans. Inf. Forensics Secur. **11**(7), 1592–1602 (2016)
10. L. Wei, D. Gao, C. Luo, False data injection attacks detection with deep belief networks in smart grid, in *2018 Chinese Automation Congress (CAC)* (2018), pp. 2621–2625
11. Y. Xiang, Z. Ding, Y. Zhang, L. Wang, Power system reliability evaluation considering load redistribution attacks. IEEE Trans. Smart Grid **8**(2), 889–901 (2016)
12. Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. **14**(1), 13 (2011)
13. L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, Z. Han, Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid **5**(2), 612–621 (2014)
14. O. Kosut, L. Jia, R.J. Thomas, L. Tong, Malicious data attacks on the smart grid. IEEE Trans. Smart Grid **2**(4), 645–658 (2011)
15. G. Chaojun, P. Jirutitijaroen, M. Motani, Detecting false data injection attacks in AC state estimation. IEEE Trans. Smart Grid **6**(5), 2476–2483 (2015)
16. L. Xie, Y. Mo, B. Sinopoli, Integrity data attacks in power market operations. IEEE Trans. Smart Grid **2**(4), 659–666 (2011)

17. S. Barreto, M. Pignati, G. Dán, J.-Y. Le Boudec, M. Paolone, Undetectable timing-attack on linear state-estimation by using rank-1 approximation. IEEE Trans. Smart Grid **9**(4), 3530–3542 (2018)
18. X. Liu, Z. Li, Local load redistribution attacks in power systems with incomplete network information. IEEE Trans. Smart Grid **5**(4), 1665–1676 (2014)
19. Y. Yuan, Z. Li, K. Ren, Quantitative analysis of load redistribution attacks in power systems. IEEE Trans. Parallel Distrib. Syst. **23**(9), 1731–1738 (2012)
20. Z. Li, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, Bilevel model for analyzing coordinated cyber-physical attacks on power systems. IEEE Trans. Smart Grid **7**(5), 2260–2272 (2016)
21. M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin, L. Zhao, Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid. IEEE Access **7**, 9836–9847 (2019)
22. J. Liang, L. Sankar, O. Kosut, Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans. Power Syst. **31**(5), 3864–3872 (2016)
23. X. Liu, Z. Li, Trilevel modeling of cyber attacks on transmission lines. IEEE Trans. Smart Grid **8**(2), 720–729 (2017)
24. Y. Tan, Y. Li, Y. Cao, M. Shahidehpour, Cyber-attack on overloading multiple lines: a bilevel mixed-integer linear programming model. IEEE Trans. Smart Grid **9**(2), 1534–1536 (2018)
25. G. Giannakis, V. Kekatos, N. Gatsis, S.-J. Kim, H. Zhu, B. Wollenberg, Monitoring and optimization for power grids: a signal processing perspective. IEEE Signal Process. Mag. **30**(5), 107–128 (2013)
26. A.J. Wood, B.F. Wollenberg, G.B. Sheblé, *Power Generation, Operation, and Control* (Wiley, New York, 2013)
27. Y. Yuan, Z. Li, K. Ren, Modeling load redistribution attacks in power systems. IEEE Trans. Smart Grid **2**(2), 382–390 (2011)
28. G. Dantzig, *Linear Programming and Extensions* (Princeton University Press, Princeton, 2016)
29. A. Gholami, T. Shekari, M.H. Amirioun, F. Aminifar, M.H. Amini, A. Sargolzaei, Toward a consensus on the definition and taxonomy of power system resilience. IEEE Access **6**, 32035–32053 (2018)
30. M.H. Amini, M. Rahmani, K.G. Boroojeni, G. Atia, S.S. Iyengar, O. Karabasoglu, Sparsity-based error detection in dc power flow state estimation, in *2016 IEEE International Conference on Electro Information Technology (EIT)* (IEEE, Grand Forks, 2016), pp. 0263–0268
31. M. Rahmani, G.K. Atia, High dimensional low rank plus sparse matrix decomposition. IEEE Trans. Signal Process. **65**(8), 2004–2019 (2017)
32. E. Candes, J. Romberg, Sparsity and incoherence in compressive sampling. Inverse Probl. **23**(3), 969 (2007)
33. E.J. Candès, J. Romberg, T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory **52**(2), 489–509 (2006)
34. E.J. Candes, T. Tao, Near-optimal signal recovery from random projections: universal encoding strategies? IEEE Trans. Inf. Theory **52**(12), 5406–5425 (2006)
35. E.J. Candes, T. Tao, Decoding by linear programming. IEEE Trans. Inf. Theory **51**(12), 4203–4215 (2005)
36. R.D. Zimmerman, C.E. Murillo-Sanchez, R.J. Thomas, MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. **26**(1), 12–19 (2011)