A Detection Mechanism Against Load-Redistribution Attacks in Smart Grids

Ramin Kaviani, Student Member, IEEE, Kory W. Hedman, Member, IEEE

Abstract—This paper presents a real-time non-probabilistic detection mechanism to detect load-redistribution (LR) attacks against energy management systems (EMSs). Prior studies have shown that certain LR attacks can bypass conventional bad data detectors (BDDs) and remain undetectable, which implies that presence of a reliable and intelligent detection mechanism to flag LR attacks, is imperative. Therefore, in this study a detection mechanism to enhance the existing BDDs is proposed based on the fundamental knowledge of the physics laws in the electric grid. A greedy algorithm, which can optimize the core LR attack problems, is presented to enable a fast mechanism to identify the most sensitive locations for critical assets. The main contribution of this detection mechanism is leveraging of power systems domain insight to identify an underlying exploitable structure for the core problem of LR attack problems, which enables the prediction of the attackers’ behavior. Additional contribution includes the ability to combine this approach with other detection mechanisms to increase their likelihood of detection. The proposed approach is applied to 2383-bus Polish test system to demonstrate the scalability of the greedy algorithm, and it solved the attacker’s problem more than 10x faster than a traditional linear optimization approach.

Index Terms—cyber-attack, false data injection attack (FDIA), load-redistribution attacks detection, greedy algorithm, linear programming (LP)

NOMENCLATURE

Sets and Indices

| Symbol | Description |
|--------|-------------|
| G      | Set of all generation units. |
| g      | Index for generation unit. |
| G(i)   | Set of all generation units at bus i (i ∈ N). |
| i      | Index for bus. |
| K      | Set of all branches. |
| k      | Index for branch. |
| M      | Set of all measurements. |
| m      | Index for measurement. |
| N      | Set of all buses. |

Parameters, Vectors and Matrices

| Symbol | Description |
|--------|-------------|
| α      | Load shift factor. |
| P̄g    | Fixed dispatch point of unit g ∈ G. |
| τ      | Residual-based bad data detector threshold. |
| c_g    | Production cost of unit g ∈ G. |
| e      | n_m × 1 vector of measurement noise error. |
| H      | n_m × n_b Jacobian matrix of the system. |
| H’     | n_b × n_b dependency matrix between power injection measurements and state variables. |
| H’_i   | i_th row of H’ (i ∈ N). |
| L_i    | Fixed active load (MW) at bus i ∈ N. |
| lb_i   | Lower bound for load deviation at each bus i ∈ N. |
| N_i    | Number of states that can be changed by attacker. |
| n_b    | Number of buses. |
| n_m    | Number of measurements. |
| n_br   | Number of branches. |
| P^max_g | Upper limit on generation capacity of unit g ∈ G. |
| P^min_g | Lower limit on generation capacity of unit g ∈ G. |
| P^max_k | Continuous rating of line k ∈ K. |
| PTDF^R_k.i | Power transfer distribution factor for transmission asset k ∈ K and bus i ∈ N (injection) with regard to reference bus R (withdrawal). |
| ub_i   | Upper bound for load deviation at each bus i ∈ N. |
| Z      | n_m × 1 vector of measurements. |

Variables

| Symbol | Description |
|--------|-------------|
| H’_c(L_i) | Active load deviation at bus i ∈ N. |
| x̂      | n_b × 1 vector of estimated state variables. |
| c      | n_b × 1 vector of false data generated by attacker. |
| P_g    | Dispatch point of unit g ∈ G. |
| P_l    | Active power flow on target line l ∈ K. |
| x      | n_b × 1 vector of actual state variables. |

I. INTRODUCTION

In power systems, state estimation (SE) is one of the key functions of EMSs since many real-time operational and market decisions are driven by its results. The SE is the process of using fields’ measurements to estimate systems’ state variables with minimum error. Due to some limitations like sensor calibration error, topology error, data transfer inaccuracy, and cyber-attack, the received measurements (inputs to SE) are not clean (noisy measurements), which would affect the accuracy of the SE process. To reduce the effect of noisy measurements on the SE process, state estimators are equipped with BDDs to flag and remove noisy data.

False data injection attack (FDIA) against SE is a class of cyber-attacks that attempts to maliciously change the measurements and interfere in the SE process by targeting the vulnerability of BDDs. BDDs are not looking for intelligent
attacks; rather, they are looking for physical limitation driven events - measurement errors, faulty equipment, etc. Therefore, it would be an easy task for intelligent attackers to bypass BDDs and remain undetectable. The researchers in [1] – [3] have shown the incapability of BDDs to detect generated FDIAs against both direct current state estimation (DCSE) and alternative current state estimation (ACSE) processes. Likewise, they have addressed the conditions under which a malicious attack could bypass BDDs and remain undetectable, while it has been assumed that the attackers have complete information of the systems. The researchers in [4] have demonstrated that launching an FDIA with the least number of measurements to be compromised without having access to all measurements, is an NP-hard problem. To tackle this issue, authors in [5] – [12] have attempted to generate FDIA with incomplete information about the systems’ topology by applying heuristic methods, greedy algorithms, graph theoretic approaches, and sparse optimization methods. The research study in [13] has illustrated that even without any information about the systems’ topology, attackers could construct undetectable FDIA.

In this study, the focus is on the LR attack, which is a kind of implementing an FDIA. In LR attacks, the attackers attempt to falsify bus injection measurements to either physically or economically damage the systems. Various researchers proposed bi-level or attacker-defender optimization problems to model LR attacks with different objectives like maximizing operation cost or maximizing power flow on a target line [14]– [19]. Authors in [20] modeled a bi-level mixed integer linear programming LR attack to address an LR attack that targets multiple transmission assets. LR attacks with incomplete systems’ information are investigated in [17], [21], [22], where the authors designed a problem to find the best local attacking region.

Such prior research efforts have done a great job demonstrating the vulnerability of traditional BDDs, which were previously designed to detect anomalies caused by some physical limitations. It is easy not to be detected when nobody is looking for you or, in other words, “The greatest trick the devil ever pulled was convincing the world he didn’t exist” [23].

Now, the research community has obviously acknowledged the existence of an attacker and his/her ability to remain undetectable, which has pushed them to seek a solution. In the first place, standing against the intelligent attackers could be started by protecting power systems from FDIAs. Protection refers to some pre-attack actions that make it hard for attackers to launch an FDIA against power systems. In this regard, [24] proposed to place secure PMUs at key buses in the system to defend against FDIAs. Likewise, various techniques from game theoretic models to greedy algorithms are suggested in [25] – [31] for identifying the smallest set of key measurement devices to be protected. However, referring to [32], attackers still could launch an attack even when all measurements have been protected against FDIAs, which implies the demand for an intelligent false data detection scheme. Therefore, designing intelligent false data detectors is the next way to stand against intelligent attackers. Various FDIA detection methods are proposed and developed in [33] – [44] based on various techniques like Kalman filters, adaptive cumulative sum method, low-rank decomposition (LD), Kullback-Leibler distance (KLD), sparse optimization, machine learning, and deep learning.

In this study, we have developed a non-probabilistic detection mechanism based on the fundamental knowledge of the laws of physics and power systems to detect LR attacks against DCSE. This is an online monitoring mechanism that allows operators to track load changes (given a target asset) at each iteration of the EMS and flag malicious or hazardous set of deviations. Our main contributions are:

1) Leveraging power systems domain insight to identify an underlying exploitable structure in LR attack problems, which helps the operator to predict the attackers’ behavior.

2) Mathematically proving the ability of a greedy algorithm to solve the exploitable structure of LR attacks’ problems to optimality, which leads the system operator to find the most sensitive locations at each iteration of EMS very fast even for large interconnections that distinguishes our approach from other approaches.

3) Developing an approach that is able to combine with other approaches (e.g., ones that use machine learning) to increase their likelihood of detection.

This paper is organized as follows. Sec. II presents a short background on DCSE, the condition to launch an undetectable FDIA against DCSE, and LR attacks. Sec. III is divided into two subsections; the first one develops a single level LP problem as the core problem of more sophisticated LR attack problems and the second one provides a mathematical proof to demonstrate the ability of a greedy algorithm to obtain the global optimum for the proposed core problem of LR attack problems. Sec. IV and V present simulation results and concluding remarks, respectively.

II. BACKGROUND

In this section, the DCSE process and the procedure to create an undetectable FDIA against it are described in II-A. Likewise, in II-B an LR-based FDIA is introduced.

A. DCSE and Undetectable FDIA

In the DCSE process, measurements are related to state variables (voltage angles) via linear equations. Eq. (II.1) represents these linear equations in a matrix form:

\[ Z = Hx + e \]  

(II.1)

Where \( Z \) is the \( n_m \times 1 \) vector of measurements, \( x \) is the \( n_o \times 1 \) vector of actual state variables of the system that needs to be estimated, \( H \) is the \( n_m \times n_o \) Jacobian matrix of the system, and \( e \) represents the \( n_m \times 1 \) vector of measurement noise error.

A common approach to measure the accuracy of the SE process is to compare the L2-norm of measurements residual, which is the difference between the vector of received measurements from measuring units and estimated measurements after the SE process, with a certain threshold (\( \tau \)). Therefore,
if the value of the residual for a set of measurements \( Z \) be greater than \( \tau \), it means that set of measurements contains unacceptable bad data that should be removed. The residual value is defined as follow where \( \hat{x} \) is the \( n_b \times 1 \) vector of estimated states:

\[
R = ||Z - H\hat{x}||
\] (II.2)

A key theorem in [1] states that the contaminated measurements vector \( Z_a = Z + a \), in which vector \( a \) represents the malicious data added to actual measurements, is able to bypass residual-based BDDs if it is a linear combination of the column vectors of the Jacobin matrix \( H \). Therefore, the authors in [1] have defined \( a = Hc \), in which \( c \) is the error generated by the attacker, and proved the incapability of residual-based BDDs to detect this attack vector \( a \):

**Proof:** Assume that the estimated states vector after adding the vector \( a \) to the actual measurements vector \( Z \) is \( \hat{x}_a = \hat{x} + c \) then the 2-norm of the residual after the attack is

\[
R_a = ||Z_a - H\hat{x}_a||
\] After substituting \( Z_a \) with \( Z + a \) and \( \hat{x}_a \) with \( \hat{x} + c \) the 2-norm of the residual is converted to

\[
R_a = ||Z - H\hat{x} + (a - Hc)||
\] With the first and main assumption in the theorem that \( a = Hc \) and the assumption that the original measurements before the attack can pass the BDD the following Eq. (II.3) is true.

\[
R_a = R = ||Z - H\hat{x}|| < \tau
\] (II.3)

**B. LR Attacks**

Every LR attack starts by falsifying bus injection measurements. In this paper, it is assumed that the attackers in LR attacks avoid changing the measurements related to generation part since the control center directly communicates with the power plant control room, which could cause an easy detection. Moreover, there might be some buses with zero injection, which implies no change in injection of these buses.

In this paper, the only way to affect the power system is to increase the loads at some buses and decrease the loads at some other buses in such a way that the total load remains unchanged (operator can easily detect an LR attack if the net change in the loads is not zero as this will easily affect the system frequency). Likewise, attackers should change the line power flow measurements to match and follow the load measurement changes [14]. In addition to the mentioned constraints, attackers in LR attacks are limited to deviate the load at each bus to be neither more or less than a constant expected value (which is usually determined by a percentage of original load value at each bus) since the operator would flag any set of load measurements that deviates far from the short-term load forecasting. At the end, after generating an undetectable LR attack, the security-constrained economic dispatch (SCED) is fed by a contaminated set of loads, and provides a set of fake dispatch points that leads the system to an insecure or inefficient operating state.

Referring to [16], a bi-level LR attack problem with limited access to specific meters is illustrated in Fig. 1. The upper-level objective is to maximize the power flow on a target line, while 1) the number of attacker’s resources is limited by \( N_1 \) and 2) the attacker can change the load at each bus just within a certain range, which is defined by \( \pm \alpha \) percent of the original load at each bus. The lower-level problem is a direct current optimal power flow (DCOPF) problem that models the system response to the attack vector.

**Fig. 1. A bi-level model for generating an LR attack with limited access to meters [16]**

**III. MODELING AND METHODOLOGY**

There are some drawbacks associated to protection-based countermeasures such as 1) reducing measurement redundancy [36] and 2) possibility of launching an attack even when all measurements have been protected [32]. Therefore, in this paper, we propose a detection-based countermeasure and show that the process of identification of LR attacks in power systems can be done using a deep knowledge of power systems. In this section, at first, an exploitable structure for LR attack problems is demonstrated, which is called the core problem of LR attack problems. Then, the mechanism to detect LR attacks is developed and described based on the provided proof, which shows a greedy algorithm is able to solve the proposed core problem for LR attacks, to optimality.

**A. The Core Problem of LR Attack Problems**

An LR attack actually moves the loads up and down in such a way that the attacker achieves the maximum damage based on her/his goal. Obviously, changing the load pattern will affect line flows in any system; power transfer distribution factors (PTDFs) or shift factors (SFs) are the factors that determine what fraction of the injection at each bus will flow across a specific line or flowgate with respect to withdrawal from reference bus \( R \). For instance, assume a particular line is overloaded by 20 MW, the operator will take a generator at a bus that has an SF for that line at 0.5 and move it by 20 MW while then also taking a different generator at another bus that has an SF for that line at -0.5 and move it by 20 MW that would result in a precise change in the
line’s flow by −20 MW and the overall change in supply would be 0 MW. In conclusion, the trivial approach for the operator who wants to reduce the flow on a line is to rank all PTDFs with flexible resources from largest to smallest (the most positive to the most negative). Then, the operator simply starts reducing the net injection of the resource at the top and simultaneously (MW for MW) increasing the resource at the bottom. If either resource runs out of capacity she/he just moves to the next resource on that end and continues until the overload disappears. The essence of the attackers’ approach is also the same as the operator problem while attackers are limited by the amount of changes they can apply to the original resources to avoid being detected.

According to the mentioned practice in the industry and PTDFs concept, there is a very clear way to define the core problem of LR attack problems, which attempt to maximize a line’s overload (in a proper direction) relative to the flexibility of resources (amount of acceptable load change at each bus) throughout the system. Hence, the optimization problem III.1–III.3 is modeled and defined as the core problem of LR attack problems.

\[
\text{maximize } \pm \sum_{i \in N} (H_i c_i) PTDF^R_{i,i} \quad \text{(III.1)} \\
\text{s.t. } -\alpha L_i \leq H_i c_i \leq \alpha L_i, \quad i \in N \quad \text{(III.2)} \\
\sum_{i \in N} H_i c_i = 0 \quad \text{(III.3)}
\]

Where \(PTDF^R_{i,i}\) is the vector of power transfer distribution factors for the target branch \(i \in K\) with respect to the injection at bus \(i \in N\) and withdrawal from the reference bus \(R. H_i c_i \) (\(\Delta L_i\)) is the false deviation generated by the attacker for the load at bus \(i \in N\). \(\alpha \) and \(L_i\) represent the load shift factor and fixed active load at bus \(i \in N\), respectively.

In this problem, the main decision variables are the bus net injection deviations (again, it is assumed that attackers only change load measurements and are not able to change generation measurements) and the objective is to maximize the overload on the target transmission line subject to the attackers’ limitations to change the resources throughout the system. Constraints in III.2 impose the deviation at each bus to be neither more or less than a constant percentage of the original load at that bus (they also impose no change at zero injection buses), and constraint III.3 makes sure that the net load in the system after the LR attack remains unchanged. In this study, linear optimal power flow models have been considered; this work is extendable for non-convex alternative current optimal power flow (ACOPF) formulations since the underlying special structure in the classical DCOPF is caused by KVL and KCL, which remain present in all OPFs.

In the following, the impact of two different LR attacks on a 3-bus system (Fig 2) is illustrated.

All buses have generation units and bus C is the reference bus. Minimum and maximum capacities of all three units are 0 and 150 MW, respectively. Assume that the attacker takes line 1 as the target line and generates two different LR attacks to maximize the overload on this line based on two different load shift factors (5%, 10%). For this example, at first, we solved the problem III.1–III.3 to find the best attack vector, then, using the generated attack vector, we modified loads in the system and run the DCOPF problem, which provides dispatch points in Table I. Secondly, we used the resulted dispatch points to run DC power flow (DCPF) while we considered actual loads to find the actual physical flows on all transmission lines, which are demonstrated in Table I.

In case 1, when \(\alpha\) is 5%, malicious deviations (\(\Delta L_A = +5\) MW, \(\Delta L_B = -5\) MW) lead the DCOPF to provide a set of insecure dispatch points (\(P_{A1}^C = 142.5\) MW, \(P_{B1}^C = 57.5\) MW, and \(P_{C1}^C = 0\)). According to the actual loads (\(L_A = 100\) MW, \(L_B = 100\) MW), this set of fake dispatch points causes \(P_{\text{target}}^1 = 34\) MW, \(P_{2}^1 = -8.5\) MW, and \(P_{3}^1 = 8.5\) MW, which show 13.3% overload on line 1. In case 2, when \(\alpha\) is 10%, the same simulation was repeated and this time the line flows are \(P_{\text{target}}^2 = 38\) MW, \(P_{2}^2 = -9.5\) MW, and \(P_{3}^2 = 9.5\) MW, which show 26.6% overload on line 1. The results demonstrate that as the attack’s energy increases (\(\alpha\) increases) the damage could be more significant, which in some point in time could cause the target line trips offline and results in a cascading blackout. However, there should be a trade-off between the attack’s energy and the detection probability since as the energy increases the detection probability increases.

### Table I. Cyber and Physical results after two different LR attacks on the target line 1 in the 3-bus test case

| Attack Scenarios | \(\alpha = 5\%\) | \(\alpha = 10\%\) |
|------------------|------------------|------------------|
| Cyber Results    | \(L_A\) (MW)     | \(L_A\) (MW)     | \(L_A\) (MW) |
| \(L_B\) (MW)     | 95               | \(L_B\) (MW)     | 90             |
| \(L_{R_{of}}\) (MW) | 0                | \(L_{R_{of}}\) (MW) | 0             |
| \(P_{1}^1\) (MW) | 142.5            | \(P_{1}^1\) (MW) | 147.5          |
| \(P_{2}^1\) (MW) | 57.5             | \(P_{2}^1\) (MW) | 52.5           |
| \(P_{3}^1\) (MW) | 0                | \(P_{3}^1\) (MW) | 0              |
| \(P_{\text{target}}^1\) | 30               | \(P_{\text{target}}^1\) (MW) | 30             |
| Cost ($)         | 11725            | Cost ($)         | 11575          |

| Physical Results | \(P_{\text{target}}^2\) (MW) | \(P_{\text{target}}^2\) (MW) | \(P_{\text{target}}^2\) (MW) |
|------------------|------------------|------------------|------------------|
| \(P_{1}^2\) (MW) | -8.5             | \(P_{1}^2\) (MW) | -9.5             |
| \(P_{2}^2\) (MW) | 8.5              | \(P_{2}^2\) (MW) | 9.5              |

B. Proving the Application of a Greedy Algorithm to Solve the Proposed Core Problem of LR Attacks

After identifying a core problem for LR attacks, the second contribution of this study is to prove that this problem, which is a variant of the fractional knapsack problem [45] from an operations research perspective, can be solved to optimality with a greedy algorithm. In this regard, the application of greedy algorithms to solve the problem III.1–III.3 to optimality has been proved and presented in this section.
Greedy algorithms attempt to build up a solution to a mathematical problem by making a sequence of choices. These choices are dependent on each other, and the previous choices in the solving process affect the other choices that can be made later in the process. Considering the values of possible choices at each step, a greedy algorithm selects the best local choice. This choice is called a greedy choice, and the resulting algorithm is called a greedy algorithm. Greedy algorithms produce good solutions for some mathematical problems. As an example, it provides the global optimum for the fractional knapsack problem.

In the following, a mathematical proof is presented to demonstrate that a greedy algorithm can solve the problem to optimality. After applying a greedy algorithm to solve this problem, at least one of the decision variables (\(\Delta L_i\)) is either at its lower bound (\(l_i\)) or upper bound (\(u_i\)), so optimality follows from the lemma below.

**Lemma:** Feasible solution (\(\Delta L_1, \ldots, \Delta L_{nb}\)) is optimal if and only if, whenever \(PTDF_{l,i} > PTDF_{l,j}\), we find that \(\Delta L_i = u_i\) or \(\Delta L_j = l_j\) (or both).

**Proof:** Suppose by contradiction that there is an optimal solution for which \(PTDF_{l,i} > PTDF_{l,j}\), \(\Delta L_i < u_i\), and \(\Delta L_j > l_j\). Compute \(\delta = \min(u_i - \Delta L_i, \Delta L_j - l_j)\). Adding \(\delta\) to \(\Delta L_i\) and subtracting it from \(\Delta L_j\) gives another feasible solution, but \(\sum_i^{nb} \Delta L_i PTDF_{l,i} \) increases by \(\delta(PTDF_{l,i} - PTDF_{l,j})\), which is positive. Hence the solution cannot be optimal.

\[\Delta L_i = u_i\] or \(\Delta L_j = l_j\) is an optimal solution. Note that \(\sum_t y_t PTDF_{l,t} > \sum_t \Delta L_t PTDF_{l,t}\).

Because \(\sum_t y_t = \sum_t \Delta L_t = 0\) there is an item \(a\) for which \(y_a > \Delta L_a\) and another item \(b\) for which \(y_b < \Delta L_b\). It follows that \(\Delta L_a < u_a\) and \(\Delta L_b > l_b\) (by the conditions that \(S\) satisfies), and hence that \(PTDF_{l,a} > PTDF_{l,b}\). Let \(\delta = \min(y_a - \Delta L_a, \Delta L_b - y_b)\). In \(S\), subtract \(\delta\) from \(y_a\) and add \(\delta\) to \(y_b\), to get a feasible solution \(O\) that changes \(\sum_t y_t PTDF_{l,t}\) by \(\delta(PTDF_{l,b} - PTDF_{l,a})\). Now if \(PTDF_{l,a} < PTDF_{l,b}\), \(O\) yields a larger sum that does \(O\); this contradicts the optimality of \(O\). So this must mean that \(PTDF_{l,a} = PTDF_{l,b}\). Then \(O\) is also optimal, but by construction has fewer items than \(O\) in which it disagrees with \(S\); this contradicts the requirement that \(O\) is an optimal solution with fewest such differences. Therefore, it is concluded that no such \(O\) can exist, and hence that \(S\) is optimal.

This proof for global optimality results in developing a mechanism to predict the attacker’s move and find the sensitive locations, given a target asset. In fact, this proof shows that the proposed core problem is solvable by a trivial sorting approach and there is no reason to solve any complicated problem for the operator to detect LR attacks since the attacker’s strategy is strikingly simple and trivial for this type of attack. By using this mechanism, the operator can determine the sensitive locations for any vulnerable asset and track the changes at these sensitive locations to flag any dangerous set of changes that contributes to overload that asset, which makes it impossible for the attacker to obtain a global solution (and also making it hard to obtain near optimality). Therefore, the attacker has to introduce some form of randomness to avoid being detected. It is predictable that even though the attacker can create a situation where randomness is applied to his/her strategy, so much of the feasible space is cut off by the attack detection mechanism that the resulting impact of this class of attacks is rendered to be very low.

**IV. Simulation and Results**

Here, we investigated the performance of our presented approach using an illustrative example in [IV-A] and a realistic system (2383-bus Polish system) in [IV-B].

**A. Illustrative Test Case**

Here, for more clarification the proposed procedure was applied to the small IEEE 6-bus test case in Fig. 3. In this experiment, we generated two random vectors \((a_1, a_2)\) in such a way that one of them is an attack vector and the other is not; then, we used our proposed mechanism to find the attack vector.

![Fig. 3. 6-Bus test case diagram](image)

Both vectors are samples from a normal distribution, but the one that is the attack is simply arranged in such a way that causes an overload on the vulnerable line from bus 3 to bus 5 (line 3-5); this is the basic technique of an unobservable attack: have the deviations fall into the potential spectrum of generally accepted noise error but have the preferred values be at preferred buses. All required information including amount of load at each bus, PTDF values of all buses with respect to line 3-5, vector \(a_1\), and vector \(a_2\) are shown in Table II.

| Bus | Load (MW) | PTDF | \(a_1\) (MW) | \(a_2\) (MW) |
|-----|----------|------|--------------|--------------|
| 1   | 10       | 0    | -0.436       | 0.976        |
| 2   | 15       | 0.0822| -0.127       | -0.954       |
| 3   | 15       | 0.289 | 1.136        | 1.143        |
| 4   | 30       | 0.0183| -0.564       | -2.051       |
| 5   | 20       | -0.1207| -0.751       | 1.519        |
| 6   | 10       | 0.1526| 0.762        | -0.633       |

The detection process starts by solving the problem [III.1 III.3] by the greedy algorithm (Algorithm 1) to find the best attack vector for line 3-5, which determines the most sensitive buses associated to this line. In Algorithm 1 at first all buses are sorted based on their PTDF absolute values in a descending order. Then, considering \(\alpha = 10\%\), the maximum possible deviation (assume that line 3-5’s initial flow is positive) is assigned to each bus from the top to the end, while at each
The Greedy solver Results (MW)

| Bus    | load(MW) | PTDF  | Best Attack(MW) | a1(MW) | a2(MW) |
|--------|----------|-------|-----------------|--------|--------|
| 3      | 15       | 0.289 | 1.0             | 0.762  | -0.633 |
| 6      | 10       | 0.152 | 1.5             | 1.136  | 1.143  |
| 5      | 20       | -0.120 | -2.9            | -0.751 | 1.519  |
| 2      | 15       | 0.0622 | 1.5             | -0.127 | -0.954 |
| 4      | 30       | 0.0183 | -1.0            | -0.564 | 2.951  |
| 1      | 10       | 0      | -1.0            | -0.456 | 0.976  |

According to Table III, a1 has 3 deviations (at buses 3, 6, and 5) out of 4 deviations at the most sensitive buses (buses 3, 6, 5 and 2) with proper directions to cause an overload on line 3-5 (assume PTDFs with absolute values below 0.05 are assumed to be zero). On the other hand, a2 has just 1 deviation (bus 3) out of 4 deviations at the most sensitive buses with proper direction, which shows that vector a1 is the attack vector with 0.5165 MW difference between cyber and physical flow on this line.

Fig. 4. 6-Bus test case diagram with the attackers’ preferred load deviations spectrum to overload line 3-5 and the a1’s load deviations spectrum: left side circles are related to a1 and right side circles are related to best attack vector.

Fig. 4 visually shows and compares the best attack and the random attack a1, where the circles at the left side of the buses show the load deviations related to a1 and the circles at the right side of the buses show the load deviations related to best attack vector (larger circle indicates more sensitive bus).

B. Case Study on the Modified 2383-Bus Polish Test System

The original 2383-Bus Polish Test System is available in [46]. The modifications include: decreasing the line ratings to create base case attacks; and set the negative loads to zero. In this section, multiple evaluations have been done. At first an attack vector was generated for line 168 by solving problem III.1-III.3 two times; one time by the GUROBI solver and one time by the greedy algorithm, which numerically demonstrates the capability of the greedy algorithm to optimize the core problem and get the same results as the GUROBI solver gets. For the second study, the effectiveness of the generated attack vector was tested by 1) the Enhanced Malicious Load Deviation Index (EMLDI) proposed in [47] and 2) showing the flow results on line 168 after the attack by doing the same simulation that was done in section III-A. At last, the capability of the proposed detection mechanism to distinguish noise vectors from attack vectors as well as its ability to detect effective random attacks have been demonstrated.

1) Solving the Problem III.1-III.3 by Two Methods: the GUROBI Solver and the Greedy Algorithm: In this subsection, capability of the greedy algorithm to solve the core problem to optimality is demonstrated by comparing the results of solving the problem III.1-III.3 by the GUROBI solver and the results from the greedy algorithm. For the sake of this discussion, we solved the problem III.1-III.3 for line 168 while α is 10% under JAVA on an Intel(R) Xeon(R) CPU with 48 GB of RAM.

The resulted attack vectors from both methods are perfectly matched each other as it is shown in Fig. 5 for some of the most sensitive buses. It should be noted that the GUROBI solves the problem III.1-III.3 in 127 ms, which is 120 ms longer than what takes for the greedy algorithm to solve this problem with the same results. This result indicates the efficiency of using the greedy solver in 5-minute operational interval EMSs.

Fig. 5. Malicious load deviations at some of the most sensitive buses with respect to the target line 168 in the 2383-Bus Polish system: achieved by solving the problem III.1-III.3 using both the GUROBI and greedy solvers.

2) Attack Efficiency Analysis Using EMLDI: In this subsection, the efficiency of the generated attack that could put the system in danger has been demonstrated by calculating the EMLDI value and also by showing the physical line flow after the attack on the target line. EMLDI is an index that is
recently proposed to measure the effect of load deviations on each vulnerable asset in the system. It utilizes load deviation in MW at each bus and the value of each bus relative to the asset under evaluation (PTDF) to flag any set of load changes that contribute to increase the flow on a target branch. Table IV illustrates different intervals for ELMIDI value and corresponding alert-level based on the definition in [47].

| ELMIDI | Alert-Level | Normal | Monitor | Warning | Danger |
|--------|-------------|--------|---------|---------|--------|
| < 0.20 |             |        |         |         |        |
| 0.20   |             |        |         |         |        |
| 0.35   |             |        |         |         |        |
| 0.50   |             |        |         |         |        |

With respect to the generated attack vector for line 168, ELMIDI is 0.9629. Clearly, this ELMIDI value shows the effectiveness of the attack vector according to the alert-intervals in Table IV.

Likewise, Table V provides line flow results, including the cyber flow, physical flow, and amount of the overload for the best attack (global solution).

TABLE V. Interpretation of different ELMIDI values [47]

The cyber flow in Table V (resulted from solving DCOPF and fake loads) shows that there is no overload on the target line in cyber world (what the operator sees), while the physical flow (resulted from solving DCOPF, actual loads, and fake dispatch points) shows 251.516 MW of overload on this line (what the attacker desires).

3) Detection Mechanism Efficiency Analysis: In this section, a study has been conducted to show 1) the efficiency of the proposed mechanism to detect malicious changes that have enough energy to put the system in danger 2) the ability of the proposed mechanism to distinguish noisy errors from malicious changes in loads. To sake of this discussion, 2000 vectors representing changes in net injection for all 2383 buses, except zero injection buses, were generated, where 1000 vectors were malicious vectors; given line 168 as the target line; with a form of randomness (they were randomly modified to not match the best attack vector) while the other 1000 vectors were samples from normal distributions. To generate 1000 random attack vectors, each time we 1) multiplied \( \alpha \) (10%) to a random number between 0.8 and 0.9, which condensated the feasible region of the original problem, 2) added a constraint to the problem III.1-III.3 to force the changes at 200 randomly selected sensitive locations (for line 168) to be zero, and 3) solved the new modified III.1-III.3 to have a random attack vector. The other 1000 Gaussian random vectors \( (\mu = 0, \delta = \alpha L / 3) \) were generated in such a way that 1) deviation at each bus could not be more or less than a minimum/maximum acceptable values, 2) there was no change at zero injection buses, and 3) the net load change in the system was very small.

Fig. 6 depicts physical flows on line 168 as the impact of each of 2000 vectors versus the number of proper changes at sensitive locations (to make the line 168 overloaded). To get the results in Fig. 6 each time 1) we added one of the 2000 vectors to the original load vector and found the fake load vector, then 2) based on the resulted fake load vector we ran DCOPF and found the fake dispatch points, and at the end 3) we ran DCPF by considering the resulted fake dispatch points and the original loads before adding either of random attack or noise error vector to the original load vector to find the physical flow on line 168 as the impact of each vector. Likewise, we did a comparison between each of the 2000 vectors and the attackers’ preferred spectrum (best attack vector), achieved in section IV-B1 to find the number of proper deviations (deviations with proper directions and enough magnitudes) at the most sensitive buses for each vector. All of the random attack vectors (red dots) cause physical overflows on the line 168 and the Gaussian random vectors (blue dots) are not able to cause physical overloads on this line. Therefore, according to the large difference between the number of proper deviations at sensitive locations for random attacks and noisy errors in Fig. 6 it is concluded that the proposed mechanism can distinguish random attacks from noisy errors and detect them.

V. CONCLUSION

Cyber-security increasingly draws people’s attention in a variety of areas in power systems. Inability of existing bad data detectors to detect all falsely injected data makes the problem critical and worrisome. In this study, by using deeper understanding of power systems, a non-probabilistic intelligent false data detector that reduces the risk of LR attacks and their impacts is introduced, designed, and evaluated. We first used power systems domain insights and PTDFs concept to identify an exploitable model for the core problem of LR attacks, then, by proving that a simple greedy algorithm is able to solve this model to optimality, the proposed detection mechanism is designed to find the most sensitive locations in power systems with respect to their impact on a target asset. Likewise, at the end, the efficiency of this detection mechanism to detect some energy-reduced random attacks and its ability to distinguish malicious changes from noise errors are shown. Besides the simple nature of this detection mechanism, which reduces the
computational complexities with respect to many potential vulnerabilities in a large network, this method could be a perfect complement for other detection mechanisms.

ACKNOWLEDGMENT

The authors would like to thank Dr. Charlie Colbourn at School of Computing, Informatics and Decision Systems Engineering, Arizona State University for his kind help through this study.

REFERENCES

[1] 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.

[2] J. Kim and L. Tong, “On topology attack of a smart grid: Undetectable attacks and countermeasures,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1294–1305, 2013.

[3] G. Hug and J. A. Giampapa, “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1362–1370, 2012.

[4] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, “On false data-injection attacks against power system state estimation: Modeling and countermeasures,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 717–729, 2014.

[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] A. Anwar, A. N. Mahmood, and M. Pickering, “Data-driven stealthy injection attacks on smart grid with incomplete measurements,” in Pacific-Asia Workshop on Intelligence and Security Informatics. Springer, 2016, pp. 180–192.

[8] J. Kim, L. Tong, and R. J. Thomas, “Subspace methods for data attack on state estimation: A data driven approach,” IEEE Trans. Signal Processing, vol. 63, no. 5, pp. 1102–1114, 2015.

[9] A. Tajer, “False data injection attacks in electricity markets by limited adversaries: Stochastic robustness,” IEEE Transactions on Smart Grid, pp. 1–1, 2017.

[10] Z.-H. Yu and W.-L. Chin, “Blind false data injection attack using pca approximation method in smart grid,” IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1219–1226, 2015.

[11] Y. Yuan, Z. Li, and K. Ren, “Quantitative analysis of load redistribution attacks in power systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1731–1738, 2012.

[12] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, “Cyber-attack on overload- ing multiple lines: A bilevel mixed-integer linear programming model,” IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1534–1536, 2017.

[13] A. Tajer and Z. Li, “Local load redistribution attacks in power systems with incomplete network information,” IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1665–1674, 2016.

[14] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, “Cyber-attack on overload- ing multiple lines: A bilevel mixed-integer linear programming model,” IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1534–1536, 2017.

[15] A. Tajer and Z. Li, “Local load redistribution attacks in power systems with incomplete network information,” IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1665–1674, 2016.

[16] Y. Liu, Z. Bao, D. Lu, and Z. Li, “Modeling of local false data injection attacks with reduced network information,” IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1868–1896, 2015.

[17] Z. Li, T. Zhao, and Y. Wu, “Cyber attacks against the economic operation of power systems: A fast solution,” IEEE Transactions on Smart Grid, vol. 8, no. 2, pp. 1023–1025, 2016.
[42] S. A. Foroutan and F. R. Salmasi, “Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 2017.

[43] A. Pinceti, O. Kosut, and L. Sankar, “Load redistribution attack detection using machine learning: A data-driven approach,” 2018, accepted in 2017 IEEE Power Energy Society General Meeting. Available upon request.

[44] Y. He, G. J. Mendis, and J. Wei, “Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[45] N. Ferdosian, M. Othman, B. M. Ali, and K. Y. Lun, “Greedy–knapsack algorithm for optimal downlink resource allocation in lte networks,” *Wireless Networks*, vol. 22, no. 5, pp. 1427–1440, 2016.

[46] R. D. Zimmerman, C. E. Murillo-Sánchez, and D. Gan, “Matpower,” PSERC.[Online]. Software Available at: http://www.pserc.cornell.edu/matpower, 1997.

[47] X. Li and K. W. Hedman, “False data injection cyber-attack detection,” *arXiv preprint arXiv:1810.05939* 2018.