Research Article – Vol. 02, Issue 03, No. 01

Advanced in Engineering and Intelligence Systems

Journal Web Page: https://aeis.bilijipub.com

Phasor Measurement Units Allocation Against Load Redistribution Attacks Based on Greedy Algorithm

Ali Rahdan[1,*] , Ali Khaleghi[1]

[1] *Department of Electrical Engineering, Shahid Beheshti University, Velenjak, Tehran, Iran*

Highlights

- Grid security faces growing cyber threats.
- Load redistribution attacks cause grid confusion.
- Efficient resource allocation for defense.
- Quick algorithms protect key substations.

Article Info

Received: 08 May 2023
Received in revised: 20 June 2023
Accepted: 13 July 2023
Available online: 30 September 2023

Keywords

Load Redistribution Attacks
Phasor Measurements Units;
False Data Injection Attacks;
PMU Allocation;
Greedy Algorithm.

Abstract

Power grid vulnerability to various cyber-attacks will undoubtedly increase with the widespread use of cutting-edge computer technologies in power systems monitoring and control. A common and effective cyber-attack on power grids is load redistribution (LR), which has the potential to confuse power re-dispatch and result in unneeded load loss. To protect the power system, it is essential to devise strategies for the best distribution of the scarce defensive resources, especially those that take the actions of the attackers into account. In order to stop LR attacks, the best budget allocation and the interplay between attack and defense are examined in this study. In particular, the bi-level modeling of LR attacks incorporates the attack and defense interactions. Based on their importance as targets for cyber protection, a few significant substations are chosen. To reduce the projected load loss subject to the attacker's capability, an efficient budget allocation approach based on greedy algorithm is devised for protecting the key substations. To select the optimum attack method and pinpoint the most vulnerable buses for crucial transmission assets, a quick greedy algorithm is proposed. The proposed approaches are put to the test in various scenarios using an IEEE test systems, and the simulation results show that they work. This study provides fresh information on efficiently preventing and reducing the LR attack.

Nomenclature

a	*Load shift factor.*	*M*	*Set of all measurements.*
a_k^{min}	*The minimum load shift factor that is the start point for transmission asset k∈K to have overflow.*	*m*	*Index for measurement.*
c_g	*Production cost of unit gϵG*	*N*	*Set of all buses.*
e	*$n_m \times 1$ vector of measurement noise errors.*	*N_1*	*Number of states that can be compromised by attacker.*
G	*Set of all generation units.*	*n_b*	*Number of buses.*
g	*Index for generation unit.*	*n_{br}*	*Number of transmission branches.*
$G(i)$	*Set of all generation units at bus iϵN*	*n_m*	*Number of measurements.*
$\boldsymbol{H}$	*$n_m \times n_b$ Jacobian matrix of the system.*	*P_g*	*Fixed dispatch point of unit g∈G*

[*] Corresponding Author: Ali Rahdan
Email: a_rahdan@sbu.ac.ir

H'	*$n_b \times n_b$ dependency matrix between power injection measurements and state variables .*	P_k^{max}	*Continuous thermal rating of transmission branch $k \in K$.*
H'_i	*i^{th} row of $H'(i \in N)$*	P_g^{max}	*Upper limit on generation capacity of unit $g \in G$.*
i	*İndex for bus*	P_g^{min}	*Lower limit on generation capacity of unit $g \in G$.*
K	*Set of all transmission branches.*	$PTDF^R_{k,\, i}$	*Power transfer distribution factor for branch $k \in K$ and bus I N (Iinjection) with regard to reference bus R*
k	*İndex for transmission branch.*	ub_i	*Upper bound for load deviation at each bus $i \in N$ $n_m \times 1$ vector of measurements.*
L_I	*Active load (MW) at bus $i \in N$.*	τ	*Residual-based bad data detector threshold.*
lb_i	*Lower bound for load deviation at each bus $i \in N$.*		

1. Introduction

Global efforts to protect the environment and promote resource conservation have prompted the creation of the next-generation power grid. One important difference between the smart grid and the traditional grid is the widespread employment of numerous cutting-edge intelligent devices and the associated cyber information and control technology. Smart meters, phasor measurement units, IEC 61850-based substations, and other examples of novel applications are typical examples [1]. The power systems have also been combined to accommodate electric vehicles [2]. Innovative approaches are being put into use for congestion control [3] and demand response [4]. The power grid gradually becomes a cyber-physical smart grid as a result of all of these applications, which also increase the operational flexibility of the grid while increasing the dependency of the grid reliability on the related cyber network. However, as the power grid's cyber layer becomes more complex, cyber vulnerabilities in its digital parts inevitably arise, making it more vulnerable to various cyber-attacks. Intruders might compromise a wide-area network, execute a man-in-the-middle assault, and then alter the instructions supplied to the circuit breaker. Additionally, the power system's operation could be disrupted if the lines or generators trip. Additionally, attackers have the ability to alter the measurements sent to a control center by breaking the password or taking advantage of SCADA network flaws. Denial of service attacks are another option for attackers to use to obstruct or slow down communication between the control center and the substations. System synchronization issues or the unavailability of crucial field devices could result from this. The power grid might be severely damaged by cyber-attacks like these, and cyber mishaps and attacks on the energy industry have already happened all over the world [5]. The power system's cyber security issues have recently attracted a lot of attention [6], [7].

A reliable state estimate is a vital part of the energy management system, providing the power grid operator with a thorough understanding of the power grid's current condition. If the state estimate result is manipulated, the power system operator could be misled into making poor choices. Recently, it was discovered in Ref. [8] that attackers might evade the detection of faulty data and purposefully influence the results of the state estimation by purposefully manipulating the measurements. Additionally, two mathematical models looking at the immediate effect and delayed consequence as well as a load redistribution assault, a plausible false data injection attack, were looked at in References [9] and [10]. The authors of these two papers [11] used bi-level optimization to examine the attacker-defender dynamic, a technique that is often used in the fields of power system security research and energy management.

This study investigates the load-redistribution (LR) assault, which is a kind of FDIA used to disrupt power grids. In order to cause either physical and financial disruption to power grids, LR assaults seek to fudge bus injection measurements. In order to simulate LR assaults, some researchers [12]–[18] proposed bi-level or attacker–defender optimization problems with goals like maximizing operating cost or power flow on a target line. The bi-level assault model in [12] describes the attacker's aim, which is to maximize operational cost (generating cost + load shedding cost), and the system's reaction, which is based on a base-case security-constrained economic dispatch (SCED). Ref [13] and [14] propose bi-level assault models. Their higher-level aim was to maximize physical damage to a target line, while their lower-level goals were to characterize the systems' reactions using a nonlinear alternating current optimum power flow (ACOPF) and DCOPF, respectively. [17] also examined the immediate and long-term financial and medical effects of LR assaults. They offered a bi-level problem to assess the worst-case economic outcome of an assault, their immediate offensive aim. They created a tri-level problem to maximize operating expense after tripping an overloaded line.

Numerous research have been conducted regarding the defense tactics for cyber-attacks. It was demonstrated in Refs. [19] and [20] that attackers can compromise the results of the state estimation by simply knowing a portion of the information about the structure of the power grid. Using the AC power system model, Ref. [21] published a graphical way to safeguard the power grid against fabricated data injection assaults by securing carefully selected measurements. Protection-based and detection-based defensive strategies were analyzed in Ref. [22] to find the crucial parameters for making the power system immune to the fake date injection attack. Ref.[23] investigates the attack and defense of incorrect data injection in the electric power market using a game-theoretic approach. Both Voltage Control and Automated Generation Control were studied in Refs. [24] and [25], where the attacker-defender interaction was studied via a Markov game. In references [26] and [27], cyber-physical switching attacks with the potential to disrupt the power system are analyzed. In references [28] and [29], cyber-attacks on the SCADA systems of the energy and water utilities are examined. [30] proposed a sparsity-based method for identifying the error in the estimate of the DC power flow state.

Aside from device status, the safe and efficient functioning of the power system is heavily reliant on the operators' responsiveness to the system's condition. As a consequence, there are two sorts of attacks against power system operations: those that can directly change device statuses, such as tripping lines and isolating buses, and those that can't but can fool power system monitoring and dispatch, such as fake data injection assaults and LR attacks. A significant amount of work has gone into finding strategies to secure the power system against the first kind of attack [24-27]. However, it is equally critical to develop ways to avoid the second kind of assault. LR attacks, as an example of a situation involving deceptive data injection, might mislead the power dispatch and result in significant load loss. As a result, we use the LR assault to illustrate the second kind of strike.

Following is a synopsis of the paper's most significant findings.

(1) System operators may rapidly discover the most susceptible buses even in networks with numerous nodes according to a mathematical argument that a greedy algorithm may best solve the exploitable structure of LR attack issues.

(2) Using knowledge from the power systems area to find a structure in LR assault problems that may be exploited, so allowing operators to anticipate the attackers' actions.

(3) A method is suggested for making the most efficient use of the limited number of processing power management units (PMU) in order to reduce the pessimistic loss brought on by LR attacks.

Specifically, we will highlight the following contributions:

1. We propose a novel approach to protecting power systems from load redistribution attacks by optimizing the allocation of defensive resources to critical substations.
2. We demonstrate the effectiveness of our approach through simulations on the IEEE test systems, which show significant reductions in projected load loss.
3. We develop a bi-level modeling framework that incorporates the interaction between attack and defense strategies, providing a more comprehensive and realistic representation of the security situation.
4. We propose an efficient budget allocation approach based on the greedy algorithm that considers the attacker's capabilities and optimizes the allocation of defensive resources to protect the most critical substations.

This paper's remaining sections are structured as follows. Section 2 provides a high-level overview of state estimates and LR attacks. In Section 3, we see how a greedy algorithm was used to decide which vital substations needed protection. In Section 4, we formulate and solve the optimal PMU allocation problem. Section 5 provides case studies based on the IEEE 14-bus and IEEE 118-bus systems, while Section 8 wraps up the paper.

2. Brief Description of FDI Attacks

A. Bypass BDD by FDI Attack

It uses linear equations to relate measured quantities to state variables (voltage angles) in the DCSE procedure. These linear equations are modeled as matrices in Eq. 1:

$$\mathbf{Z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \qquad (1)$$

The 2-norm of the measurements residual is usually compared to a specified value (τ) to assess SE process precision. If the residual 2-norm exceeds, Z has unsatisfactory data. In equation 2, the residual's 2-norm is derived as follows: II.II is the Euclidean norm, which specifies the vector coordinate's distance from the vector space's origin, and xx is the nb*1 vector of estimated states.

$$\| \mathbf{R} \|_2 = \| \mathbf{Z} - \mathbf{H}\hat{\mathbf{x}} \|_2. \qquad (2)$$

A key theorem in [31] states that the vector of contaminated measurements Z_a=Z+a, where a stands for the malicious data added to real measurements, may avoid residual-based BDDs if it is a linear combination of H. In order to show that the residual-based BDD is unable to recognize the attack vector a, the authors in [31] created a=Hc.

B. LR Attacks

Every LR assault begins with false bus injection measurements. Because of the direct connection between the control room and the power plants, it is expected that in LR attacks, attackers would not tamper with generation-related measures. It is also preferable to prevent deviations at zero injection buses.

According to this research, increasing loads on certain buses while lowering loads on others is the only viable approach for launching an LR assault on electricity grids. The net load must be maintained constant to prevent frequency issues. As a result, power flow measurements should be adjusted by attackers to account for fluctuations in load. In addition, the load variation at each bus must fall within a narrow range of fixed thresholds. Since the load variations are larger than the short-term load estimates, the operator would draw attention to that particular set of load data. Most of the time, these constants are determined as a percentage of the projected load value at each bus in both directions.

An undetected LR attack is then launched, in which a tainted set of loads and a set of fraudulent dispatch points are fed into the SCED, resulting in unsafe or inefficient system operation. To optimize the flow of a targeted transmission branch (line l) with restricted access to certain meters, as shown in Fig. 1 [14], for example, a bi-level LR attack scenario might be used. At the highest level, the attacker takes into account both the available resources (N1) and the load fluctuations on the target line to achieve maximum power flow. The bottom layer is a dynamic counterattack planning function (DCOPF) that mimics the system's response to the assault vector produced on the upper level.

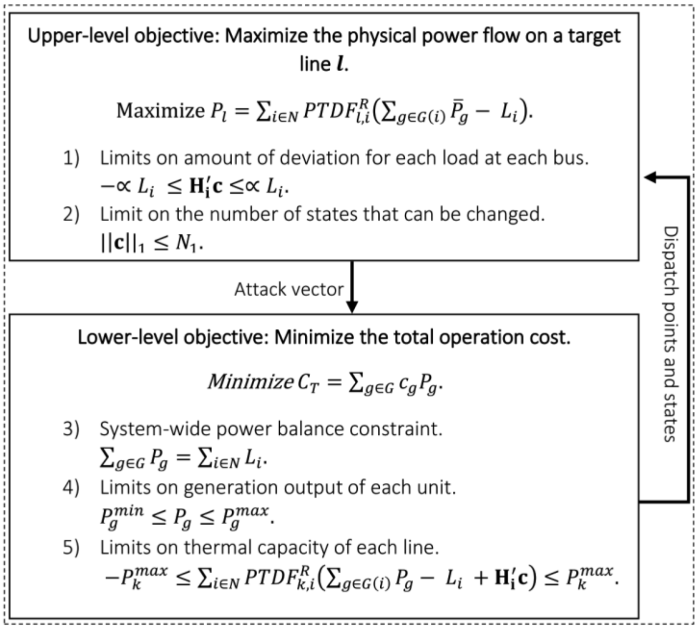
Upper-level objective: Maximize the physical power flow on a target line $\boldsymbol{l}$.
Maximize $P_l = \sum_{i \in N} PTDF_{l,i}^{R}\left(\sum_{g \in G(i)} \bar{P}_g - L_i\right)$.
1) Limits on amount of deviation for each load at each bus.
$-\propto L_i \le \mathbf{H}_i'\mathbf{c} \le \propto L_i$.
2) Limit on the number of states that can be changed.
$||\mathbf{c}||_1 \le N_1$.
Attack vector
Lower-level objective: Minimize the total operation cost.
$Minimize\, C_T = \sum_{g \in G} c_g P_g$.
3) System-wide power balance constraint.
$\sum_{g \in G} P_g = \sum_{i \in N} L_i$.
4) Limits on generation output of each unit.
$P_g^{min} \le P_g \le P_g^{max}$.
5) Limits on thermal capacity of each line.
$-P_k^{max} \le \sum_{i \in N} PTDF_{k,i}^{R}\left(\sum_{g \in G(i)} P_g - L_i + \mathbf{H}_i'\mathbf{c}\right) \le P_k^{max}$.
Dispatch points and states

Fig. 1. Bi-level load redistribution attack model

3. Modeling And Methodology

On the basis of our extensive power system understanding, we put out a detection strategy against LR attacks. First, a structure that can be exploited to solve the fundamental issue with bi-level LR attack concerns is found. The theory for the optimality requirements of that exploitable structure is then used to construct and explain the suggested method.

A. The Core Issue's Identified Exploitable Structure

It is the goal of LR attacks to cause as much physical damage as possible to a target transmission asset by shifting load measurements up and down. The LR attack problems' central challenge is described as the maximization of line power flow relative to the system's resource flexibility.

$$\underset{\mathbf{H}_i'\mathbf{c}}{\text{Maximize}} \pm \sum_{i \in N} (\mathbf{H}_i'\mathbf{c}) PTDF_{l,i}^{R} \tag{3}$$

$$\text{s.t.} -\alpha L_i \le \mathbf{H}_i'\mathbf{c} \le \alpha L_i i \in N, \tag{4}$$

$$\sum_{i \in N} \mathbf{H}_i'\mathbf{c} = 0, \tag{5}$$

To stress the need of bus angle changes for attackers to achieve desirable load variations, we utilized the $\mathbf{H}_i'\mathbf{c}$. If, due to the aforementioned issue, the load on bus 2 deviates by 5 MW ($\mathbf{H}_2'\mathbf{c} = \Delta L_2 =$ 5MW), the attacker must ensure that the value of $\mathbf{H}_2'\mathbf{c}$ is 5 MW. Each bus's predicted load is shown as L_i, and load shift factor is shown as α.

The primary decision factors for problems (3)–(5) are the load deviations. This is done so that the overflow on a specific transmission asset may be maximized. The overflow direction on a target transmission asset, according to the notation, may be either positive or negative depending on the flow of power before the assault on the target asset. For instance, in equation 3, the attacker should use "plus" if the pre-attack power flow of the target asset is "plus" 100 megawatts (MW), and they should use "minus" if the pre-attack power flow is "minus" 100 megawatts (MW).

For 4 to hold, the allowed range for bus-to-bus variation must be less than or equal to 4% of the bus's estimated load (they also require that there be no change for zero injection buses). Requirement 5 ensures that the after-LR-assault net burden does not change.

This research exclusively considers linear optimum power flow models due to the fact that the unique structure of the classical DCOPF is caused by Kirchhoff's Voltage Law (KVL) and Kirchhoff's Current Law (KCL), which are present in all optimal power flows. However, non-convex ACOPF formulations are within the scope of this investigation (OPFs).[32], [33]

B. Finding the sensitive buses by Greedy Algorithm

The next step is to show that, from the perspective of operations research, the central issue may be optimally addressed by means of a greedy algorithm. In order to put together a solution to a mathematical problem, greedy techniques make a sequence of choices. All of these choices are interconnected, and the ones taken at the outset of the problem-solving process affect the options available later on. At each stage, a greedy algorithm considers the current value of the alternatives available and picks the one that provides the best local result. The algorithm that results from such a choice is known as a "greedy algorithm" because of its excessive focus on maximization of reward. Greedy algorithms give great answers to certain mathematical problems. For the fractional knapsack problem, for instance, it yields the global optimal [34].

The mathematical argument that a greedy algorithm may handle problems (3)–(5) optimally is given in the section that follows. As shown in the following theorem, if a greedy algorithm is employed to find a solution to this issue and at least one of the choice variables (ΔL_i) is at its lower limit (l_i) or upper bound (u_i), then optimality will be achieved.

Theorem 1. Feasible solution $(\Delta L_1, \dots, \Delta L_{n_b})$ is optimal if and only if, whenever $PTDF_{l,i}^R > PTDF_{l,j}^R$, we find that $\Delta L_i = u_i$ or $\Delta L_j = l_j$ (or both).

Assume, contradictorily, that there is a unique best solution for $PTDF_{l,i}^R > PTDF_{l,j}^R, \Delta L_i < u_i$, and $\Delta L_j > l_j$. Compute $\delta = \min(u_i - \Delta L_i, \Delta L_j - l_j)$. Then, add δ to ΔL_i and subtract it from ΔL_j, that suggests another approach that could work. However, $\sum_t^{n_b} \Delta L_t PTDF_{l,t}^R$ increases by $\delta(PTDF_{l,i}^R - PTDF_{l,j}^R)$, which is a good thing. Therefore, it is clear that this is not the best possible solution.

Suppose by contradiction $\mathbf{S} = (\Delta L_1, \dots, \Delta L_{n_b})$ is a feasible solution for which whenever $PTDF_{l,i}^R > PTDF_{l,j}^R$, $\Delta L_i = u_i$ or $\Delta L_j = l_j$ but is not an optimal solution. Choose an optimal solution $\mathbf{O} = (y_1, \dots, y_{n_b})$ in which the number of times that $\Delta L_t \neq y_t, (t \in N)$ is as small as possible. Note that $\sum_t^{n_b} y_t PTDF_{l,t}^R > \sum_t^{n_b} \Delta L_t PTDF_{l,t}^R$. Because $\sum_t^{n_b} y_t = \sum_t^{n_b} \Delta L_t = 0$ 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 $PTDF_{l,a}^R \leq PTDF_{l,b}^R$. Let $\delta = \min(y_a - \Delta L_a, \Delta L_b - y_b)$. In $\mathbf{O}$, subtract δ from y_a and add δ to y_b, to get a feasible solution $\mathbf{O}'$ that changes $\sum_t^{n_b} y_t PTDF_{l,t}^R$ by $\delta(PTDF_{l,b}^R - PTDF_{l,a}^R)$. Now if $PTDF_{l,a}^R < PTDF_{l,b}^R$, $\mathbf{O}'$ yields a larger sum that does $\mathbf{O}$; this contradicts the optimality of $\mathbf{O}$. So, this must mean that $PTDF_{l,a}^R = PTDF_{l,b}^R$. If $\mathbf{O}$ is an ideal solution with the fewest such discrepancies, then $\mathbf{O}'$ is also optimal, but by construction, it disagrees with S on fewer things than $\mathbf{O}$ does. As a result, it is determined that there cannot be an $\mathbf{O}$ and that S is therefore the best option.

This proof of global optimality, given a target transmission asset, allows for the development of a mechanism that can foresee the actions of attackers and pinpoint the weak buses. LR assaults are easy to spot since the attackers' methods are so simple, and this proof shows that the fundamental problem's identified structure can be handled using a simply sorting strategy. Operators can quickly identify the vulnerable buses for any crucial transmission asset by employing this approach. As a result, attackers are unable to find a global solution (also very close to optimality). Attackers must therefore use some sort of randomness to prevent detection. It is anticipated that even if attackers can set up a scenario in which randomness is applied to their strategy, the suggested assault defense mechanism cuts off a significant portion of the viable space, making the repercussions of this type of attacks very minimal.

4. Concept of Observability and PMU Allocation

A. Observability of Power systems

In general, the power system observability means the estimation of network variables to estimate the system state. If the network state estimation is calculated and if the grid state estimation encounters a problem, the network will not be observable [35]. The network variables are usually considered as buses phasor voltage. When phasor units are connected to a bus, the voltage and its phase angle can be measured. They can also figure out the phasor of all the branches that are currently wired to that bus. Therefore, utilizing the fundamental principles of KVL, KCL of power, we can determine the magnitude and phase angle of voltage on buses linked to buses fitted with phasor measurement units. Therefore, buses in which phasor measurement units are installed have direct observability, and buses connected to buses with phasor measurement units have indirect observability. Buses that do not have relationship with buses with phasor measurement units are not observable (Fig 2).

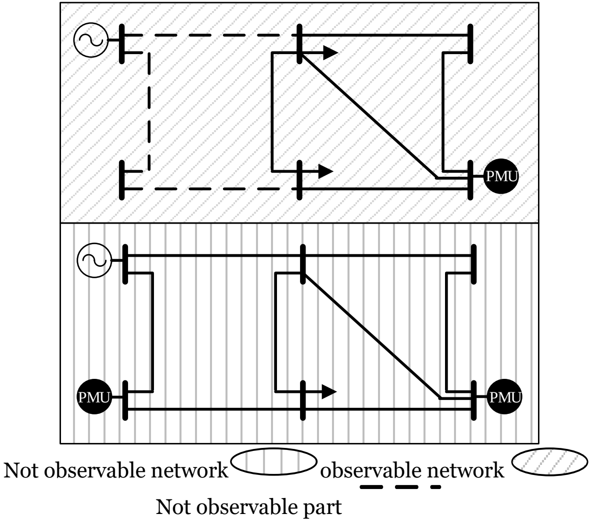

Fig. 2. Network observability using PMU

B. Formulization of PMU Allocation Problem

The voltage and current phasors of a bus and the voltage phasors of all branches linked to that bus can be estimated by a PMU put in the bus. Thus, when PMU is installed at strategic points in the network, the information needed to observe the systems can be obtained. Estimating the network observability and reducing the number of PMU are the two main goals. In this paper, the location of phasor units is investigated so that in addition to the mineralization of number of required units, the peripheral objectives including the largest number of observability and total observability of entire network can be fulfilled. After identifying all crucial transmission assets' vulnerable buses, For a system with n buses, the optimal location problem is expressed via the equation (6) [36]:

$$min \sum_{i=1}^{n} w_i x_i \tag{6}$$

$$s.t \quad y = Ax \geq b \tag{7}$$

$$x(p) = 1 \qquad p \in determined\ sensitive\ buses \tag{8}$$

Where w is a matrix of installed PMU costs or a bus weight matrix that may fluctuate based on the significance of each bus, and n is the total number of buses in the system. It is frequently referred to as the matrix n×n, and the following definitions of A and b apply:

$$A_{n\times n}(i,j) = \begin{cases} 1 & i = j \\ 1 & if\ buses\ i\ and\ j\ are\ connected \\ 0 & otherwise \end{cases} \tag{9}$$

$$x_{n\times 1}(i) = \begin{cases} 1 & if\ PMU\ installed\ in\ bus\ i \\ 0 & other \end{cases} \tag{10}$$

$$b = [1\ 1\ 1\ 1\ 1 \dots 1\ 1]^T \tag{11}$$

In equation (1) is used for complete observability of the system, and the ith row of the matrix Ax is the number of frequency of the observability of the ith bus which should be at least one.

5. Simulation and Results

In this part, we calculate cyber load by first running the Section IV optimization problem on the IEEE 14-bus system. Then, we use the greedy technique outlined in Section III.B to determine the ideal location for encrypted PMUs on substations for IEEE 14-bus and IEEE 118-bus systems. AC power flow, AC state estimation, and ACOPF are all implemented using the MATPOWER package in MATLAB. The PMU allocation optimization problem is solved via ILP.

A. consequence of LR attack on IEEE 14-Bus

In this section, the load redistribution attack is implemented on IEEE standard 14-bus system. The system has 14 buses, and 20 lines. There are a total of 41 measurements in the system. The load deviation limit is set at α=20%.

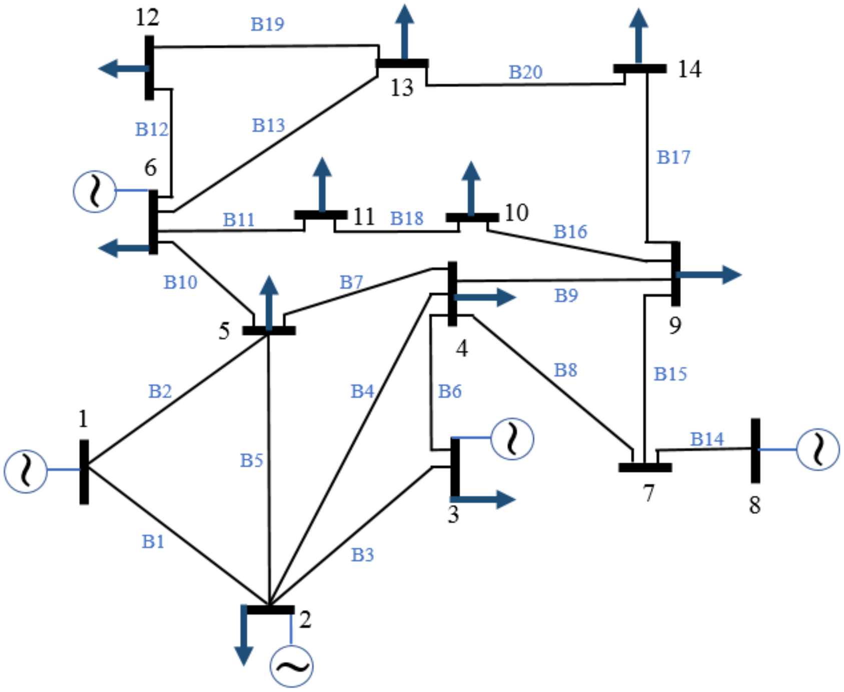

Fig. 3. IEEE 14-bus test system diagram

Note that in the load redistribution attack, the output measurements of the generators should not be attacked. The attacker's goal is to execute a load redistribution attack without being detected by the system control center with the following assumptions:

1) The attacker has complete information about network topology and network parameter.

2) The attacker has the ability to change the load and flow measurements of the line.

Table 1. Attack vector C (voltage angles) to increase the flow of line 12

Bus No.	*vector C*	*Bus No.*	*vector C*	*Bus No.*	*vector C*
1	0	6	0	11	*-0.34*
2	0	7	0	12	*0.7*
3	0	8	0	13	*0.6*
4	0	9	0	14	*1.38*
5	0	10	*-0.35*		

As an example, we consider the target line to be the 12th (B12) line between the 6th and 12th buses. Assuming that bus number 6 is the reference bus. The maximum flow change on the line by implementing the LR attack based on proposed method is determined to be 2.14 MW.

Now, based on the attack vector (changes in the bus voltage angle) (Table 1) and the bus voltage angle in the

Now, based on the amount of load changes and the existing relationship between the state vector (voltage angle of buses), load changes and system susceptance matrix, the value of state vector C (voltage angle of buses) can be determined (table 1).

non-attack mode (Table 2), we get the system voltage angle after the attack (Table 3). Figure 4 shows the change in measurements after and before the attack.

Table 2. voltage angle *x* without attack

Bus No.	*vector C*	*Bus No.*	*vector C*	*Bus No.*	*vector C*
1	*-5.53*	6	*0*	11	*-16.54*
2	*-14.2*	7	*-14.75*	12	*-17.02*
3	*-11.41*	8	*-14.75*	13	*-17.06*
4	*-9.76*	9	*-16.51*	14	*-17.9*

5	*-16.08*	10	*-16.75*		

Table 3. voltage angle $\hat{x} = x + c$ with attack

Bus No.	*vector C*	*Bus No.*	*vector C*	*Bus No.*	*vector C*
1	*-5.53*	6	*0*	11	*-16.2*
2	*-14.2*	7	*-14.75*	12	*-17.72*
3	*-11.41*	8	*-14.75*	13	*-17.66*
4	*-9.76*	9	*-16.51*	14	*-19.27*
5	*-16.08*	10	*-16.4*		

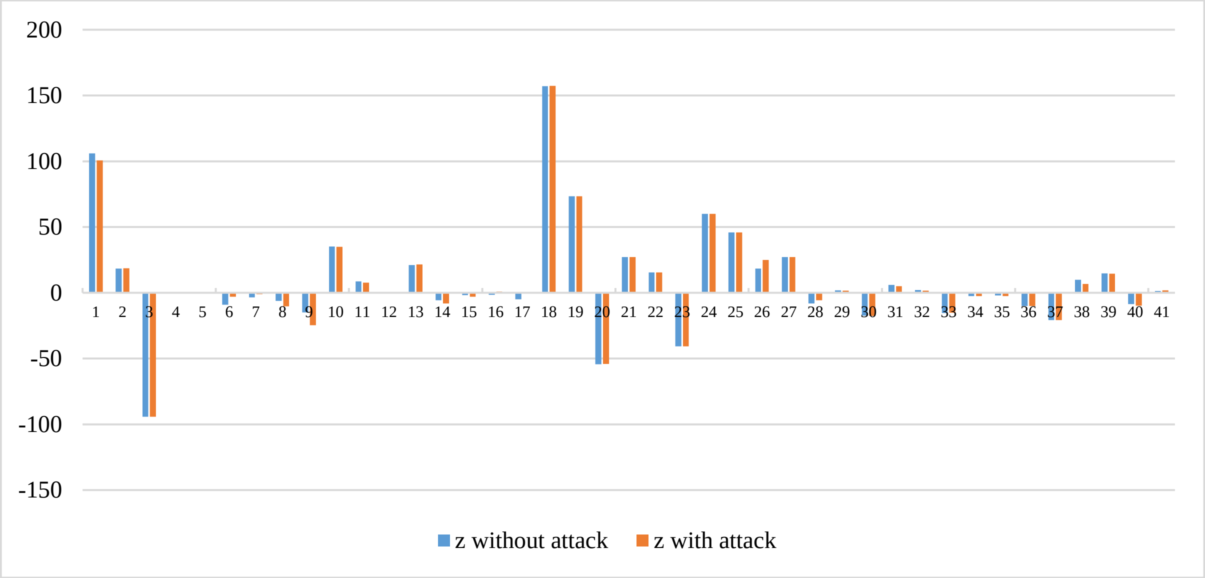

Fig. 4. System measurement values before and after the attack

When the attacker finishes designing and manipulating the measurements, the new measurement data will be entered into the SCADA system and then they will be entered into the estimation system section. The state estimation system estimates the state vectors and checks their residual (r<τ). The output of the state estimation system was the state vectors (Table 3) and based on these state vectors and the power flow problem, the load values (Figure 5) and system generation are determined. Based on the consumption load values obtained from the previous step, optimal power flow is implemented, which determines the optimal amount of generator generation in optimal power flow (Figure 6) and these values will be the new generation values of generators for the next time frame of the system. The point here is that the generation values of the generators have been determined based on the manipulated cyber load, while in our main system the load values were the same as the initial values, so this issue disrupts the normal operation of the system and causes overflow (Figure 7) is on the lines.

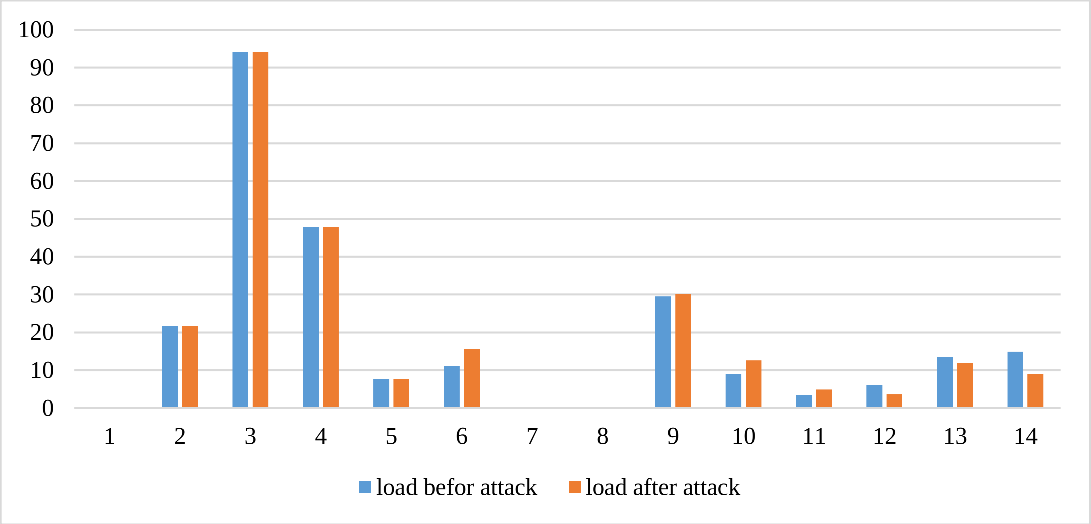

Fig. 5. Cyber load values of the system before and after the attack

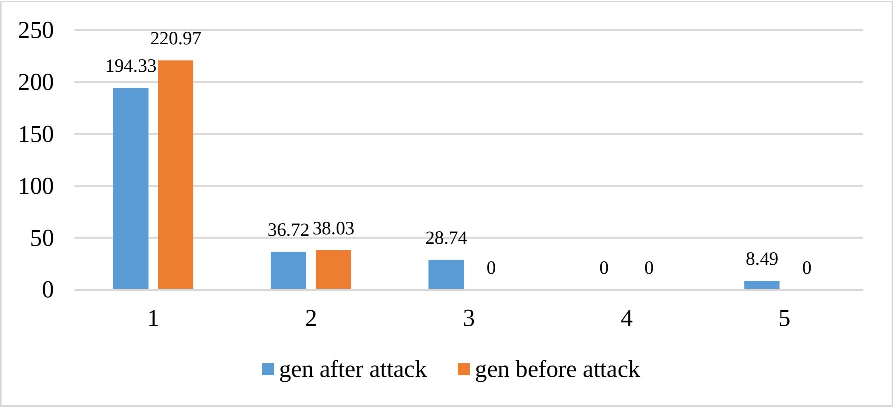

Fig. 6. Generation values of generators based on cyber load obtained from OPF

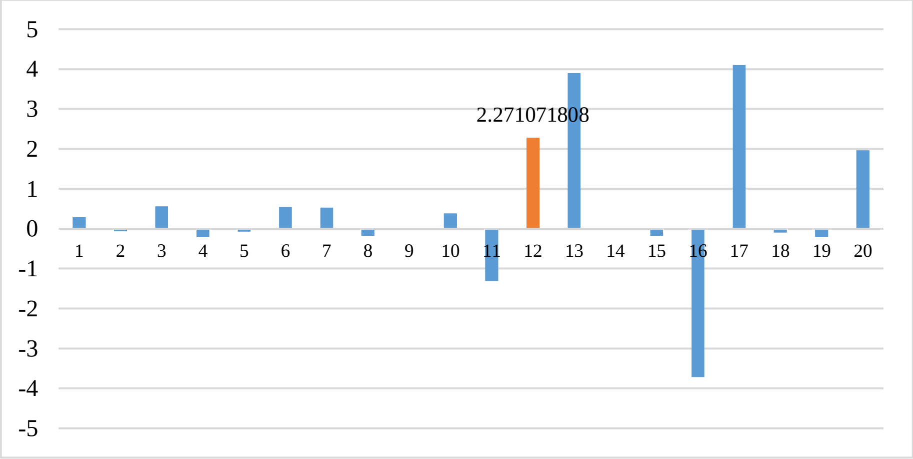

Fig. 7. Changes in power flow of lines after applying new generation values to the system in the presence of real load

B. PMU allocation

We begin by looking at how cyber risk affects the best allocation approach. The attacker is assumed to target just one PMU in this comparison, and the odds of successful compromise are set to 0, 0.01, 0.05, 0.1, and 0.5, respectively. Keep in mind that a compromise chance of 0 indicates that there is no cyber danger, and that other probabilities indicate varying degrees of risk (i.e., the larger probability, the more risk). Additionally, we consider the transmission line's dependability to be 0.99.

PMUs are placed using the greedy procedure. Table 4 presents the best tactics for various levels of cyber risk. If there is no cyber risk, it can be shown that an extra 4 PMUs are needed, bringing the total number of observables up to 20. However, if there is a cyber-risk, 3 or more extra PMUs are needed to ensure the risk level, and there are more than 20 observables in all. We see that as the probability is compromised, the number of PMUs needed grows. As an illustration, as the compromise probability rises from 0 to 0.5, the number of PMUs needed for the IEEE 14-bus increases from 4 to 9.

It would be interesting to research the effects of ignoring cyber threats in real-world situations. We take into account the following two PMU deployment possibilities from Table 4 and 5 for this purpose.

Table 4. PMU location where 'No.' indicates the total number of additional PMUs.

Sensitive Buses	*{6,7,12,13,14}*	
Manipulated probability	*PMU Location*	*No.*
0	*{2,7,10,13}*	*4*
0.01	*{2,6,7,11,12,13,14}*	*7*
0.05	*{2,6,7,10,11,12,13,14}*	*8*
0.1	*{1,4,6,7,8,10,11,12,13,14}*	*9*
0.5	*{1,4,6,7,8,10,11,12,13,14}*	*9*

Table 5. PMU Location where 'No.' indicates the total number of additional PMUs.

Sensitive Buses	*{8,12,13,14,19,30,33,38,70,77,80,94,97,98,101}*							
Manipulated probability	*PMU Location*							*No.*
0	*21*	*17*	*15*	*12*	*9*	*5*	*3*	*32*
	44	*40*	*36*	*30*	*29*	*23*		
	64	*62*	*57*	*54*	*51*	*46*		
	87	*85*	*80*	*77*	*75*	*71*		
	115	*110*	*105*	*102*	*94*	*90*		
	116							
0.01	*14*	*13*	*12*	*10*	*8*	*5*	*1*	*39*
	32	*31*	*30*	*27*	*21*	*19*		
	45	*40*	*38*	*36*	*34*	*33*		
	70	*64*	*62*	*56*	*52*	*49*		
	91	*87*	*85*	*80*	*77*	*71*		
	110	*105*	*101*	*98*	*97*	*94*		
	118	*116*						
0.05	*14*	*13*	*12*	*10*	*8*	*5*	*1*	*40*
	30	*28*	*27*	*24*	*22*	*19*		
	40	*38*	*36*	*34*	*33*	*32*		
	63	*62*	*56*	*52*	*49*	*45*		
	87	*85*	*80*	*77*	*73*	*70*		
	94	*91*						
0.1	*14*	*13*	*12*	*10*	*8*	*5*	*1*	*43*
	30	*28*	*27*	*24*	*22*	*19*		
	40	*38*	*36*	*34*	*33*	*32*		
	63	*62*	*56*	*52*	*49*	*45*		
	85	*82*	*80*	*77*	*73*	*70*		
	90	*86*						

0.5	*14*	*13*	*12*	*10*	*8*	*5*	*1*	*43*
	30	*28*	*27*	*24*	*22*	*19*		
	40	*38*	*36*	*34*	*33*	*32*		
	63	*62*	*56*	*52*	*49*	*45*		
	85	*82*	*80*	*77*	*73*	*70*		
	90	*86*						

6. Conclusion

In this research, we create measures to shield against LR assaults. We look into many approaches to see which works best for allocating resources. Case studies are conducted using a representative IEEE test system. It is possible that this research will help provide light on how to best spend scarce financial and defensive resources to safeguard the electrical grid against possible LR attacks. To begin, we borrowed concepts from the field of power systems to develop a usable model for the core difficulty of LR attacks. The proposed defense mechanism seeks to determine which buses have the biggest impact on a particular transmission asset by showing that a straightforward greedy algorithm can optimally solve this model. According to the results, the greedy approach is quite fast; finding the global solution only takes a few milliseconds (for each transmission asset). Once the PMU-observable system and sensitive buses have been determined, the PMU allocation can be determined. Given that different PMU initializations might lead to significantly different optimal techniques for assigning PMUs, our approach is superior to the heuristic approach.

REFERENCES

[1] J. Zheng, D. W. Gao, and L. Lin, “Smart meters in smart grid: An overview,” in *2013 IEEE green technologies conference (GreenTech)*, IEEE, 2013, pp. 57–64.

[2] M. H. Amini, K. G. Boroojeni, C. J. Wang, A. Nejadpak, S. S. Iyengar, and O. Karabasoglu, “Effect of electric vehicle parking lots’ charging demand as dispatchable loads on power systems loss,” in *2016 IEEE International Conference on Electro Information Technology (EIT)*, IEEE, 2016, pp. 499–503.

[3] F. Kamyab, M. Amini, S. Sheykhha, M. Hasanpour, and M. M. Jalali, “Demand response program in smart grid using supply function bidding mechanism,” *IEEE Trans Smart Grid*, vol. 7, no. 3, pp. 1277–1284, 2015.

[4] K. G. Boroojeni, M. H. Amini, S. S. Iyengar, M. Rahmani, and P. M. Pardalos, “An economic dispatch algorithm for congestion management of smart power networks: An oblivious routing approach,” *Energy Systems*, vol. 8, pp. 643–667, 2017.

[5] J. A. Lewis, “The electrical grid as a target for cyber attack,” *Center for Strategic and International Studies*, 2010.

[6] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, *Smart grids: security and privacy issues*, vol. 221. Springer, 2017.

[7] K. G. Boroojeni, M. H. Amini, S. S. Iyengar, K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, “Overview of the security and privacy issues in smart grids,” *Smart grids: security and privacy issues*, pp. 1–16, 2017.

[8] 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, pp. 1–33, 2011.

[9] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *IEEE Trans Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[10] 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.

[11] M. H. Amini, J. Frye, M. D. Ilić, and O. Karabasoglu, “Smart residential energy scheduling utilizing two stage mixed integer linear programming,” in *2015 North American Power Symposium (NAPS)*, IEEE, 2015, pp. 1–6.

[12] W. Deng, Z. Xiang, K. Huang, J. Liu, C. Yang, and W. Gui, “Detecting Intelligent Load Redistribution Attack Based on Power Load Pattern Learning in Cyber-Physical Power Systems,” *IEEE Transactions on Industrial Electronics*, 2023.

[13] J. Liang, L. Sankar, and O. Kosut, “Vulnerability analysis and consequences of false data injection attack on power system state estimation,” *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2015.

[14] M. S. Ghazizadeh and M. R. Aghamohammadi, “A Deep Learning-Based Attack Detection Mechanism against Potential Cascading Failure Induced by Load Redistribution Attacks,” *IEEE Trans Smart Grid*, 2023.

[15] J. Salmeron, K. Wood, and R. Baldick, “Analysis of electric grid security under terrorist threat,” *IEEE Transactions on power systems*, vol. 19, no. 2, pp. 905–912, 2004.

[16] X. Liu, Z. Li, Z. Shuai, and Y. Wen, “Cyber attacks against the economic operation of power systems: A

fast solution," *IEEE Trans Smart Grid*, vol. 8, no. 2, pp. 1023–1025, 2016.

[17] Z. Liu and L. Wang, "Defense strategy against load redistribution attacks on power systems considering insider threats," *IEEE Trans Smart Grid*, vol. 12, no. 2, pp. 1529–1540, 2020.

[18] R. Kaviani and K. W. Hedman, "Identifying an exploitable structure for the core problem of load-redistribution attack problems," in *2019 North American Power Symposium (NAPS)*, IEEE, 2019, pp. 1–6.

[19] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

[20] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

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

[22] 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, 2013.

[23] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[24] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, IEEE, 2012, pp. 212–219.

[25] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 223–232, 2014.

[26] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans Emerg Top Comput*, vol. 1, no. 2, pp. 273–285, 2013.

[27] A. Khaleghi, M. O. Sadegh, M. Ghazizadeh-Ahsaee, and A. M. Rabori, "Transient fault area location and fault classification for distribution systems based on wavelet transform and adaptive neuro-fuzzy inference system (ANFIS)," *Advances in Electrical and Electronic Engineering*, vol. 16, no. 2, pp. 155–166, 2018.

[28] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, IEEE, 2011, pp. 380–388.

[29] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2012.

[30] M. H. Amini, M. Rahmani, K. G. Boroojeni, G. Atia, S. S. Iyengar, and O. Karabasoglu, "Sparsity-based error detection in DC power flow state estimation," in *2016 IEEE International Conference on Electro Information Technology (EIT)*, IEEE, 2016, pp. 263–268.

[31] 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, pp. 1–33, 2011.

[32] D. Deka, R. Baldick, and S. Vishwanath, "Jamming aided generalized data attacks: Exposing vulnerabilities in secure estimation," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, 2016, pp. 2556–2565.

[33] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[34] 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, pp. 1427–1440, 2016.

[35] A. Khaleghi, M. O. Sadegh, and M. G. Ahsaee, "Permanent Fault Location in Distribution System Using Phasor Measurement Units (PMU) in Phase Domain.," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 8, no. 5, 2018.

[36] F. Aminifar, M. Fotuhi-Firuzabad, and A. Safdarian, "Optimal PMU placement based on probabilistic cost/benefit analysis," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 566–567, 2012.