Iranian Journal of Electrical and Electronic Engineering 04 (2022) 2569
Microgrid Special Issue 2022: Operation, Control, and Applications

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Research Paper

Resilient Configuration of Distribution System versus False Data Injection Attacks Against State Estimation

R. Behnam*(C.A.), and G. B. Gharehpetian *

Abstract: State estimation is used in power systems to estimate grid variables based on meter measurements. Unfortunately, power grids are vulnerable to cyber-attacks. Reducing cyber-attacks against state estimation (SE) is necessary to ensure power systems safe and reliable operation. False data injection (FDI) is a type of cyber-attack that tampers with measurements. This paper proposes network reconfiguration as a strategy to decrease FDI attacks on distribution system SE. It is well-known that network reconfiguration is a common approach in distribution systems to improve the system's operation. In this paper, a modified switch opening and exchange (MSOE) method is used to reconfigure the network. The proposed method is tested on the IEEE 33-bus and IEEE 69-bus systems. It is shown that network reconfiguration decreases the power measurements manipulation under false data injection attacks. Also, the resilient configuration of the distribution system is achieved, and the best particular configuration for reducing FDI attacks on each bus is obtained.

Keywords: Cyber-attack, false data injection (FDI) attacks, distribution system reconfiguration, state estimation.

1 Introduction

DUE to the combination of information and communications technology with measurements in distribution systems, the measurements are significantly threatened by cyber-attacks [1]. For example, Ukraine's power grid experienced a significant blackout because of cyber-attacks in 2015 [2]. In 2019, Venezuela's power system experienced several cyber-attacks resulting in massive blackouts [3].

State estimation (SE) is applied to determine distribution system state variables according to meter measurements, and then the estimated state will be used to monitor the system [4].

Iranian Journal of Electrical and Electronic Engineering, 2022. Paper first received 20 Jun 2022, revised 11 Oct 2022, and accepted 01 Oct 2022

*The authors are with the Electrical Engineering Department Faculty, Amirkabir University of Technology, Tehran, Iran. E-mails: reza.be74@aut.ac.ir, and grptian@aut.ac.ir. Corresponding Author: R. Behnam.

https://doi.org/10.22068/IJEEE.18.4.2569

Many recent types of research have focused on the effect of FDI on SE. For example, the impact of FDI on SE, which misleads system operators, was first introduced in [5]. Monitoring and controlling the power system play a crucial role in maintaining a power system's safe and reliable operation. In this regard, cyber security is considered too important. Cyber-attacks are categorized into three types: physical, communication, and information attacks. Physical device damage, such as measurement devices, is the target of physical attacks. The target of communication attacks is manipulating communication protocols. In information attacks, FDI is used to tamper with control system commands, which are based on measurements. The impacts of cyber-attacks against voltage control in distribution systems, when several photovoltaic systems are connected, have been presented in [6]. One of the topics in stealthy attacks is the security index. The security index is a benchmark that is used to determine the slightest effort to manipulate each measurement. The security index has been studied in

[7]; two indices have been used to quantify the least effort needed to perform a successful FDI attack against particular measurements. The attackers require to know the entire network topology to increase the successful attack rate, but access to all information is difficult for attackers [8-9]. FDI attacks with incomplete information have been investigated in [10]. In [11], a FDI attack has been executed on automatic synchronization systems in microgrids, the attack has manipulated the synchronization, and also the attack has led to the microgrid blackout.

Simple FDI can be detected by bad data detection and identification algorithms. Currently, the detection strategy of FDI is categorized into three types: state-estimation-based, trace-prediction-based, and artificial-intelligence-based strategy. A matrix separation was used for the detection of FDI attacks on the power grid in [12]. In [13], two machine learning-based techniques have been used to detect FDI attacks in smart grids. In [14], a strategy based on a dimensionality-reduction method and a Gaussian mixture model has been proposed to detect cyber-attacks. In [15], the authors have used a neural-network algorithm to detect the FDI attack in real time. In [16], the authors have used a neural-network based algorithm to detect the FDI attack in real time. However, the proposed algorithm could not reduce the impacts of FDI attacks. In [17], an image processing algorithm and deep convolutional neural network have been used to detect FDI attacks. Graph signal processing has been used to detect FDI attacks, and the Graph Fourier Transform of the phase angles has been used for FDI attack detection.

Normally closed (sectionalizing) and normally opened (tie) switches are the two types of switches in distribution systems. Network reconfiguration is based on changing the status of switches. Network topologies have been assumed to have a fixed structure in most of the research, but operators alter the topology of the network for different reasons. The topology of conventional distribution systems is usually radial with unidirectional power flows [18]. Many recent types of research on network reconfiguration have focused on issues such as; reconfiguration for power loss reduction in distribution systems [19]. In [20], the objective function of reconfiguration was to improve reliability and reduce power losses. In this paper, network reconfiguration will be used as a strategy to take action against FDI attacks. In this paper, it is assumed that attackers mislead the distribution system operator by injecting false data to change SE (bus voltage) data. The main contributions of this paper are as follows:

- An objective function is proposed to determine the impacts of FDI attacks against SE (voltage bus) on active and reactive power measurements.
- Network reconfiguration is used as a strategy to reduce FDI attacks effects.
- The best configuration of the distribution system is determined to decrease FDI attacks effects on each bus.
- (MSOE) method are applied as a strategy to reconfigure the network.

The rest of the paper is organized as follows: The FDI attacks against SE and the objective function are presented in section II and section III, respectively. Section IV introduces network reconfiguration as an algorithm to reduce FDI attacks and shows the proposed network reconfiguration procedure. The impacts of the proposed algorithm on the IEEE 33-bus and 69-bus systems are studied in section V. Finally, in section VI, the conclusions are drawn, and the direction for prospective research is suggested.

2 State estimation Estimation

In [21], the authors have proposed the distribution system state estimation model based on the nodal voltage. For the reliability of distribution systems, it is necessary real-time monitoring of the system. Meters are used to monitor the distribution systems, and operators estimate the state of the system by these meter measurements. A set of variables (usually voltage magnitudes and phase angles) for calculating the other quantities of a distribution system, if they are known, is called the system state. So, the distribution system operating point is determined by the system state. It is assumed that m meters are usually used to monitor a distribution system with s state variables ($m>s$ which indicates measurement redundancy). As a result, the distribution system can be seen/observed by these meters. The state estimation involves estimating state variables $x \in R$ when they are based on meter measurements $z \in R$, where noise $e \in R$ is independent and follows a distribution with zero mean. The relation between meter measurements z and state variables x is represented, as follows:

$$z = h(x) + e \tag{1}$$

where, $h(x) = [h1(x), \dots, hi(x), \dots, hm(x)]$ are measurements and functions of x.

The purpose of state estimation is to estimate state variables x that is the best fit of meter measurements z according to the equation 1. Weighed least squares (WLS) are the basic approach to the state estimation. The WLS based state estimation is to solve the following optimization problem:

$$\min_x J(x) = \sum_{i=1}^{m} w_i [z_i - h_i(x)]^2 = [z - h(x)]^T W [z - h(x)] \quad (2)$$

where, w_i represents the weight associated with the meter measurement z_i. The solution of the optimization problem 2 gives the best estimated state $\hat{x}$ which must satisfy the following optimization condition:

$$\partial J(x) / \partial x = 0 \Rightarrow H^T(\hat{x}) W [z - h(\hat{x})] = 0 \quad (3)$$

where, $H(x)=\partial h(x)/\partial x$ is the Jacobian matrix of the measurement functions h(x). The solution of this nonlinear equation can be obtained by different iterative methods. To compute the correction Δx^k, an equation of the following type is solved at each iteration:

$$[G(x^k)]\Delta x^k = H^T(x^k) W [z - h(x^k)] \quad (4)$$

where, $k \in N$ denotes the index of iterations. This equation is called the normal equation of the WLS based state estimation, where $G(x)$ is called the gain function and is usually chosen as:

$$G(x) = H^T(x) W H(x) \quad (5)$$

The AC state estimation has been represented in detail in [22].

3 FDI Attacks Model

In this paper, the attacker can manipulate the voltage of buses during the SE procedure. The FDI in a distribution system SE model is introduced as follows:

$$\Delta V_{i,mea} = a_{V_i} \quad (6)$$

where, $a_{V_i} \in \Re$ is defined as the FDI in the bus i voltage. The FDI on the bus voltage causes a change in the current measurement. The change of the original current measurement is expressed as follows:

$$\Delta I_{i,mea} = a_{I_i} \quad (7)$$

where, a_{I_i} is the change in the original current measurement. The changes of the original power measurements of the bus i under the cyber-attack are:

$$\left(\frac{P_i + jQ_i + \Delta P_i + j\Delta Q_i}{V_{i,are} + jV_{i,aim}} \right)^* = \left(I_{i,re} + jI_{i,im} \right) + \left(a_{I_{i,re}} + ja_{I_{i,im}} \right) \quad (8)$$

where, $V_{i,are}$ and $V_{i,aim}$ stand for the real and imaginary part of the voltage at bus i after the FDI attack, respectively. Thus, $V_{i,are} = V_{i,re} + \Delta V_{i,re}$ and $V_{i,aim} = V_{i,im} + \Delta V_{i,im}$. $\Delta V_{i,re}$ and $\Delta V_{i,im}$ represent the change of the real and imaginary parts of the bus voltage state after a cyber-attack, respectively. P_i and Q_i are the active and reactive powers injection at the bus i, respectively. ΔP_i and ΔQ_i represent the change of the active and reactive powers injection at the bus i, respectively. $I_{i,re}$ and $I_{i,im}$ denote the real and imaginary part of the current injection at bus i. $a_{I_{i,re}}$ and $a_{I_{i,im}}$ are the real and imaginary parts of the FDI in the current measurement, respectively.

Under cyber-attack, the changes of the active and reactive powers following out of bus i are rewritten, as follows:

$$\frac{[(P_i + \Delta P_i)V_{i,are} + (Q_i + \Delta Q_i)V_{i,aim}]}{V_{i,are}^2 + V_{i,aim}^2} + j\frac{[(P_i + \Delta P_i)V_{i,aim} - (Q_i + \Delta Q_i)V_{i,are}]}{V_{i,are}^2 + V_{i,aim}^2} = \left(I_{i,re} + a_{I_{i,re}} \right) + j\left(I_{i,im} + a_{I_{i,im}} \right) \quad (9)$$

According to equation (9), ΔP_i and ΔQ_i will obtain, as follows:

$$(P_i + \Delta P_i)V_{i,are} + (Q_i + \Delta Q_i)V_{i,aim} = \left(I_{i,re} + a_{I_{i,re}} \right)(V_{i,are}^2 + jV_{i,aim}^2) \quad (10)$$

$$(P_i + \Delta P_i)V_{i,aim} - (Q_i + \Delta Q_i)V_{i,are} = \left(I_{i,im} + a_{I_{i,im}} \right)(V_{i,are}^2 + jV_{i,aim}^2) \quad (11)$$

Considering $I_{i,re}$ and $I_{i,im}$, as follows:

$$I_{i,re} = \frac{P_i V_{i,re} + Q_i V_{i,im}}{V_{i,re}^2 + V_{i,im}^2} \quad (12)$$

$$I_{i,im} = \frac{P_i V_{i,im} - Q_i V_{i,re}}{V_{i,re}^2 + V_{i,im}^2} \quad (13)$$

According to equations (12) and (13), the equations (10) and (11) will be rewritten as follows:

$$P_i\Delta V_{i,re}+\Delta P_i\Delta V_{i,re}+\Delta P_i V_{i,re}+P_i V_{i,re}+Q_i\Delta V_{i,im}+\Delta Q_i\Delta V_{i,im}+\Delta Q_i V_{i,im}+Q_i V_{i,im}$$
$$=\left(\frac{P_i V_{i,re}+Q_i V_{i,im}}{V_{i,re}^2+V_{i,im}^2}+a_{I_{i,re}}\right)((V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2) \quad (14)$$

$$P_i\Delta V_{i,im}+\Delta P_i\Delta V_{i,im}+\Delta P_i V_{i,im}+P_i V_{i,im}-Q_i\Delta V_{i,re}-\Delta Q_i\Delta V_{i,re}-\Delta Q_i V_{i,re}-Q_i V_{i,re}$$
$$=\left(\frac{P_i V_{i,im}-Q_i V_{i,re}}{V_{i,re}^2+V_{i,im}^2}+a_{I_{i,im}}\right)((V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2) \quad (15)$$

By solving equations (14) and (15), ΔP_i and ΔQ_i will be obtained, as follows:

$$\Delta P_i=\frac{(V_{i,re}+\Delta V_{i,re})(a'_{I_{i,re}}-K_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2}+\frac{(V_{i,im}+\Delta V_{i,im})(a'_{I_{i,im}}-J_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2} \quad (16)$$

$$\Delta Q_i=\frac{(V_{i,im}+\Delta V_{i,im})(a'_{I_{i,re}}-K_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2}-\frac{(V_{i,re}+\Delta V_{i,re})(a'_{I_{i,im}}-J_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2} \quad (17)$$

where,

$$a'_{I_{i,re}}=a_{I_{i,re}}((V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2) \quad (18)$$

$$K_i'=P\Delta V_{re}+Q\Delta V_{im}-K_i \quad (19)$$

$$K_i=\left(\frac{P_i V_{i,re}+Q_i V_{i,im}}{V_{i,re}^2+V_{i,im}^2}\right)\times(\Delta V_{i,re}^2+2V_{i,re}\Delta V_{i,re}+\Delta V_{i,im}^2+2V_{i,im}\Delta V_{i,im}) \quad (20)$$

$$a'_{I_{i,im}}=a_{I_{i,im}}((V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2) \quad (21)$$

$$J_i'=P\Delta V_{im}-Q\Delta V_{re}-J_i \quad (22)$$

$$J_i=\left(\frac{P_i V_{i,im}-Q_i V_{i,re}}{V_{i,re}^2+V_{i,im}^2}\right)\times(\Delta V_{i,re}^2+2V_{i,re}\Delta V_{i,re}+\Delta V_{i,im}^2+2V_{i,im}\Delta V_{i,im}) \quad (23)$$

As we know,

$$a_{I_i}=-(Y_{i,re}+jY_{i,im})(\Delta V_{i,re}+j\Delta V_{i,im}) \quad (24)$$

So, $a_{I_i,re}$ and $a_{I_i,im}$ are calculated as follows:

$$a_{I_i,re}=-(\Delta V_{i,re}Y_{i,re}-\Delta V_{i,im}Y_{i,im}) \quad (25)$$

$$a_{I_i,im}=-(\Delta V_{i,re}Y_{i,im}+\Delta V_{i,im}Y_{i,re}) \quad (26)$$

So, equations (16) and (17) are rewritten as follows:

$$\Delta P_i=\frac{(V_{i,re}+\Delta V_{i,re})(-(\Delta V_{i,re}Y_{i,re}-\Delta V_{i,im}Y_{i,im})-K_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2}+\frac{(V_{i,im}+\Delta V_{i,im})(-(\Delta V_{i,re}Y_{i,im}+\Delta V_{i,im}Y_{i,re})-J_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2} \quad (27)$$

$$\Delta Q_i=\frac{(V_{i,im}+\Delta V_{i,im})(-(\Delta V_{i,re}Y_{i,re}-\Delta V_{i,im}Y_{i,im})-K_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2}-\frac{(V_{i,re}+\Delta V_{i,re})(-(\Delta V_{i,re}Y_{i,im}+\Delta V_{i,im}Y_{i,re})-J_i')}{(V_{i,re}+\Delta V_{i,re})^2+(V_{i,im}+\Delta V_{i,im})^2} \quad (28)$$

According to equations (27) and (28), the NR, by changing parameters (bus voltage and admittances connected to each bus) in these equations can reduce the FDI impacts against SE on power measurements.

In equation (29), the normalized values ($x^{norm}=\frac{x-x_{\min}}{x_{\max}-x_{\min}}$) of ΔP and ΔQ are used to minimize the impacts of the FDI:

$$F_{FDI}=\alpha_1.|\Delta P|^{norm}+\alpha_2.|\Delta Q|^{norm} \quad (29)$$

where, F_{FDI} represents the effects of FDI at the power measurements of the bus under attack. α_1 and α_2 are weighting factors. In this paper, the importance of the active and reactive power for system operators is the same.

Based on equation (29), it can be said that for each bus under attack, a resilient configuration can be found. So, the purpose is to find the best particular resilient configuration which can be applied for all FDI attacks. Therefore, $F_{FDI,tot}$ is suggested by the following equation:

$$F_{FDI,total}=\sum_{j=1}^{N}\beta_j.F_{FDI,j} \quad (30)$$

where, $F_{FDI,j}$ is the objective function, given by equation (29), when FDI attack has occurred on bus *j*. *N* and β_j are the number of buses in the system and weighting factors, respectively. It is assumed that the importance of the busses is the same.

To minimize the objective function given in (30), some constraints should be considered. These constraints are described as follows:

- Power source limit: Total loads of a network must lie under the capacity limit of the power source.
- Voltage constraint: The voltage magnitude of each bus must lie within allowable limits.
- Current constraint: Current magnitude of each branch cannot exceed the permission ranges.
- Radial network constraint: Network topology must be radial, which means the number of nodes should be larger than the number of lines by one unit.
- Feasibility: Each node should be connected to at least one other node. This means all the nodes must be energized.

4 Proposed Algorithm

There are numerous techniques for network reconfiguration [23]. A review of different approaches for distribution network reconfiguration has been presented in [24]. The (MSOE) is a valuable algorithm with strong search ability. Due to accuracy in solving and the optimality of the proposed method in comparison to other algorithms, the (MSOE) method is used to reconfigure the network in current research.

The main idea of the (MSOE) algorithm can be described in two steps. In the first step, the initial status of each switch is assumed to be closed, and this assumption will make loops in the network. The objective function in the system for each open switch was determined. Then, a switch with the minimum objective function has been selected.

Based on the minimum objective function, the other tie-switches have been selected. In the next iterations, all switches in the previous tie-switch loop must be removed from the search space of possible tie-switches. In step 2, the status of a sectionalizing switch in the initial topology has been changed to a tie-switch, and step 1 was run to get an optimal topology [25]. The overview of the steps of the proposed algorithm is given in Fig. 1 like a flowchart.

5 Case Studies

In this section, the IEEE 33-bus system and IEEE 69-bus systems shown in Fig. 2 and 3, are used to demonstrate the performance of the proposed strategy. The 33-bus test system has been used for feeder reconfiguration in many types of research. The data of this network is given in [26]. The system consists of one source transformer, 32 bus bars, and five tie switches; the dashed line s33, s34, s35, s36, and s37 represent the tie switches. The location and number of the measurements are the same as the line numbers.

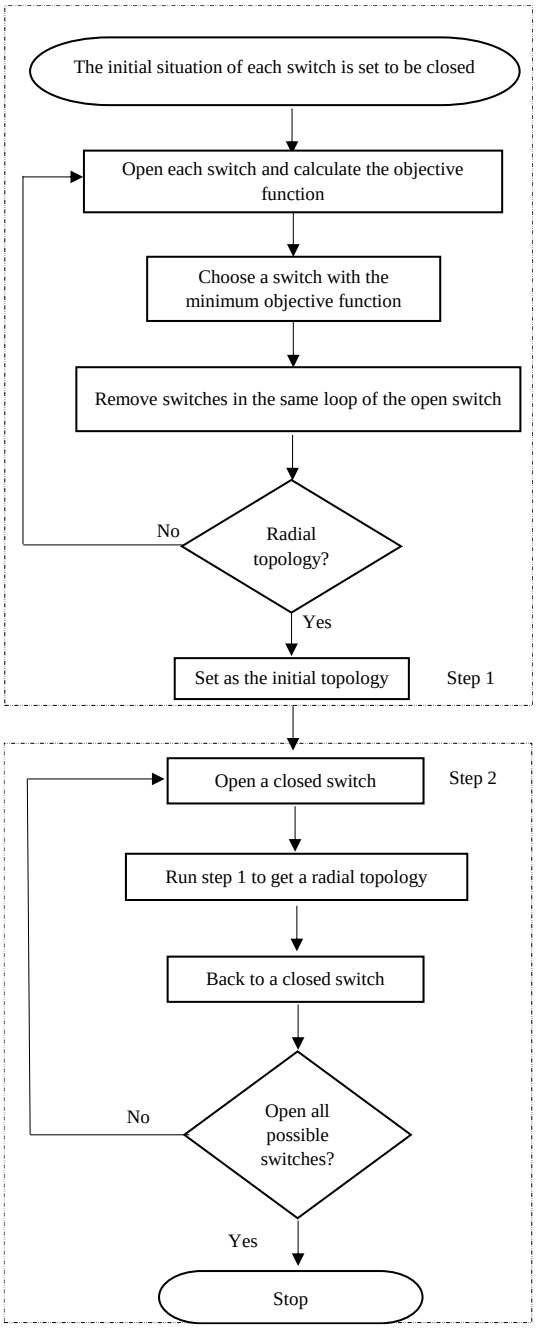


Fig. 1 Flowchart of the modified and exchange method.

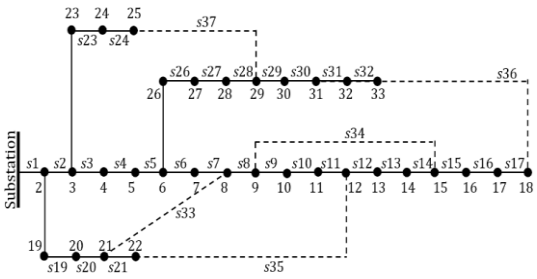


Fig. 2 IEEE 33-bus system.

Table 1 Resilient configurations for FDI attacks on different buses

Number of bus	Open switch	$F_{FDI}*10^{-3}$(pu)			$F*10^{-3}$(pu)		
		$\lvert\Delta P\rvert$	$\lvert\Delta Q\rvert$	F	$\lvert\Delta P\rvert$	$\lvert\Delta Q\rvert$	F
2	s14, s20, s21, s32,s37	140	57	100	150	58	100
3	s14, s20, s21, s32,s37	47	15	31	56	20	38
4	s14, s20, s21, s32,s37	23	2.7	13	45	14	29
5	s14, s20, s21, s32,s37	6.1	2.8	4.5	29	11	20
6	s13, s19, s21, s31,s37	0.1	1.1	0.6	54	30	42
7	s10, s12, s19, s31,s37	0.2	0.4	0.3	12	13	13
8	s12, s20, s21, s24,s36	0.3	0.5	0.4	12	3.1	7.6
9	s12, s21, s33, s36,s37	0.1	0.4	0.2	13	6.5	9.8
10	s12, s21, s33, s36,s37	0.7	1.1	0.9	51	10	30
11	s12, s21, s33, s36,s37	1.1	1.4	1.2	67	11	39
12	s12, s21, s33, s36,s37	0.8	0.5	0.7	27	6.1	17
13	s20, s34, s35, s36,s37	1.5	0.8	1.1	12	9.4	11
14	s20, s34, s35, s36,s37	2.1	1.1	1.6	17	13	15
15	s10, s12, s19, s31,s37	0.2	0.4	0.3	19	11	15
16	s9, s12, s19, s28,s32	0.3	0.1	0.2	12	7.4	9.6
17	s12, s19, s24, s32,s35	0.2	0.3	0.2	12	7.7	9.6
18	s23, s32, s33, s34,s35	0.2	0.3	0.2	12	7.7	9.6
19	s11, s14, s17, s33,s37	5	17	11	41	27	34
20	s11, s14, s17, s33,s37	2.5	6.7	4.6	16	13	15
21	s12, s15, s20, s21,s23	0.2	0.2	0.2	18	16	17
22	s7, s23, s34, s35,s36	0	0.2	0.1	2.9	2	2.4
23	s19, s28, s32, s34,s35	0.4	1.2	0.8	24	12	18
24	s16, s28, s33, s34,s35	0	1	0.5	15	8.1	12
25	s19, s28, s32, s34,s35	0	0.3	0.2	15	8.1	12
26	s12, s21, s23, s33,s36	1	8.2	4.6	68	21	45
27	s14, s20, s21, s27,s30	1.8	1.1	1.4	34	13	23
28	s17, s21, s23, s33,s34	0.5	1	0.8	13	8.1	11
29	s15, s21, s33, s34,s37	0.8	0.3	0.6	23	9.6	16
30	s14, s20, s21, s30,s37	0	4.9	2.5	21	8.8	15
31	s19, s32, s34, s35,s37	4.4	0.6	2.5	20	16	18
32	s23, s32, s33, s34,s35	4	1.4	2.7	24	23	24
33	s17, s21, s33, s34,s37	2	2.3	2.1	9.7	11	10

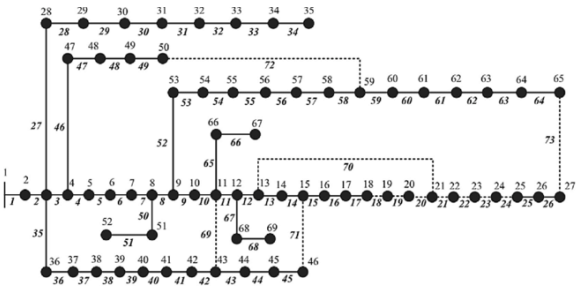


Fig. 3 IEEE 69-bus system.

In Table 1, it is assumed that the attacker can compromise the SE for the voltage on each node of the IEEE-33 bus system. The attacker can decrease the voltage magnitude and voltage angle of each bus by 0.01 p.u, and 0.1 degrees. Table 1 lists the resilient configuration for each FDI attack and compares the objective function of the resilient configuration topology with the initial topology. These simulations can be repeated for different magnitudes of FDI attacks. As it can be seen in this table, the resilient configuration of the system depends on the location of the FDI attack. According to the results of this table, reconfiguration can reduce the impacts of FDI on the active and reactive power measurements.

Also, Table 1 compares the objective functions of initial topology and reconfigured topologies. As we can see from this table, the network reconfiguration can reduce the impacts of the FDI on the power measurements. In the next stage, the magnitude of the FDI changes, and our purpose is to investigate the impacts of the FDI magnitude on the resilient configuration. In this regard, the magnitude of the FDI attack is changed from -0.03 p.u to 0.03 p.u and the results are presented in Table 2. The angle of the FDI attack is changed from -0.2° to 0.2° and the results are given in Table 3. It can be seen that changing the value of the FDI attack can alter the resilient configuration.

According to the TABEL I, the resilient configuration depends on the location of the FDI attack. In this regard, according to equation (30), our purpose is to find the resilient configuration which is

independent of the location of the FDI attack. So, the configuration which minimizes $F_{FDI,total}$ (equation 30) is presented in Table 4. In this table, it is assumed $\Delta V = +0.01 \prec -0.1^{\circ}$ p.u. According to this table, by opening s10, s14, s19, s26, and s31 switches the minimum of the $F_{FDI,total}$ will be achieved. Table 5 represents the impact of network reconfiguration on $F_{FDI,total}$ in IEEE 69-bus system.

In the next stage, our purpose is to compare the results of the initial configuration with the reconfigured system obtained in Table 4. It is assumed that the attacker can change the voltage of each bus by $\Delta V = -0.01 \prec -0.1^{\circ}$. Table 6 compares the changes of active and reactive measurements in the initial configuration and the reconfigured system if the attack happens in each bus. The results of this table show that the reconfigured system can reduce the impacts of the FDI attack on the power measurements.

To evaluate the performance of the proposed method and the resilience of systems, the energy not supplied (ENS) index is defined as follows:

$$U_i = \lambda_i . r_i \tag{31}$$

$$ENS = \sum_{i=1}^{N} P_i U_i \tag{32}$$

where, λ_i and r_i are the failure rate and repair rate of a component, respectively. In the final stage, the effect of network reconfiguration on *ENS* index is presented in Table 7. According to the results of Table 7, network reconfiguration has a significant impact on *ENS*.

Table 2 Different magnitude of the FDI

Bus number	ΔV (p.u)	Open switch	$\lvert\Delta P\rvert.10^{-3}$	$\lvert\Delta Q\rvert.10^{-3}$	$F.10^{-3}$
5	$-0.03 \prec -0.1^{\circ}$	s14, s20, s21, s32,s37	58	29	43
5	$-0.01 \prec -0.1^{\circ}$	s14, s20, s21, s32,s37	6.1	2.8	4.5
5	$+0.01 \prec -0.1^{\circ}$	s9, s12, s16, s19,s26	0.4	2.3	1.3
5	$+0.03 \prec -0.1^{\circ}$	S6, s13, s21, s26,s29	16	1.5	9.1
17	$-0.03 \prec -0.1^{\circ}$	s19, s21, s30, s34,s37	0.8	0.067	0.44
17	$-0.01 \prec -0.1^{\circ}$	s12, s19, s24, s32,s35	0.2	0.26	0.2
17	$+0.01 \prec -0.1^{\circ}$	s17, s19, s26, s34,s35	0.1	2	1
17	$+0.03 \prec -0.1^{\circ}$	s9, s12, s17, s19,s27	0.3	0.26	0.28

Table 3 Different angle of the FDI

Bus number	ΔV (p.u)	Open switch	$\lvert\Delta P\rvert.10^{-3}$	$\lvert\Delta Q\rvert.10^{-3}$	$F.10^{-3}$
5	$-0.01 \prec -0.2^{\circ}$	s14, s20, s21, s32,s37	8.8	7.3	8
5	$-0.01 \prec -0.1^{\circ}$	s14, s20, s21, s32,s37	6.1	2.8	4.5
5	$-0.01 \prec +0.1^{\circ}$	s14, s20, s21, s32, s37	0.77	6.1	3.4
5	$-0.01 \prec +0.2^{\circ}$	s14, s19, s21, s36, s37	1.6	11	6.2
17	$-0.01 \prec -0.2^{\circ}$	s12, s20, s24, s32,s35	1.6	1.3	1.4
17	$-0.01 \prec -0.1^{\circ}$	s12, s19, s24, s32,s35	0.15	0.26	0.2
17	$-0.01 \prec +0.1^{\circ}$	s17, s19, s24, s34,s35	0.02	0.14	0.079
17	$-0.01 \prec +0.2^{\circ}$	s14, s17, s20, s35,s37	0.078	0.14	0.11

Table 4 Network configuration for Ftot in IEEE 33 bus

	Open switch	$F_{FDI,total}.10^{-2}$
Initial configuration	s33, s34, s35, s36,s37	2.4
Reconfigured system	s10, s14, s19,s26,s31	1.8

Table 5 Network configuration for F_{tot} in IEEE 69 bus

	Open switch	$F_{FDI,total}.10^{-2}$
Initial configuration	s69, s70, s71, s72,s73	3.1
Reconfigured system	S17, s24, s40,s43,s49	2.6

Table 6 Impacts of the reconfigured system on the FDI attack

Bus number (under attack)	Initial configuration		Reconfigured System	
	$\lvert\Delta P\rvert.10^{-2}$	$\lvert\Delta Q\rvert.10^{-2}$	$\lvert\Delta P\rvert.10^{-2}$	$\lvert\Delta Q\rvert.10^{-2}$
2	16.1	3.5	13.6	8.3
3	6.1	1.1	5.4	3
4	4.8	0.7	4.3	2.2
5	3.2	0.7	2.8	1.6
6	6	2.3	4.9	3.9
7	1.4	1.1	1.2	1.6
8	1.3	0.1	1.6	0.8
9	1.4	0.5	1.5	1.1
10	5.3	0.3	1.5	1.1
11	7.1	0.1	2.5	0.8
12	2.9	0.2	3.1	1.4
13	1.3	0.8	1.2	1.3
14	2	1.1	1.2	1.3
15	2.1	0.8	1.1	0.8
16	1.3	0.6	1.1	1
17	1.3	0.6	1.1	1
18	1.3	0.6	1.8	1.6
19	4.7	2.1	2	1.7
20	1.9	1	1.1	1.3
21	2.2	1.3	1.8	2
22	2.2	1.3	0.8	0.9
23	2.6	0.8	2.3	1.6
24	1.7	0.6	1.8	1.3
25	1.7	0.6	2.1	1.7
26	7.3	1.1	1.7	1.5
27	3.7	0.7	0.6	0.5
28	1.5	0.6	1.3	1.1
29	2.5	0.6	3.3	2.4
30	2.3	0.6	2.2	1.9
31	2.3	1.4	2.2	1.3
32	2.9	2	1.1	1.4
33	2.9	2	0.8	1.3

Table 7 *ENS* index in IEEE 33-bus

	Open switches	*ENS*
GA [27]	7-9-30-34-37	53798.2
Proposed	7-14-19-30-37	53299.3

6 Conclusion

Due to the development of the application of communication technology in traditional power grids and microgrids, cyber threats are increasing. In this paper, FDI attacks have been studied as a type of cyber-attacks. SE has been discussed, and the basic principles of cyber-attack have been presented. Notably, the FDI attacks have been formulated and modeled in a balanced and symmetric distribution system. The (MSOE) algorithm has been used as a network reconfiguration strategy to decrease the FDI attacks against SE in distribution systems. In the most recent research on FDI attacks, the networks under study have been considered with a fixed topology. In this study, reconfiguration has been used to improve the resiliency of the network versus FDI attacks. The IEEE 33-bus and IEEE 69-bus have been used to demonstrate the effectiveness of network reconfiguration. Based on Table 4 and Table 5, it can be said that the network reconfiguration reduces the impact of the FDI attack on measurements in IEEE 33 bus and 69 bus test systems by 25% and 16%, respectively. Network reconfiguration can reduce the impacts of the FDI on power active and reactive measurements. Also, this paper illustrates the impacts of the magnitude of FDI attacks on the best configuration of the system. In our future works, other types of cyber-attacks and various power system performance indexes in the optimization model will be considered.

Intellectual Property

The authors confirm that they have given due consideration to the protection of intellectual

property associated with this work and that there are no impediments to publication, including the timing to publication, with respect to intellectual property.

Funding

No funding was received for this work.

CRediT Authorship Contribution Statement

R. Behnam: Methodology, Software, Validation, Formal analysis, Writing-Original Draft, Visualization**. G. B. Gharehpetian:** Conceptualization, Methodology, Formal analysis, Writing-Review & Editing, Visualization

Declaration of Competing Interest

The authors hereby confirm that the submitted manuscript is an original work and has not been published so far, is not under consideration for publication by any other journal and will not be submitted to any other journal until the decision will be made by this journal. All authors have approved the manuscript and agree with its submission to "Iranian Journal of Electrical and Electronic Engineering".

References

[1] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning," *Computers & Security*, vol. 97, p. 101994, 2020.

[2] T. Liu and T. Shu, "On the security of ANN-based AC state estimation in smart grid," *Computers & Security*, vol. 105, p. 102265, 2021.

[3] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 669-678, 2020.

[4] M. A. Rahman, A. Datta, and E. Al-Shaer, "Security design against stealthy attacks on power system state estimation: A formal approach," *Computers & security*, vol. 84, pp. 301-317, 2019.

[5] 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.

[6] Y. Isozaki *et al.*, "Detection of cyber attacks against voltage control in distribution power grids with PVs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824-1835, 2015.

[7] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*, 2010.

[8] N. Živković and A. T. Sarić, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, 2018.

[9] A. Anwar, A. N. Mahmood, and M. Ahmed, "False data injection attack targeting the LTC transformers to disrupt smart grid operation," in *International Conference on Security and Privacy in Communication Networks*, 2014, Springer, pp. 252-266.

[10] H. Margossian, M. A. Sayed, W. Fawaz, and Z. Nakad, "Partial grid false data injection attacks against state estimation," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 623-629, 2019.

[11] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, and D. Kundur, "False data injection attacks against synchronization systems in microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4471-4483, 2021.

[12] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612-621, 2014.

[13] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644-1652, 2014.

[14] H. Shi, L. Xie, and L. Peng, "Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method," *Computers & Electrical Engineering*, vol. 91, p. 107058, 2021.

[15] C. Liu, R. Deng, W. He, H. Liang, and W. Du, "Optimal coding schemes for detecting false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 738-749, 2021.

[16] H. Moayyed, M. Mohammadpourfard, C. Konstantinou, A. Moradzadeh, B. Mohammadi-Ivatloo, and A. P. Aguiar, "Image processing based approach for false data injection attacks detection in power systems," *IEEE Access*, vol. 10, pp. 12412-12420, 2021.

[17] E. Drayer and T. Routtenberg. Detection of false data injection attacks in power systems with graph fourier transform. *In 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 890-894, 2018.

[18] B. Mahdad, "Optimal reconfiguration and reactive power planning based fractal search algorithm: A case study of the Algerian

distribution electrical system," *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 78-101, 2019.

[19] A. Merlin and H. Back, "Search for minimum-loss operating spanning tree configuration in an urban power distribution system," *presented at the Proc. 5th Power System Computation Conference*, 1975, pp. 1-18, 1975.

[20] D. Anteneh, B. Khan, O. P. Mahela, H. H. Alhelou, and J. M. Guerrero, "Distribution network reliability enhancement and power loss reduction by optimal network reconfiguration," *Computers & Electrical Engineering*, vol. 96, p. 107518, 2021.

[21] M. E. Baran and A. W. Kelley, "State estimation for real-time monitoring of distribution systems," *IEEE Transactions on Power systems*, vol. 9, no. 3, pp. 1601-1609, 1994.

[22] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871-2881, 2018.

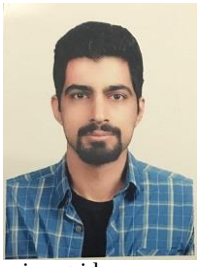
[23] K. Jasthi and D. Das, "Simultaneous distribution system reconfiguration and DG sizing algorithm without load flow solution," *IET Generation, Transmission & Distribution*, vol. 12, no. 6, pp. 1303-1313, 2018.

[24] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *2010 First IEEE International Conference on Smart Grid Communications*, IEEE, pp. 226-231, 2010.

[25] V. Vai, S. Suk, R. Lorm, C. Chhlonh, S. Eng, and L. Bun, "Optimal reconfiguration in distribution systems with distributed generations based on modified sequential switch opening and exchange," *Applied Sciences*, vol. 11, no. 5, p. 2146, 2021.

[26] Y.-K. Wu, C.-Y. Lee, L.-C. Liu, and S.-H. Tsai, "Study of reconfiguration for the distribution system with distributed generators," *IEEE transactions on Power Delivery*, vol. 25, no. 3, pp. 1678-1685, 2010.

[27] M. R. Narimani, A. Azizi Vahed, R. Azizipanah-Abarghooee, and M. Javidsharifi, "Enhanced gravitational search algorithm for multi-objective distribution feeder reconfiguration considering reliability, loss and operational cost," *IET Generation, Transmission & Distribution*, vol. 8, no. 1, pp. 55-69, 2014.



Reza Behnam received his B.Sc. and M.Sc. degrees in electrical engineering in 2017 and 2020 from Isfahan University of Technology, Isfahan, Iran, and Amirkabir University of Technology (AUT), Tehran, Iran, respectively. His research interests include smart grid issues, power management in microgrids, power system operation and planning, power system optimization, renewable energies, and energy storage systems.

Gevork B. Gharehpetian (M'00–SM'08) received his BS, MS and PhD degrees in electrical engineering in 1987, 1989 and 1996 from Tabriz University, Tabriz, Iran and Amirkabir University of Technology (AUT), Tehran, Iran and Tehran University, Tehran, Iran, respectively, graduating all with First Class Honors. As a PhD student, he has received scholarship from DAAD (German Academic Exchange Service) from 1993 to 1996 and he was with High Voltage Institute of RWTH Aachen, Aachen, Germany. He has been holding the Assistant Professor position at AUT from 1997 to 2003, the position of Associate Professor from 2004 to 2007 and has been Professor since 2007. He was selected by the MSRT (Ministry of Science Research and Technology) as the distinguished professor of Iran, by IAEEE (Iranian Association of Electrical and Electronics Engineers) as the distinguished researcher of Iran, by Iran Energy Association (IEA) as the best researcher of Iran in the field of energy, by the MSRT as the distinguished researcher of Iran, by the Academy of Science of the Islamic Republic of Iran as the distinguished professor of electrical engineering, by National Elites Foundation as the laureates of Alameh Tabatabaei Award and was awarded the National Prize in 2008, 2010, 2018, 2018, 2019 and 2019, respectively. Based on the Web of Science database (2005-2019), he is among world's top 1% elite scientists according to ESI (Essential Science Indicators) ranking system. Prof. Gharehpetian is distinguished, senior and distinguished member of CIGRE, IEEE and IAEEE, respectively. Since 2004, he has been the Editor-in-Chief of the Journal of IAEEE. He is the author of more than 1300 journal and conference papers. His teaching and research interests include Smart Grid, Microgrids, FACTS and HVDC Systems, Monitoring of Power Transformers and its Transients.