Journal of Engineering Science and Technology Review 14 (3) (2021) 124 - 139

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Probabilistic Defense and Impact of Generator Ramp Constraints Induced Load Redistribution Attacks in Power Systems

Kommoju C Sravanthi and Mercy Rosalina Kotapuri*

Department of Electrical and Electronics Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, Andhra Pradesh, India.

Received 7 December 2020; Accepted 2 April 2021

Abstract

Despite today's smart grid's deployment of more information and communication systems, it is more prone to data injection attacks. Researchers have developed several methodologies for successful intrusion into the system by means of False Data Injection Attacks (FDIAs) which result in system vulnerability. Practical FDIAs are called Load Redistribution Attacks (LRAs). LRAs target bus active power injections and line active power flows. The most damaging Load Redistribution Attack Vector (LRAV) of a classical LRA is found by solving a Bilevel Programming Problem (BPP) where attacker in the upper level develops most damaging LRAV and operator in the lower level performs basic static Security Constrained Optimal Power Flow (SCOPF) along with false measurements. But in dynamic operations, generator ramp rates play a crucial role. So, in this article, generator ramp rate constraints are included in SCOPF to show the impact of Generator Ramp Rate Constraints induced LRA (GRC-LRA) in means of Economic Loss, $/MWh, without attacking any generator. GRC-LRA vector is solved by using Karush-Kuhn-Tucker (KKT) based single level Mixed Integer Linear Programming Problem (MILPP) and Benders Decomposition methods. An optimal attack-defense strategy is also found by playing static zero-sum game, a method of probabilistic defense. Attack and defense mechanisms for GRC-LRA are tested on modified IEEE-14 bus test system and validated at fixed and variable ramp rates in low load varying and high load varying conditions.

Keywords: Load Redistribution Attack (LRA); Generator Ramp Constraints induced Load Redistribution Attack (GRC-LRA); Bilevel Programming Problem (BPP); KKT based single level MILPP Method; Benders Decomposition Method; Probabilistic defense; Static Zero-Sum Game;

1. Introduction

Modern power systems is a fundamental asset in the development of every nation's economy, reliability and security. Smart grid advancements in power grid have made the power system not only physical but also cyber. Cyber-Physical Power System (CPPS) is complex as the cyber layer covers every part of the physical layer by sensing, communicating and processing to operate Supervisory Control and Data Acquisition (SCADA) system in a better way [1]. Even though CPSS has many advancements, it is vulnerable to cyber threats/attacks due to its wide usage of information and communication systems [2]. It is a real experience to Ukrainian power system, by coming across such cyber attacking through a pre-installed malware by opening breakers autonomously [3]. So it is a fact to get aware of the effect of cyber-threats on the power systems.

Various researchers have developed many proposals and more literature to develop, analyze and defend cyber-attacks [4]. CPSS' components can be hacked or their keys can be cracked to disrupt the grid, furthermore smart measuring units can be compromised, to create man-in-middle attacks [5], to build Denial-of-Service (DoS) attacks [6] by injecting false/bad data into smart units. To detect false/bad data injected into the system, classical bad data detection methods (χ^2 −distribution hypothesis testing) were been used by the operator at control center. But Liu et al. have proposed that there is a chance to bypass those classical detection methods and intrude into the system by injecting undetectable false data into the system and named that attack called False Data Injection Attack (FDIA) and that specific attack vector is False Data Injection Attack Vector (FDIAV) [7]. FDIAs divert the operator to make erroneous decisions due to incorrect state estimates caused by FDIAVs.

FDIA that especially targets bus active power injection measurement values and line active power flow measurement values is popular as Load Redistribution Attack (LRA) and that injected vector is Load Redistribution Attack Vector (LRAV). These practical FDIAs (LRAs) were proposed by Yuan et al. to deteriorate the system economics and reliability [8]. Generally, basic detection methods are based on residual analysis, i.e., if the residue of actual and estimated measurements is within tolerance, then as per χ^2 - hypothesis testing, the measurement doesn't have bad data. If tolerance value is low, then the capability of detecting bad data can be high. So, if an attack vector is within tolerance then perhaps the attacking values cannot be detected. It should be also noted that an attack vector can be undetectable, if mean of change in errors is zero. Hence a successful LRAV can be developed such that the sum of load changes must be equal to zero. In other means, actual load should be redistributed among the loads. Hence, this attack is named as LRA. LRAVs were developed based on Kirchoff's laws [8]. LRAs severely cause load shedding, economic loss and line outages too. LRAVs are of two types one is Immediate LRA [8] and other is Delayed LRA [9]. LRAs are generally solved by framing Bilevel Programming Problem (BPP) solved by Karush-

*E-mail address: kmr_eee@vignan.ac.in
ISSN: 1791-2377
doi:10.25103/jestr.143.15

Kuhn-Tucker (KKT) conditions based single level MILPP [10] or by Benders decomposition [9]. Liu et al. have approximated the load shedding and economic loss on solving two levels individually within less time [11]. Choeum and Choi have proposed a new type LRA in three-phase distribution system in which BPP is solved by KKT based single-level MILPP and results are validated on IEEE-13 node distribution feeder [12]. Kaviani and Hedman have developed a new structure of LRA problem, mentioned that attackers view can be trivial and used physical laws on transmission line flows (by making the sum of change in line flows equals to zero) to build a successful LRAV [13].

More research is done on various types of attacks like local LRAs [14, 15], cyber-physical coordinated LRAs [16-18], cascading failures coordinated with LRAs [19] and also the reliability analysis after a successful LRA [20, 21]. Shayan and Amraee developed LRAs in conjunction with Security Constrained Unit Commitment (SCUC) problem (with ramp constraints, minimum up and down times). To lessen LRAV's loss, Cyber Secured Unit Commitment (CSUC) problem has also been developed [22]. Dae-Hyun Choi and Le Xie have proposed a special type ramp induced data attacks that target the real-time market by using look-a-head SCOPF dispatch model. Initial generation dispatches are disrupted by attacker. Obviously ramp rate constraints (dependent on initial dispatches) can get deviated from actuals which result in financial arbitrage in the market. In this type of attack, attacker needs to compromise the generator's measuring unit [23]. Che et al. have developed a special type of attack called "Ramp Induced Data Attacks" which create power imbalance (either surplus/deficient power generation) by attacking a generator but not loads [24]. From literature, it should be noted that generator ramp rates can provide assistance for an attacker to maximize his/her objectives and it is needed to concentrate on ramp constraints integrated attacks. Xiang and Wang proposed that an optimal attack-defense strategy can be found by probabilistic based game theory, where critical measuring units are selected based on critical operating points in the system [26] or entropic degree [27]. This method of selecting may not be applicable all time if any load changes occur.

In this article, the impact of ramp rates of a generator is shown in means of economic loss without attacking a generator but attacking loads/lines using LRA. This is achieved by inducing ramp rate constraints along with LRA on basic SCOPF problem, proposed as Generator Ramp Constraints induced Load Redistribution Attack (GRC-LRA). It should be noted that in the proposed GRC-LRA, no generator is attacked. In the upper-level of GRC-LRA's BPP, an LRAV is developed for given load/line attacking resources and in the lower level of dynamic SCOPF (basic SCOPF and generator ramp rates) contributes to deviated uneconomic generation dispatches.

Major Contributions of this research article are as follows:

1. Framing the overall BPP of GRC-LRA to find the most damaging GRC-LRAV and solving it by KKT conditions based single-level MILLPP and Benders decomposition methods.
2. Finding the critical measuring units and obtaining the probabilities of an optimal attack-defense strategy of GRC-LRAV using static zero-sum game theory.
3. Exhibiting a numerical analysis to show the impact of GRC-LRAV on a modified IEEE-14 bus test system with low load changing and high load changing at fixed, variable ramp rates and protection against GRC-LRA.

This research article is organized in a way that section 2 deals with literature of FDIAs, LRAs and modelling of ramp constraints in SCED/SCOPF whereas section 3 presents a BPP to find most damaging GRC-LRAV, two methods to solve that BPP by using KKT based single-level MILPP and Benders decomposition methods and probabilistic defense static zero-sum game theory. Section 4 depicts a numerical analysis of LRAV versus GRC-LRAV applied on modified IEEE-14 bus test system in two load varying conditions at fixed and variable ramp rates. Moreover, Section 4 also represents probabilities of optimal attack-defense strategies and finally conclusions are described in section 5.

2. Background

2.1 False Data Injection Attacks (FDIAs) and Load Redistribution Attack (LRA)

Power system online monitoring system is more prone to undetectable false data that can be injected into the network measurement devices like Phasor Measurement Units (PMUs)/Remote Terminal Units (RTUs) which are used for measuring, controlling and observing the system time-to-time [25]. Generally, sensed real-time active and reactive power injections and line flows are sent to the control center by means of communication and security equipment like Intelligent Electronic Devices (IEDs), firewalls and WANs. At the control center various analysis like DC state estimation, SCOPF/SCED, load forecasting, contingency analysis and Energy Marketing System (EMS) marketing will be undergone. Undetectable FDIAs, developed by Liu et al. in 2011 makes system vulnerable. If $\boldsymbol{z}$, $\boldsymbol{a}$ and $\boldsymbol{z_a}$ are the actual, attack and damaged/attacked measurement vectors respectively. Let $\widehat{\boldsymbol{x}}$ be the actual state estimate of $\boldsymbol{z}$, $\widehat{\boldsymbol{x}}_{\boldsymbol{f}}$ be the false state estimate of $\boldsymbol{z_a} = \boldsymbol{z} + \boldsymbol{a}$, c be the reflected erroneous estimate of $\boldsymbol{z_a}$ and $\boldsymbol{H}$ be the Jacobian matrix, then the L_2 norm of the residual with damaged measurements is $||\boldsymbol{z_a} - \boldsymbol{H} * \widehat{\boldsymbol{x}}_{\boldsymbol{f}}||$ is simplified as shown in Eq.1.

But $\widehat{\boldsymbol{x}}_{\boldsymbol{f}} = \widehat{\boldsymbol{x}} + \boldsymbol{c}$,

then $||\boldsymbol{z_a} - \boldsymbol{H} * \widehat{\boldsymbol{x}}_{\boldsymbol{f}}|| = ||\boldsymbol{z_a} - \boldsymbol{H} * (\widehat{\boldsymbol{x}} + \boldsymbol{c})||$

$$\Rightarrow ||\boldsymbol{z_a} - \boldsymbol{H} * \widehat{\boldsymbol{x}}_{\boldsymbol{f}}|| = ||\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}\widehat{\boldsymbol{x}} - \boldsymbol{Hc})||$$

$$\Rightarrow ||\boldsymbol{z_a} - \boldsymbol{H} * \widehat{\boldsymbol{x}}_{\boldsymbol{f}}|| = ||(\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}) + (\boldsymbol{a} - \boldsymbol{Hc})|| \quad (1)$$

If $\boldsymbol{a} = \boldsymbol{Hc}$, L_2-norm of attacked measurement residual becomes L_2-norm of non-attacked measurement residual [7]. Hence, it can be clear that L_2-norm of damaged measurement residual is also within the threshold and it is obvious that $\boldsymbol{z_a}$ can bypass classical detection method and disrupt the system. The attack vector $\boldsymbol{z_a}$ is called FDIAV.

A practical example of FDIA is LRA. In LRA the attacker targets are bus active power injections' and line active power flows' measurements. Load Redistribution Attack Vector (LRAV), the name itself defines that load must be redistributed among loads and that vector can be undetectable if the sum of redistributed load is zero (as per Gaussian distribution mean of errors is zero). Redistribution among loads should be done within a tolerance $\pm\tau$, so that LRAV can be undetectable by control center [8].

Attacker always seeks to maximize the operating cost with minimum number of resources and tries to develop a most damaging undetectable LRAV within the available resources abided to his/her constraints at one-time step. In the next time step the operator tries to minimize operating cost subjected to basic SCOPF constraints like supply-load

balance, power flow constraints, and generator, line and load curtailment bounds. This problem can be framed as a BPP where in the upper level attacker maximizes and in the lower level operator minimizes the operating cost. The bilevel representation to obtain a most damaging undetectable LRAV is given in Fig. 1 [8].

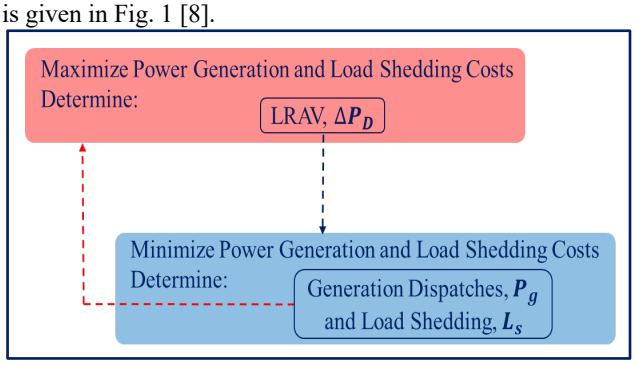

Fig. 1. Bilevel Representation of LRA

The mathematical representation of a most damaging LRAV's BPP is given by Eq.2-Eq.14, where upper level replicates attacker and lower level denotes operator. Objective functions of upper level, Eq.2 and lower level, Eq.9 are maximization and minimization of generational operational and load shedding costs respectively. Eq.3 and Eq.4 show that sum of load redistributed must be zero and load change at particular node must be within tolerance $\pm\tau$, Eq.5 gives the changes in line flows due to LRAV, however Eq.6 and Eq.7 deal with attacker compromising the measurements and Eq.8 shows the number of attackable resources. Furthermore, Eq.10-Eq.14 are the basic SCOPF constraints and their bounds.

$$\underset{\Delta \boldsymbol{P_D}}{\text{Max}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^* + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^* \tag{2}$$

$$s.t. \sum_{k=1}^{N_d} \Delta P_{D_k} = 0 \tag{3}$$

$$-\tau P_{D_k} \le \Delta P_{D_k} \le \tau P_{D_k} \tag{4}$$

$$\boldsymbol{\Delta P_L = -SF.KD.\Delta P_D} \tag{5}$$

$$\Delta P_{D_k} = 0 \Leftrightarrow \theta_{D_k} = 0 \Longrightarrow \begin{cases} \Delta P_{D_k} + \tau P_{D_k}\theta_{D_k} \ge 0 \\ \Delta P_{D_k} - \tau P_{D_k}\theta_{D_k} \le 0 \\ \theta_{D+_k} + \theta_{D-_k} - 2\theta_{D_k} \le 0 \\ \Delta P_{D_k} + (-\tau P_{D_k} - \varepsilon)\theta_{D+_k} \ge -\tau P_{D_k} \\ \Delta P_{D_k} + (\tau P_{D_k} + \varepsilon)\theta_{D-_k} \le \tau P_{D_k} \\ \theta_{D+_k} + \theta_{D-_k} + \theta_{D_k} \le 2 \\ \theta_{D+_k} + \theta_{D-_k} - \theta_{D_k} \ge 0 \\ \theta_{D+_k}, \theta_{D-_k}, \theta_{D_k} \in \{0,1\} \end{cases} \tag{6}$$

$$\Delta P_{L_l} = 0 \Leftrightarrow \theta_{L_l} = 0 \Longrightarrow \begin{cases} \Delta P_{L_l} + M\theta_{L_l} \ge 0 \\ \Delta P_{L_l} - M\theta_{L_l} \le 0 \\ \theta_{L+_l} + \theta_{L-_l} - 2\theta_{L_l} \le 0 \\ \Delta P_{L_l} + (-M - \varepsilon)\theta_{L+_l} \ge -M \\ \Delta P_{L_l} + (M + \varepsilon)\theta_{L-_l} \le M \\ \theta_{L+_l} + \theta_{L-_l} + \theta_{L_l} \le 2 \\ \theta_{L+_l} + \theta_{L-_l} - \theta_{L_l} \ge 0 \\ \theta_{L+_l}, \theta_{L-_l}, \theta_{L_l} \in \{0,1\} \end{cases} \tag{7}$$

$$\sum_{k=1}^{N_d} \theta_{D_k} + 2\sum_{l=1}^{N_l} \theta_{L_l} \le R_t \tag{8}$$

$$\{\boldsymbol{P_g}^*, \boldsymbol{L_s}^*\} = \underset{\boldsymbol{P_g}, \boldsymbol{L_s}}{\text{Min}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^* + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^* \tag{9}$$

$$\sum_{i=1}^{N_g} P_{g_i} = \sum_{k=1}^{N_d} (P_{D_k} - L_{s_k}) \tag{10}$$

$$\boldsymbol{P_L = SF.KP.P_g - SF.KD.(P_D + \Delta P_D - L_s)} \tag{11}$$

$$-P_{L_l}^{max} \le P_{L_l} \le P_{L_l}^{max} \tag{12}$$

$$P_{g_i}^{min} \le P_{g_i} \le P_{g_i}^{max} \tag{13}$$

$$0 \le L_{s_k} \le P_{D_k} + \Delta P_{D_k} \tag{14}$$

2.2 Ramp Constraints in SCOPF/SCED

Practically, generators may take time to reach a new level from the operating point especially in case of steam and hydrothermal generating units (due to their inner dynamics) which is called ramping. Generally, ramping in generators is of three types: startup, shutdown and operating ramp constraints. Startup and shutdown ramping constraints exist when a decommitted generator is committed and a committed generator is decommitted correspondingly. When a unit is committed from off position, the generator reaches its minimum operating capacity by increasing gradually within some time periods is startup ramping. If a generator is to be decommitted to off position, the generator reaches it minimum operating capacity by decreasing gradually within some time periods is shutdown ramping. These two ramping constraints come into existence in unit commitment problem. But in economic dispatch operating ramp constraints are considered which are neither startup ramping nor shutdown ramping constraints. Operating ramping deals with the generation dispatches of two successive time periods subjected to generator bounds. Let $P_{g_i}(t)$ and $P_{g_i}(t-1)$ be the dispatches of i^{th} generator at time steps of t and $t-1$. Let $R\_u_{g_i}$ and $R\_d_{g_i}$ be the ramp rates for up and down ramping of i^{th} generator and $\Delta t = (t) - (t-1)$ be time step size then ramp up (Eq.15) and ramp down (Eq.16) constraints, as functions of generation power dispatches are as follows:

$$P_{g_i}(t) - P_{g_i}(t-1) \le R\_u_{g_i} + P_{g_i}^{min} \tag{15}$$

$$P_{g_i}(t-1) - P_{g_i}(t) \leq R\_d_{g_i} + P_{g_i}^{min} \quad (16)$$

$\forall\, i\epsilon\, 1,2,\dots,N_g$ and $\forall\, t\epsilon\, 1,2,\dots,T$.

Eq.15 and Eq.16 approximate that i^{th} generator may be able to step up or down from the operating point within the ramp up and down limits respectively, but not beyond.

3. Generator Ramp Constraints Induced LRA (GRC-LRA)

The main aim of this research is to show the impact of ramp constraints on the system when an attacker is intruded into the system and able to develop a successful LRAV. As in practice, for high rating generating units, ramp constraints are mandate and hence ramp constraints need to be included while analyzing LRAs. So to find most damaging Generator Ramp Constraints Induced Load Redistribution Attack Vector (GRC-LRAV), the incorporation of ramp constraints at upper or lower level of BPP must be known. It is an assumption in LRAs that generators cannot be attacked [8] and in this article no generator is attacked. So, inclusion of ramp constraints in the upper level is not possible however it is needed to include ramp up and ramp down constraints in the lower level of BPP i.e., in SCED/SCOPF. Hence the overall problem of most damaging GRC-LRAV is as follows, given by Eq.17-Eq.20:

$$\underset{\Delta P_D}{\text{Max}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^* + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^* \quad (17)$$

$$s.t.\,(3)-(8) \quad (18)$$

$$\{P_g^*, L_s^*\} = \underset{P_g, L_s}{\text{Min}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^* + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^* \quad (19)$$

$$s.t.\,(10)-(14),(15),(16) \quad (20)$$

The BPP to find most damaging LRAV with induced generator ramp constraints (i.e., GRC-LRAV) can be solved by various methods. Basic method is like converting the BPP into single level MILPP using KKT conditions or dual conditions and thereafter solving single level MILPP by using MILPP solvers [8-10]. Other method is solving BPP directly by one of the decomposition methods like Benders decomposition [9]. In this article, most damaging GRC-LRAV is obtained by solving using KKT conditions based single-level MILPP and Benders decomposition methods.

3.1 Most Damaging GRC-LRAV by KKT Conditions based MILPP

The most damaging GRC-LRAV is obtained by converting upper and lower levels of GRC-LRA's BPP into single level MILPP using KKT conditions are given below. The overall objective function is maximization of operational cost subjected to upper level constraints Eq.3-Eq.8, lower level constraints Eq.10-Eq.14 and Eq.9 is replaced by new equations with new variables Eq.21-Eq.30.

$$\underset{\Delta P_D}{\text{Max}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^* + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^*$$

$$s.t.\,(18),(20)$$

$$-\vartheta_l - \underline{\mathrm{A}}_l + \overline{\mathrm{A}}_l = 0 \quad (21)$$

$$c_i - \lambda + (SF.KP_i)^T.\vartheta - \underline{B}_i + \overline{\mathrm{B}}_i + ru_i^t - ru_i^{(t+1)} + rd_i^t + rd_i^{(t+1)} = 0\ ;\ \forall\, t\epsilon\, 1,2,\dots,T-1 \quad (22)$$

$$c_i - \lambda + (SF.KP_i)^T.\vartheta - \underline{B}_i + \overline{B}_i + ru_i^t - rd_i^t = 0\ ;\ \forall\, t = T \quad (23)$$

$$cs_k - \lambda + (SF.KD_k)^T.\vartheta - \underline{\Gamma}_k + \overline{\Gamma}_k = 0 \quad (24)$$

$$\underline{\mathrm{A}}_l, \overline{\mathrm{A}}_l, \underline{\mathrm{B}}_i, \overline{\mathrm{B}}_i, \underline{\Gamma}_k, \overline{\Gamma}_k \geq 0 \quad (25)$$

$$\begin{cases} \underline{\mathrm{A}}_l \leq M\omega_{\underline{\mathrm{A}},l} \\ P_{L_l} + P_{L_l}^{max} \leq M(1-\omega_{\underline{\mathrm{A}},l}) \\ \overline{\mathrm{A}}_l \leq M\omega_{\overline{\mathrm{A}},l} \\ P_{L_l}^{max} - P_{L_l} \leq M(1-\omega_{\overline{\mathrm{A}},l}) \\ \omega_{\underline{\mathrm{A}},l} + \omega_{\overline{\mathrm{A}},l} \leq 1 \end{cases} \quad (26)$$

$$\begin{cases} \underline{\mathrm{B}}_i \leq M\omega_{\underline{\mathrm{B}},i} \\ P_{g_i} - P_{g_i}^{min} \leq M(1-\omega_{\underline{\mathrm{B}},i}) \\ \overline{\mathrm{B}}_i \leq M\omega_{\overline{\mathrm{B}},i} \\ P_{g_i}^{max} - P_{g_i} \leq M(1-\omega_{\overline{\mathrm{B}},i}) \\ \omega_{\underline{\mathrm{B}},i} + \omega_{\overline{\mathrm{B}},i} \leq 1 \end{cases} \quad (27)$$

$$\begin{cases} \underline{\Gamma}_k \leq M\omega_{\underline{\Gamma},k} \\ L_{s_k} \leq M(1-\omega_{\underline{\Gamma},k}) \\ \overline{\Gamma}_k \leq M\omega_{\overline{\Gamma},k} \\ P_{D_k} + \Delta P_{D_k} - L_{s_k} \leq M(1-\omega_{\overline{\Gamma},k}) \\ \omega_{\underline{\Gamma},k} + \omega_{\overline{\Gamma},k} \leq 1 \end{cases} \quad (28)$$

$$\begin{cases} ru_i^t \leq M\omega_{ru_i^t} \\ P_{g_i}(t-1) - P_{g_i}(t) + R\_u_i + P_{g_i}^{min} \leq M(1-\omega_{ru_i^t}) \\ rd_i^t \leq M\omega_{rd_i^t} \\ P_{g_i}(t) - P_{g_i}(t-1) + R\_d_i + P_{g_i}^{min} \leq M(1-\omega_{rd_i^t}) \\ \omega_{ru_i^t} + \omega_{rd_i^t} \leq 1 \end{cases}$$

$$\forall\, t\epsilon\, 1,2,\dots,T \quad (29)$$

$$\omega_{\underline{\mathrm{A}},l}, \omega_{\overline{\mathrm{A}},l}, \omega_{\underline{\mathrm{B}},i}, \omega_{\overline{\mathrm{B}},i}, \omega_{\underline{\Gamma},k}, \omega_{\overline{\Gamma},k}, \omega_{ru_i^t}, \omega_{rd_i^t} \epsilon \{0,1\} \quad (30)$$

$\forall\, l\epsilon\, 1,2,\dots,N_l, \forall\, i\epsilon\, 1,2,\dots,N_g, \forall\, k\epsilon\, 1,2,\dots,N_d,$

Eq.21-Eq.30 are KKT based necessary feasibility constraints and Eq.26-Eq.29 are obtained by complementary slackness conditions.

3.2. Most Damaging GRC-LRAV by Benders Decomposition.

Benders decomposition algorithm has the capability to decompose an integer programming or MILPP into master problem and sub problem(s) which can be solved separately by iterative process. General Benders decomposition method when used to find worst GRC-LRAV may result in local optima. So, it is better to use multi-start Benders decomposition algorithm to obtain global optima of most damaging GRC-LRAV [9].

The Master Problem (MP) of GRC-LRA's BPP is given by equation Eq.31:

$$\underset{\Delta P_D}{\text{Min}} -\alpha$$

$$s.t. (18)$$

$$-C_{g_i}P_{g_i}^{*} - cs_k L_{s_k}^{*} - \boldsymbol{\mu}^{(m-1,n-1)*}$$

$$(\Delta \boldsymbol{P_D} - \left(\Delta \boldsymbol{P_D}^{(m-1,n-1)}\right) \leq \alpha \; if \; m > 1$$

$$-C_{g_i}P_{g_i} - cs_k L_{s_k}^{*} - \boldsymbol{\mu}^{(last\ m\ at\ n-1,n-1)*}$$

$$\left(\Delta \boldsymbol{P_D} - \Delta \boldsymbol{P_D}^{(last\ m\ at\ n-1,n-1)}\right) \leq \alpha \; if \; n > 1 \qquad (31)$$

And the Sub Problem (SP) of GRC-LRA's BPP is given by Eq.32

$$\underset{P_g,L_s}{\text{Min}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i}^{*} + \sum_{k=1}^{N_d} C_{s_k} * L_{s_k}^{*}$$

$$s.t. (20)$$

$$\Delta P_{D_k} - \Delta P_{D_k}^{(m,n)} = 0 \qquad (32)$$

Let the global optima of BPP be z_{opt}, Benders loops iteration counter be m and the Benders restarting counter be n. The procedure to solve GRC-LRA's BPP by multi start Benders decomposition is given as follows:

1. Initialize n=1, m=1 and $z_{opt} = \infty$.

2. Solve MP and update $\Delta P_{D_k} = \Delta P_{D_k}^{(m,n)}$ and $z_{lo}^{(m,n)} = \alpha^{(m,n)}$.

3. Solve SP and update $P_g^{(m,n)}$, $L_s^{(m,n)}$ and $Z_{up}^{(m,n)}$

$$= \begin{cases} min\left\{\sum_{i=1}^{N_g} C_{g_i}P_{g_i}^{(m,n)} + \sum_{k=1}^{N_d} C_{s_k}L_{s_k}^{(m,n)}, \infty\right\} & if\ m = 1 \ \&\ n = 1 \\ min\left\{\sum_{i=1}^{N_g} C_{g_i}P_{g_i}^{(m,n)} + \sum_{k=1}^{N_d} C_{s_k}L_{s_k}^{(m,n)}, Z_{up}^{(m-1,n)}\right\} & if\ m > 1 \\ min\left\{\sum_{i=1}^{N_g} C_{g_i}P_{g_i}^{(m,n)} + \sum_{k=1}^{N_d} C_{s_k}L_{s_k}^{(m,n)}, Z_{up}^{(last\ m\ at\ n-1,n-1)}\right\} & if\ m = 1 \ \&\ n \neq 1 \end{cases}$$

4. To avoid the global optima not to stuck at local optimal ΔP_{D_k} need to be updated as:

$$\begin{cases} if\ \Delta P_{D_k}^{(m,n)} = \tau P_{D_k}^{(m,n)},\ and\ \mu_k^{(m,n)} > 0, then\ set\ \mu_k^{(m,n)} = 0 \\ if\ \Delta P_{D_k}^{(m,n)} = -\tau P_{D_k}^{(m,n)},\ and\ \mu_k^{(m,n)} < 0, then\ set\ \mu_k^{(m,n)} = 0 \end{cases}$$

5. Update global optima as $z_{opt} = z_{up}^{(m,n)}$ if $z_{up}^{(m,n)} < z_{opt}$.

6. Check the convergence criteria $|z_{up}^{(m,n)} - z_{lo}^{(m,n)}| < \varepsilon$. If "Yes" then go to step-10, else go to step-7.

7. If $z_{up}^{(m,n)} - z_{lo}^{(m,n)} > 0$, update $m = m + 1$ and go to step-2.

8. If $z_{up}^{(m,n)} - z_{lo}^{(m,n)} < 0$, go to step-9.

9. Update $n = n + 1$, go to step-2 (neglect $\mu^{(m,n)}$ of all previous iterations except the last iteration $\mu^{(m,n-1)}$).

10. Stop.

The flowchart of solving GRC-LRAV by Benders decomposition method is shown in Fig. 2.

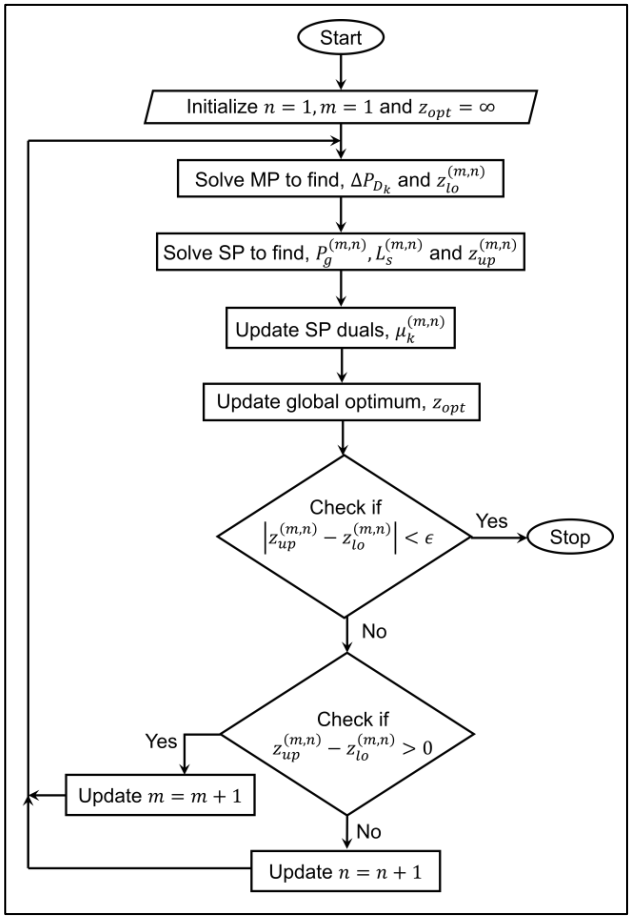

Fig. 2. Flowchart to obtain most damaging GRC-LRAV by Benders decomposition

3.3. Probabilistic Defense Against GRC-LRAV:

Various analysis regarding LRAs or GRC-LRAs is carried out to find an optimal defense mechanism against attacks as attacker tries to maximize the economic loss and defender targets to minimize it [26, 27]. So certain optimal cyber-defense must be provided such that attacker cannot inject a

successful LRAV into the system even if he/she intrudes. An LRAV can become unsuccessful/detectable, if $\sum_{m=1}^{k} \Delta P_{D_m} \neq 0$. If any of the critical measuring units is not attackable (means defended), then that unit won't help the attacker to develop a successful LRAV. Attacker may not have access to all measuring units and defender also can't defend all units (may be due to budget issues). So, certain critical measuring units must be considered which have high rank in attacking. If any unit has high rank of attacking, then that unit is highly probable for defending. That unit can be called as a critical measuring unit. It is also not an optimal strategy to protect only one unit all time. To obtain optimal defense, attack or defense strategies should be changing. Hence it can be derived that the units must have some probability for attacking or defending. In the literature, critical measuring units are selected based on entropic degree [27] and units operating at critical points [26]. These methods are deficient if the load changes.

To select an optimal number of critical measurements for prior known load and given attack resources, a method can be followed as follows:

Step-1: Apply defense to the measuring unit of k^{th} load or l^{th} line i.e., $\theta_{D_k} = \{\}$ or $\theta_{L_l} = \{\}$ and find economic loss where $\{\}$ represents null set.

Step-2: Find economic loss to all units where one unit is defended each time.

Step-3: Select the units which give minimum economic loss $\cong 0$ and treat them as critical units.

It is to be noticed that this method is applicable if the approximate load demand is known prior to both attacker and defender and the maximum approximate number of attacker resources should also be known.

Hence to find an optimal attack-strategy, probabilistic based game theory framework can be used. This game has two players, attacker and defender. Attacker tries to maximize his/her utility and defender minimize his/her utility. The utility function in this game is economic loss. Attacker and defender have their own strategies (actions) and are independent. Hence this game is a static game. It is considered that attacker and defender spends unit cost for attacking or defending [26]. Perhaps, an optimal attack-defense strategy can be obtained from a Nash equilibrium point by playing a static zero-sum game. Nash equilibrium is an equilibrium point for both players which says that any player moving from this point may not get extra incentives. In this problem, Nash equilibrium (optimal attack-defense strategy) results in pure probability of one attack-one defense strategy or mixed probabilities of possible attack or defense strategies [26]. Based on the Nash equilibrium, it is found that which attack strategy is highly probable and based on that defense can be provided by the operator.

4. Numerical Example

The main aim of the article is to show the impact of generator ramp constraints induced into LRA's BPP model i.e., to show the economic loss created by most damaging GRC-LRAV and also to obtain optimal attack-defense strategy considering economic loss as utility. Sections 4.1. and 4.2. show the analysis in two scenarios namely fixed ramp rates and variable ramp rates. In each scenario (in each section of 4.1. and 4.2.), it is again considered that the load variations are low and high. Low load variations are given in sub-sections-4.1.1. and 4.2.1. and high load variations are given in 4.1.2. and 4.2.2. Moreover, it is also analyzed in a way that if fixed ramp rates are slack (not-tight) or tight, are demonstrated in subsections 4.1.1. and 4.1.2. whereas, variable ramp rates as slack and tight in low load and high load changes are analyzed in subsections 4.2.1.1., 4.2.1.2., 4.2.2.1. and 4.2.2.2 respectively. Section 4.3. shows the selection of critical measuring units and probabilities of optimal attack-defense strategies.

In this research article, the test case considered is modified IEEE-14 bus system where data is obtained from MATPOWER [28]. Modified IEEE-14 bus system has five generators, one zero injection bus, eleven load buses and twenty transmission lines. As per the assumptions in LRA, it is clear that generators and zero injection buses can't be attacked. However, the attackable measuring units are one measuring unit at each load bus and two measuring units for each line. Hence the maximum number of attackable resources be 11+2*20=51 for a modified IEEE-14 bus system. For analysis, it is considered that the maximum power transfer capabilities of the first, second and remaining lines are 160MW, 70MW and 60MW respectively. It is also considered that the attacker may be capable to attack 20 measuring units. CPLEX solvers are used to solve the MILPPs and LPPs in this work [29].

Basically in look-a-head market, generation dispatches are calculated for all hours of next day whereas in real-time market, generator dispatches are calculated for every 10-15 minutes. So the step size in look-a-head market is high and which means that the load change can be large and similarly in real-time market step size is comparatively low where load change is also low. At the two loading conditions the load changes from $t-1$ to t is low and the other is the load change from $t-1$ to t is high. It is considered that for analysis in high load variations, the number of time instances be 24 and in low load variations the number is 6. In this research, the ramp rates, $R\_u_{g_i}$ and $R\_d_{g_i}$ are considered as fixed and variable in all time instances. It is also assumed that the attacker might not attack all time during all instances. He/she also tries to induce the LRAV at the instant when the load is high or the load change is high, so that the attacker can maximize his/her profit.

Most damaging GRC-LRAV of the test system in low load and high load variations' scenarios at fixed/variable ramp rates is found by using two methods explicitly KKT conditions based single level MILPP and Benders decomposition methods. The number of variables used to solve Eq.18, Eq.20, Eq.21-Eq.30 by KKT conditions based single level MILPP and to solve MP (Eq.31) and SP (Eq.32) by Benders decomposition respectively, are given in Tab.1.

4.1 Economic Loss due to Most Damaging GRC-LRAV at Fixed Ramp Rates

4.1.1 Scenario-1: Low Load Variation with *T*=6 at Slack and Tight Fixed Ramp Rates

Let the load variations within six time instances and the attack triggering are as given in Tab.2. For better analysis of GRC-LRAV, it is considered that the ramp rates are slack (not-tight) and tight which are given by R_u_g=R_d_g= [150 25 15 25 10] and R_u_g=R_d_g= [30 5 3 5 2] respectively. It is also assumed that generator dispatches at 0^{th} instant are $P_g^{(0)}$= [230 5.41 14.33 0 8.27] where the considered initial load demand is 258MW.

Table 1. Parameters to obtain most damaging GRC-LRAV of a modified IEEE-14 bus test system

Parameter	KKT Conditions based single level MILPP		Benders Decomposition	
	Low Load Change	High Load Change	Low Load Change	High Load Change
Variables Number	2070	8280	961	3841
Equalities' Number	468	1872	318	1272
Inequalities' Number	3162	12648	1933	7729
Integer Constrained Variables	1050	4200	558	2232

Table 2. Low load variation and attack triggers with $T = 6$

Time Instances	1	2	3	4	5	6
Load	259	254	260	260	253	259
$\boldsymbol{R}$	0	0	20	0	0	20

Most damaging GRC-LRAV, at low load varying conditions i.e., analogous to real-time market operations, applied on test system is obtained by solving KKT conditions based single level MILPP and Benders decomposition method. As the variable size is high (as shown in Tab.1), it is not possible to represent all solved variables. So, generation dispatches (P_g), load shedding (L_s), attack vector (ΔP_D) and operational cost are represented in Tab.3 and Tab.4.

P_g, L_s and ΔP_D satisfying all constraints of GRC-LRAV at low load variation within 6 time instances with tight ramp rates are shown in Tab.3. If attack is not triggered, irrespective of ramp rates, load shedding is zero. At 3rd and 6th instances attack is triggered. Hence, in case of LRA, total load shedding is 26.3421MW whereas in case of GRC-LRA, total load shedding is 40.5788MW as shown in Tab.3. It is to be noted that in this research, generator is not attacked (only loads and lines are attacked), so the attack vector, ΔP_D in case of LRA and GRC-LRA is same as shown in the 3rd and 4th rows of Tab.3.

Total operational cost and load shedding at low load variation at fixed tight ramp rates in 6 time steps of LRA and GRC-LRA are given in Tab.4.

Table 3. Generator power dispatches, P_g and attack vector, ΔP_D in LRA and GRC-LRA at tight fixed ramp rates in low load variation

R_u_g=R_d_g= [30 5 3 5 2] for six instances		Bus No.	Time Instances					
			1	**2**	**3**	**4**	**5**	**6**
LRA	$\boldsymbol{P_g}$	1	230.00	230.00	196.52	230.00	230.00	196.14
		2	5.47	5.14	0.00	5.54	5.07	0.00
		3	14.67	12.94	30.00	15.02	12.60	30.00
		6	0.00	0.00	0.00	0.00	0.00	0.00
		8	8.85	5.92	20.00	9.44	5.33	20.00
	$\boldsymbol{L_s}$	-	**0**	**0**	**13.4819**	**0**	**0**	**12.8602**
GRC-LRAV	$\boldsymbol{P_g}$	1	229.57	228.78	206.11	230.00	223.11	207.19
		2	5.00	0.00	0.00	1.11	0.00	0.00
		3	17.33	20.33	23.33	24.00	27.00	30.00
		6	0.20	0.00	0.00	0.00	0.00	0.00
		8	6.89	4.89	6.89	4.89	2.89	4.89
	$\boldsymbol{L_s}$	-	**0**	**0**	**23.6677**	**0**	**0**	**16.9111**
LRAV	$\Delta \boldsymbol{P_D}$	2	Eleven zeros	Eleven zeros	-10.8918	Eleven zeros	Eleven zeros	-10.8500
		3			38.553			38.4047
		4			-23.9922			-23.9000
		5			-3.6688			-3.6547
		6			0			0
		9			0			0
		10			0			0
		11			0			0
		12			0			0
		13			0			0
		14			0			0
GRC-LRAV	$\Delta \boldsymbol{P_D}$	2	Eleven zeros	Eleven zeros	-10.8918	Eleven zeros	Eleven zeros	-10.8500
		3			38.553			38.4047
		4			-23.9922			-23.9000

		5			-3.6688			-3.6547
		6			0			0
		9			0			0
		10			0			0
		11			0			0
		12			0			0
		13			0			0
		14			0			0

Table 4. Operational cost and load shedding due to LRA and GRC-LRA at fixed ramp rates in low load variation

Attack Resources, R	**Operational Cost, $/MWh**				**Load Shedding, MW**			
	Fixed Slack Ramp [150 25 15 25 10]		Fixed Tight Ramp [30 5 3 5 2]		Fixed Slack Ramp [150 25 15 25 10]		Fixed Tight Ramp [30 5 3 5 2]	
	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA
[0;0;0;0;0;0]	33638.52	33638.52	33638.52	33653.13	0	0	0	0
[0;0;20;0;0;20]	36567.46	36671.8	36567.46	37523.68	26.3420	29.2941	26.3420	40.5788

Economic loss only due to attack=Operational cost with R in LRA − Operational cost without R in LRA $\Longrightarrow$ $36567.46 - 33638.52 = 2928.94$

Economic loss only due to ramp=Operational cost without R in GRC-LRA− Operational cost without R in LRA $\Longrightarrow$ $33653.13 - 33638.52 = 14.61$

Economic loss due to attack and ramp separately= Economic loss only due to attack+ Economic loss only due to ramp $\Longrightarrow$ $2928.94 + 14.61 = 2943.55$

Economic loss due to both attack and ramp in GRC-LRA= Operational cost with R in GRC-LRA− Operational cost without R in LRA $\Longrightarrow$ $37523.68 - 33638.52 = 3885.16$

From the above economic loss analysis, it is clear that the economic loss in GRC-LRAV regarding scenario-1 is 3885.16$/MWh and sum of economic loss due to ramp and attack individually is 2543.55$/MWh as shown in Tab.5 and Fig.3. So, economic loss in GRC-LRAV is 1341.223$/MWh greater than the summation of economic losses due to LRAV and ramp.

Table 5. Economic loss due to Ramp, LRA and GRC-LRA at fixed ramp rates in low load variation

Ramp Limits	**Economic Loss, $/MWh**			
	Ramp	**LRA**	**Ramp and LRA**	**GRC-LRA**
Fixed Slack Ramp	0	2928.938	2928.938	3033.286
Fixed Tight Ramp	14.612	2928.938	2543.542	3885.161

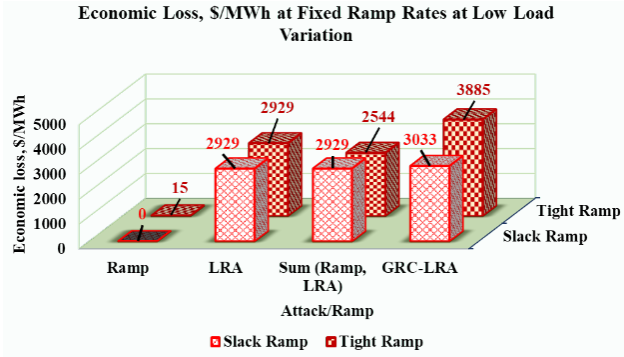

Fig. 3. Comparison of economic loss w.r.t. Ramp, LRA, $\sum Ramp, LRA$ and GRC-LRA at fixed ramp rates in low load variation

4.1.2 Scenario-2: High Load Variation with T=24 at Slack and Tight Fixed Ramp Rates

Let the load changes and attack triggering within 24 time steps is as given in Tab.6. Let the slack and tight ramp rates are R_u_g=R_d_g= [150 25 15 25 10] and R_u_g=R_d_g= [60 10 6 10 4] respectively. It is assumed that generators power dispatches at 0^{th} instant are $P_g^{(0)} = [111\ 0\ 0\ 0\ 0]$. Total operational cost and load shedding of high load variation at fixed slack and tight ramp rates in 24 time steps of LRA and GRC-LRA are given in Tab.7.

From Tab.7 economic loss calculations are done which are given in Tab.8. The economic loss in GRC-LRAV at slack ramp constraints ($R\_u_g = R\_d_g = [150\ 25\ 15\ 25\ 10]$) is 5480.489$/MWh and economic loss due to ramp and attack separately is 4317.856$/MWh as shown in Tab.8. So, economic loss in GRC-LRA at fixed slack ramp rate in high load varying conditions is 4211.243$/MWh greater than the sum of economic losses of attack and ramp individually. From Tab.8 it is also clear that the economic loss in GRC-LRAV at tight ramp constraints ($R_u_g = R_d_g = [60\ 10\ 6\ 10\ 4]$) is 8755.397$/MWh and economic loss due to ramp and attack separately is 4544.154$/MWh as shown in Tab.8 and Fig.4. So, economic loss in GRC-LRA is 4211.243$/MWh greater than the sum of economic losses due to attack and ramp individually.

Table 6. Load changes and attack triggering within 24 time steps

Time Instances	1	2	3	4	5	6
Load	148	173	220	244	259	248
R	0	0	0	0	20	20
Time Instances	7	8	9	10	11	12
Load	227	202	176	134	100	130

R	0	0	0	0	0	0
Time Instances	13	14	15	16	17	18
Load	157	168	195	225	244	241
R	0	0	0	0	20	20
Time Instances	19	20	21	22	23	24
Load	230	210	176	157	138	103
R	0	0	0	0	0	0

Table 7. Operational cost and load shedding due to LRA and GRC-LRA at fixed ramp rates in High Load Variation

Attack Resources, R	**Operational Cost, $/MWh**				**Load Shedding, MW**			
	Fixed Slack Ramp [150 25 15 25 10]		Fixed Tight Ramp [60 10 6 10 4]		Fixed Slack Ramp [150 25 15 25 10]		Fixed Tight Ramp [60 10 6 10 4]	
	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA
[0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0]	91604.8	91604.8	91604.8	91831.09	0	0	0	0
[0;0;0;0;20;20;0;0;0;0;0;0;0;0;0;20;20;0;0;0;0;0;0]	95922.65	97085.28	95922.65	100360.2	24.089	34.816	24.089	65.252

Table 8. Economic loss due to Ramp, LRA and GRC-LRA at Fixed Ramp Rates in High Load Variation

Ramp Limits	**Economic Loss, $/MWh**			
	Ramp	**LRA**	**Ramp and LRA**	**GRC-LRA**
Fixed Slack Ramp	0	4317.856	4317.856	5480.489
Fixed Tight Ramp	226.298	4317.856	4544.154	8755.397

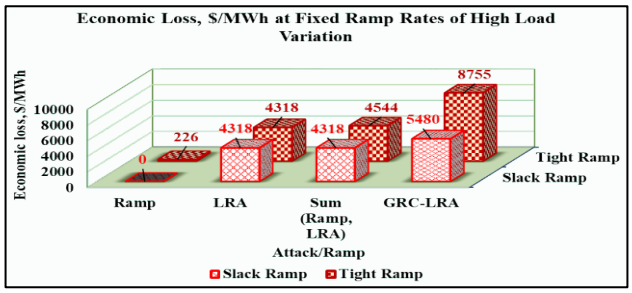

Fig. 4. Comparison of Economic loss w.r.t. Ramp, LRA, $\sum Ramp, LRA$ and GRC-LRA at fixed ramp rates of high load variation

4.2 Economic Loss due to Most Damaging GRC-LRAV at Variable Ramp Rates

4.2.1 Scenario-1: Low Load Variation with *T*=6

Similar to fixed ramp rates for the low load variation, the generation dispatches at 0^{th} instant are $P_g^{(0)}$= [230 5.41 14.33 0 8.27].

4.2.1.1 Slack Variable Ramp Rates

In this article, most damaging GRC-LRAV is obtained at the variable ramp rates in all time instances. Variable ramp rates are simulated in random within the ± 10 tolerance of fixed ramp rates i.e., slack fixed ramp rates ($R\_u_g = R\_d_g$ = [150 25 15 25 10]) are considered and the slack variable ramp rates are generated such that [135 22.5 13.5 2.5 9] $\leq R_{u_g}(or)\ R\_d_g \leq$ [165 27.5 16.5 27.5 11]. The considered variable slack ramp rates at low load variation are presented in Tab.A1.

Total operational cost and load shedding of low load variation in 6 time steps at slack variable ramp rates in case of LRA and GRC-LRA are given in Tab.9.

From Tab.9 economic loss calculations are done which are given in Tab.10. It is clear that the economic loss in GRC-LRAV at variable slack ramp rates given in Tab.A1 is 3067.124$/MWh and economic loss due to ramp and attack separately is 2928.938$/MWh as shown in Tab.10 and Fig.5. So, economic loss in GRC-LRA is 138.1861$/MWh greater than the summation individual loss by ramp and LRA.

4.2.1.2 Tight Variable Ramp Rates

Tight variable ramp rates are also simulated in random within the ± 10 tolerance of fixed tight ramp rates ($R\_u_g = R\_d_g$ = [30 5 3 5 2]) are considered and the tight variable ramp rates are generated such that [33 5.5 3.3 5.5 2.2] $\leq R_{u_g}(or)\ R\_d_g \leq$ [27 4.5 2.7 4.5 1.8]. The considered variable tight ramp rates at low load variation are presented in Tab.A2. Total operational cost and load shedding of low load variation in 6 time steps at tight variable ramp rates in case of LRA and GRC-LRA are given in Tab.9.

From Tab.9 economic loss calculations are done which are given in Tab.10. It is clear that the economic loss in GRC-LRAV at variable tight ramp rates mentioned in Tab.A2 is 3882.804$/MWh and economic loss due to ramp and attack separately is 2942.423$/MWh as shown in Tab.10 and Fig.5. So, economic loss in GRC-LRA is 940.3808$/MWh greater than the summation individual loss by ramp and LRA.

Table 9. Operational cost and load shedding due to LRA and GRC-LRA at Variable ramp rates in Low Load Variation

Attack Resources, R	Operational Cost, $/MWh				Load Shedding, MW			
	Variable Slack Ramp		Variable Tight Ramp		Variable Slack Ramp		Variable Tight Ramp	
	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA
[0;0;0;0;0;0]	33638.52	33638.52	33658.52	33652.00	0	0	0	0
[0;0;20;0;0;20]	36567.46	36705.64	36567.46	37521.32	26.3420	30.0018	26.3420	40.5374

Table 10. Economic loss due to Ramp, LRA and GRC-LRA at Variable Ramp Rates in Low Load Variation

Ramp Limits	Economic Loss, $/MWh			
Name	Ramp	LRA	Ramp and LRA	GRC-LRA
Variable Slack Ramp	0	2928.938	2928.938	3067.124
Variable Tight Ramp	13.485	2928.938	2942.423	3882.804

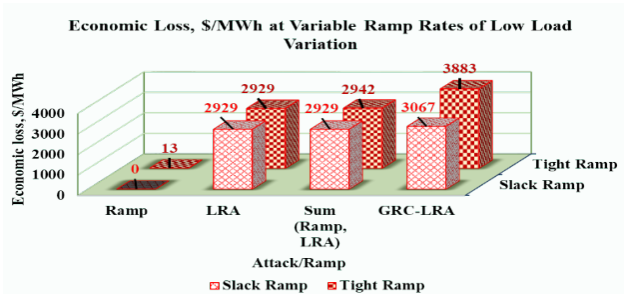

Fig. 5. Comparison of Economic loss w.r.t. Ramp, LRA, $\sum Ramp, LRA$ and GRC-LRA at variable ramp rates of low load variation

4.2.2 Scenario-1: High Load Variation with T=24

Similar to fixed ramp rates for the high load variation, the generation dispatches at 0^{th} instant are $P_g^{(0)}$= [110 0 0 0 0].

4.2.2.1 Slack Variable Ramp Rates

In this article, most damaging GRC-LRAV is obtained at the variable ramp rates in all time instances. Variable ramp rates are simulated in random within the ± 10 tolerance of fixed ramp rates i.e., slack fixed ramp rates ($R\_u_g = R\_d_g$ = [150 25 15 25 10]) are considered and the slack variable ramp rates are generated such that [135 22.5 13.5 2.5 9] $\leq R_{u_g}(or)\ R\_d_g \leq$ [165 27.5 16.5 27.5 11]. The considered variable slack ramp rates at high load variation of 24 instances are presented in Tab.A3.

Total operational cost and load shedding of low load variation in 24 time steps at slack variable ramp rates in case of LRA and GRC-LRA are given in Tab.11.

From Tab.11 economic loss calculations are done which are given in Tab.12. It is clear that the economic loss in GRC-LRAV at variable slack ramp rates represented in Tab.A3 is 5485.389$/MWh and economic loss due to ramp and attack separately is 4317.856$/MWh as shown in Tab.12 and Fig.5. So, economic loss in GRC-LRA is 1167.533$/MWh greater than the summation individual loss by ramp and LRA.

4.2.2.2 Tight Variable Ramp Rates

Tight variable ramp rates are also simulated in random within the ± 10 tolerance of fixed tight ramp rates ($R\_u_g = R\_d_g$ = [60 10 6 10 4]) are considered and the tight variable ramp rates are generated such that [54 9 5.4 9 3.6] $\leq R_{u_g}(or)\ R\_d_g \leq$ [66 11 6.6 11 4.4]. The considered variable tight ramp rates at low load variation are presented in Tab.A4.

Total operational cost and load shedding of low load variation in 24 time steps at tight variable ramp rates in case of LRA and GRC-LRA are given in Tab.11.

Table 11. Operational cost and load shedding due to LRA and GRC-LRA at Variable ramp rates in High Load Variation

Attack Resources, R	Operational Cost, $/MWh				Load Shedding, MW			
	Variable Slack Ramp		Variable Tight Ramp		Variable Slack Ramp		Variable Tight Ramp	
	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA	LRA	GRC-LRA
[0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0]	91604.8	91604.8	91604.8	91832.43	0	0	0	0
[0;0;0;0;20;20;0;0;0;0;0;0;0;0;0;0;0;0;20;20;0;0;0;0;0;0]	95922.65	97090.18	95922.65	100354.5	24.088	34.5210	24.088	64.5967

From Tab.11 economic loss calculations are done which are given in Tab.12. It is clear that the economic loss in GRC-LRAV at variable tight ramp rates given in Table.A4 is 8749.746$/MWh and economic loss due to ramp and attack separately is 4545.491$/MWh as shown in Tab.12 and Fig.6. So, economic loss in GRC-LRA is 4204.255$/MWh greater than the summation individual loss by ramp and LRA as shown in Fig.6.

GRC-LRA's BPP is solved by using both KKT conditions based single level MILPP method and Benders decomposition method. Comparison of two solving methods is done in terms of operational cost, load shedding, economic

loss and computational time at tight variable ramp rates as given in Tab.13. The difference between single level MILLP and Benders decomposition in terms of economic loss, load shedding is almost zero and the computational time for single level MILPP is more compared to Benders decomposition (less variable number in Benders decomposition) as shown in Tab.13.

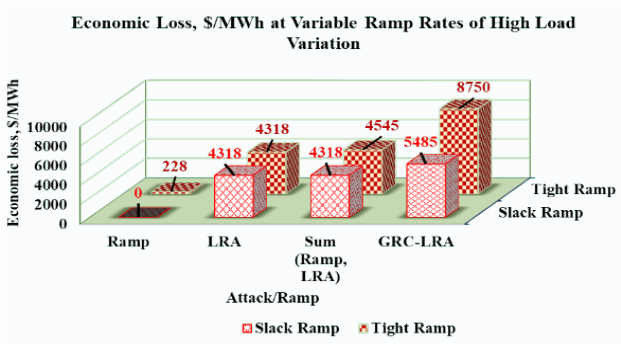

Fig. 6. Comparison of Economic loss w.r.t. Ramp, LRA, $\sum Ramp, LRA$ and GRC-LRA at variable ramp rates of high load variation

Table 12. Economic loss due to Ramp, LRA and GRC-LRA at Variable Ramp Rates in High Load Variation

Ramp Limits	Economic Loss, $/MWh			
Name	Ramp	LRA	Ramp and LRA	GRC-LRA
Variable Slack Ramp	0	4317.856	4317.856	5485.389
Variable Tight Ramp	227.6344	4317.856	4545.491	8749.746

Table 13. Comparison of Single-level MILPP and Benders decomposition methods in solving GRC-LRA at tight ramp rates of high load variation

In GRC-LRA	Single level MILPP	Benders decomposition	Difference
Operational cost, $/MWh	100354.542010487	100354.542010454	0
Load Shedding, MW	64.5967751310903	64.596775131090300	0
Economic loss, $/MWh	8749.74640800931	8749.74640800925	0
Computational Time, s	2000.831727	333.507929	–

4.3 Optimal Attack-Defense Strategy by Probabilistic Defense against GRC-LRA

An optimal attack-defense against GRC-LRAV is applied by finding optimal critical measuring units, then by framing possible attack strategies and further by playing static zero-sum game. In this article, an optimal attack-defense strategy is represented for high load variation of the test system at tight variable ramp rates.

4.3.1 Critical Measuring Units for Optimal Attack-Defense Strategy

Let the attack resources of the test system operating at high load variation with $T = 24$ and subjected to tight variable ramp rates as shown in Tab.A4. The economic loss due to GRC-LRAV in that case is 8749.746$/MWh. Based on the algorithm given in Section-3.3, the critical measuring units are derived based on the rank of the measuring unit after defending only that specific unit, are shown in Tab.14.

Now select the units $P_{D_6}, P_{D_5}, P_{D_9}$ and P_{D_7} (ranks of 1 to 4) and if defense is applied to all those four units at once, then the resultant economic loss ≅0. Hence these units can be considered as critical measuring units.

4.3.2 Probabilities of Optimal Attack-Defense Strategy of GRC-LRA

As mentioned in section-3.3, among four critical units, let the attacker has access to three units and the remaining non-critical units (maximum attack resources of 20). Let the defender has access to one critical unit among four.

Then the maximum number of possible attack strategies be $4_{C_3} = 4$ and maximum number of possible defense strategies is $4_{C_3} = 4$ [26]. The possible attack and defense strategies with their corresponding economic loss is shown in Tab.15.

The probabilities of optimal attack-defense strategy against GRC-LRAV (at Nash equilibrium) are given in Tab.16.

Table 14. Rank of measuring unit after defending each unit

Measuring Unit	P_{D_1}	P_{D_2}	P_{D_3}	P_{D_4}	P_{D_5}	P_{D_6}	P_{D_7}	P_{D_8}	P_{D_9}	$P_{D_{10}}$	$P_{D_{11}}$
Economic Loss After Defense	1195.104	1195.104	1195.104	1195.104	788.4727	500.0059	897.4489	997.5169	869.1998	1088.753	1195.104
Rank	7	7	7	7	2	1	4	5	3	6	7
Measuring Unit	P_{L_1}	P_{L_2}	P_{L_3}	P_{L_4}	P_{L_5}	P_{L_6}	P_{L_7}	P_{L_8}	P_{L_9}	$P_{L_{10}}$	$P_{L_{11}}$

Economic Loss After Defense	8749.746	7353.715	6757.732	7454.855	8001.295	7284.631	6677.091	6684.905	7290.3	6699.124	7427.436
Rank	20	15	11	17	18	12	8	9	13	10	16
Measuring Unit	$P_{L_{12}}$	$P_{L_{13}}$	$P_{L_{14}}$	$P_{L_{15}}$	$P_{L_{16}}$	$P_{L_{17}}$	$P_{L_{18}}$	$P_{L_{19}}$	$P_{L_{20}}$		
Economic Loss After Defense	8749.746	8749.746	8749.746	8749.746	8749.746	8044.641	7348.206	6757.732	8749.746		
Rank	20	20	20	20	20	19	14	11	20		

Table 15. Utility table, economic loss, $/MWh of all possible attack and defense strategies

Strategies	$\boldsymbol{D_1 = P_{D_5}}$	$\boldsymbol{D_2 = P_{D_6}}$	$\boldsymbol{D_3 = P_{D_7}}$	$\boldsymbol{D_4 = P_{D_9}}$
$\boldsymbol{A_1 = P_{D_5}, P_{D_6}, P_{D_9}}$	435.1796	562.2581	897.4489	227.6344
$\boldsymbol{A_2 = P_{D_5}, P_{D_7}, P_{D_9}}$	461.3374	500.0059	562.2581	250.1581
$\boldsymbol{A_3 = P_{D_5}, P_{D_6}, P_{D_7}}$	227.6344	250.1581	227.6344	869.1998
$\boldsymbol{A_4 = P_{D_6}, P_{D_7}, P_{D_9}}$	788.4727	461.3374	435.1796	227.6344

Table 16. Probabilities of optimal attack-defense strategy (Nash equilibrium) at variable tight ramp rates of high loading variation

Attack Probabilities, $P_{A\_S_a}$		**Defense Probabilities, $P_{D\_S_d}$**	
$\boldsymbol{P_{A_1}}$	0.4667	$\boldsymbol{P_{D_1}}$	0.1532
$\boldsymbol{P_{A_2}}$	0	$\boldsymbol{P_{D_2}}$	0.5363
$\boldsymbol{P_{A_3}}$	0.3293	$\boldsymbol{P_{D_3}}$	0
$\boldsymbol{P_{A_4}}$	0.2040	$\boldsymbol{P_{D_4}}$	0.3105
$\sum_{i=1}^{N_{S_A}} P_{A_{S_i}} = 0.4667 + 0 + 0.3293 + 0.2040$		$\sum_{i=1}^{N_{S_D}} P_{D_{S_i}} = 0.1532 + 0.5363 + 0 + 0.3105$	
$\Rightarrow \sum_{i=1}^{N_{S_A}} P_{A\_S_i} = 1$		$\Rightarrow \sum_{i=1}^{N_{S_D}} P_{D\_S_i} = 1$	

5. Conclusions

Cyber attacks in power systems are noteworthy as they can make system's economy, security and reliability vulnerable. Disruptive agents (attackers) can intrude into the system with complete or incomplete network information and inject undetectable false data into the system to mislead state estimation. Such kind of undetectable false data attacks are called FDIAs. LRAs are practical FDIAs that target bus power injections and line power flows to create unnecessary load shedding and line outages also that lead to considerable economic loss. To find the most damaging LRAV, a BPP is framed with attacker in upper level and basic SCOPF (operator) in the lower level. In this article generator ramp constraints are induced into basic SCOPF, to find the impact of ramp constraints on economic loss when an attack is triggered. The effect of ramp rates can directly effect a generator (when attacked) and create loss [23, 24]. The advantageous issue in this work is even if loads/lines are attacked in place of a generator, fixed/variable ramp rates can lead to more economic loss than basic LRA.

Mathematical model of GRC-LRA is framed on incorporating ramp constraints to basic LRA modelling. GRC-LRA's impact on operational cost/economic loss of the system is found by using two solvers. One is BPP is converted to KKT conditions based single-level MILPP method and the other is solving BPP directly by Benders decomposition method. GRC-LRA's effect is studied on the modified IEEE-14 bus test system. To illustrate the impact of ramp constraints in a better way, load is considered in two modes in which one of them is low load variation with 6 time instances and the other is high load variation with 24 time instances. In each mode of operation, again fixed and variable ramp rates are considered, whereas in further in each fixed and variable ramp rates are considered as slack (not-tight) or tight. Economic loss in two loading modes at fixed slack, fixed tight, variable slack and variable tight ramp rates are elucidated in Tab.5 and Fig.3, Tab.8 and Fig.4, Tab.10 and Fig.5 and, Tab.12 and Fig.6 respectively. From the aforementioned tables it is clear that the economic loss in GRC-LRA case is more than the sum of economic loss in ramp and LRA individually. From this study it can be concluded that generator ramp constraints must be considered while analyzing LRAs against power grid dynamically. For providing optimal defense, optimal critical measuring units are selected based on the ranking on measuring units shown in Tab.14. Probabilities of optimal attack-defense strategies are obtained by playing static zero-sum game on the utility table given in Tab.15. The optimal probabilities are given in Tab.16. Hence, this research gives the in-sight of the impacts of optimal attacking and defending strategies at fixed and variable ramp rates induced into LRA on SCOPF in power systems.

Acknowledgement

The authors like to show their sincere gratitude to the management, faculty and colleagues of Vignan's Foundation for Science, Technology and Research who have helped to carry out this research.

References

1. T. Zhang, Y. Wang, X. Liang, Z. Zhuang and W. Xu, Cyber attacks in cyber-physical power systems: A case study with GPRS-based SCADA systems, 29th Chin. Control. and Decis. Conf. (CCDC), pp. 6847-6852 (2017). https://doi.org/10.1109/CCDC.2017.7978413
2. Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, Cyber–physical security of a smart grid infrastructure, Proc. of the IEEE, **100(1)**, 195 (2011). https://doi.org/10.1109/CISS.2010
3. G. Liang, S. R. Weller, J. Zhao, F. Lu and Z. Y. Dong, The 2015 ukraine blackout: Implications for false data injection attacks, IEEE Transactions on Power Systems, **32(4)**, 3317 (2016). https://doi.org/10.1109/TPWRS.2016.2631891
4. K. Chatterjee, V. Padmini and S. A. Khaparde, Rev. of cyber-attacks on Power Syst. Oper., in 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, India, pp. 1-6 (2017). https://doi.org/10.1109/TENCONSpring.2017.8070085
5. Y. Yang, K. McLaughlin, T. Littler, S. Sezer, Eul Gyu Im, Z. Q. Yao, B. Pranggono and H. F. Wang, Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems, in 2012 Int. Conf. on Sustain. Power Gener. and Supply (SUPERGEN-2012), Hangzhou, China, pp. 1-8 (2012). https://doi.org/10.1049/cp.2012.1831
6. Y. Shen, M. Fei and D. Du, Cyber security study for power systems under denial of service attacks, Transactions of the Institute of Measurement and Control **41(6)**, 1, (2017). https://doi.org/10.1177/0142331217709528
7. 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 **14(1)**, 1, (2011). https://doi.org/10.1145/1653662.1653666
8. Y. Yuan, Z. Li and K. Ren, Modeling Load Redistribution Attacks in Power Systems, IEEE Transactions on Smart Grid, **2(2)**, 382, (2011). https://doi.org/10.1109/TSG.2011.2123925
9. Y. Yuan, Z. Li and K. Ren, Quantitative Analysis of Load Redistribution Attacks in Power Systems, IEEE Transactions on Parallel and Distribution Systems, **23(9)**, 1731, (2012). https://doi.org/10.1109/TPDS.2012.58
10. J. M. Arroyo and F. D. Galiana, On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem, IEEE Transactions on Power Systems, **20(2)**, 789, (2005). https://doi.org/10.1109/TPWRS.2005.846198
11. X. Liu, Z. Li, Z. Shuai and Y. Wen, Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution, IEEE Transactions on Smart Grid **8(2)**, 1023, (2017). https://doi.org/10.1109/TSG.2016.2623983
12. D. Choeum and D. H. Choi, Vulnerability Assessment of Conservation Voltage Reduction to Load Redistribution Attack in Unbalanced Active Distribution Networks, IEEE Transactions on Industrial Informatics, (2020). https://doi.org/10.1109/TII.2020.2980590
13. R. Kaviani and K. W. Hedman (2019) Identifying an Exploitable Structure for the Core Problem of Load-Redistribution Attack Problems, in 2019 North American Power Symposium (NAPS), Wichita, KS, USA, pp. 1-6 (2019). https://doi.org/10.1109/NAPS46351.2019.9000221
14. X. Liu and Z. Li, Local Load Redistribution Attacks in Power Systems with Incomplete Network Information, IEEE Transactions on Smart Grid **5(4)**, 1665, (2014). https://doi.org/10.1109/TSG.2013.2291661
15. X. Liu and Z. Li, Local Topology Attacks in Smart Grids. IEEE Transactions on Smart Grid, **8(6)**, 2617, (2017). https://doi.org/10.1109/TSG.2016.2532347
16. Y. Xiang, L. Wang, D. Yu and N. Liu, Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks, in 2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA , pp. 1-5 (2015). https://doi.org/10.1109/PESGM.2015.7286402
17. Y. Xiang, L. Wang and N. Liu, A framework for modeling load redistribution attacks coordinating with switching attacks, in 2017 IEEE Power & Energy Soc. Gen. Meet., pp 1-5 (2018). https://doi.org/10.1109/PESGM.2017.8274621
18. Z. Li, M. Shahidehpour, Z. Alabdulwahab and A. Abusorrah, Bilevel model for analyzing coordinated cyber-physical attacks on power systems, IEEE Transactions on Smart Grid, **7(5)**, 2260, (2015). https://doi.org/10.1109/TSG.2015.2456107
19. Fu J, Wang L, Hu B, Xie K, Chao H, Zhou P, A Sequential Coordinated Attack Model for Cyber-Physical System Considering Cascading Failure and Load Redistribution in 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, pp. 1-6, (2018). https://doi.org/10.1109/EI2.2018.8582135
20. Y. Xiang, Z. Ding, Y. Zhang and L. Wang, Power system reliability evaluation considering load redistribution attacks, IEEE Trans on Smart Grid, **8(2)**, 889, (2016). https://doi.org/10.1109/TSG.2016.2569589
21. Z. Ding, Y. Xiang and L. Wang (2016) Quantifying the influence of local load redistribution attack on power supply adequacy. In: 2016 IEEE Power and Energy Society General Meeting (PESGM), pp 1-5. Boston, MA, USA. https://doi.org/10.1109/PESGM.2016.7741526
22. H. Shayan and T. Amraee, Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads, IEEE Transactions on Smart Grid, **10(6)**, 6449, (2019). https://doi.org/10.1109/TSG.2019.2904873
23. D. H. Choi and L. Xie, Ramp-induced data attacks on look-ahead dispatch in real-time power markets, IEEE Trans on Smart Grid, **4(3)**, 1235, (2013). https://doi.org/10.1109/TSG.2012.2228508
24. L. Che, X. Liu, Z. Shuai and J. Zhao, The Impact of Ramp-Induced Data Attacks on Power System Operational Security, IEEE Transactions on Industrial Informatics, **15(9)**, 5064, (2019).
25. K. B. Krishna, K. M. Rosalina, N. Ramaraj, Complete and Incomplete Observability Analysis by Optimal PMU Placement Techniques of a Network, Journal of Electrical Engineering & Technology, **13(5)**, 1814, (2018). https://doi.org/10.5370/JEET.2018.13.5.1814
26. Y. Xiang and L. Wang, A game-theoretic approach to optimal defense strategy against load redistribution attack, in 2015 IEEE Power & Energy Society General Meeting, pp. 1-5 (2015). https://doi.org/10.1109/PESGM.2015.7286529
27. Y. Xiang and L. Wang, A game-theoretic study of load redistribution attack and defense in power systems, Electrical Power Systems Research **151**, 12, (2017). https://doi.org/10.1016/j.epsr.2017.05.020
28. R. D. Zimmerman, C. E. Murillo-Sánchez and R. J. Thomas, MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education, IEEE Transactions on Power Systems, **26(1)**, 12, (2011). https://doi.org/10.1109/TPWRS.2010.2051168
29. IBM ILOG CPLEX Optimization Studio. Version 12.9.0. Available: https://www.ibm.com/inen/products/ilogcplexoptimizationstudio

Appendix

Tab.A1 and Tab.A2 represent the slack and tight variable ramp rates at low load variation $\forall\, t = \{1,2,\dots,6\}$ respectively. However, Tab.A3 and Tab.A4 represent the slack and tight variable ramp rates at high load variations $\forall\, t = \{1,2,\dots,24\}$ respectively.

Table A1. Slack Variable Ramp Rates at Low Load Variation of $T = 6$

	P_{g_1}	P_{g_2}	P_{g_3}	P_{g_6}	P_{g_8}
$t = 1$	159	26.5	15.9	26.5	10.6
$t = 2$	162	27	16.2	27	10.8
$t = 3$	139.5	23.25	13.95	23.25	9.3
$t = 4$	162	27	16.2	27	10.8
$t = 5$	154.5	25.75	15.45	25.75	10.3
$t = 6$	138	23	13.8	23	9.2

Table A2. Tight Variable Ramp Rates at Low Load Variation of $T = 6$

	P_{g_1}	P_{g_2}	P_{g_3}	P_{g_6}	P_{g_8}
$t = 1$	30	5	3	5	2
$t = 2$	29.7	4.95	2.97	4.95	1.98
$t = 3$	30.9	5.15	3.09	5.15	2.06
$t = 4$	31.2	5.2	3.12	5.2	2.08
$t = 5$	31.5	5.25	3.15	5.25	2.1
$t = 6$	28.8	4.8	2.88	4.8	1.92

Table A3. Slack Variable Ramp Rates at High Load Variation of $T = 24$

	P_{g_1}	P_{g_2}	P_{g_3}	P_{g_6}	P_{g_8}
$t = 1$	156	26	15.6	26	10.4
$t = 2$	157.5	26.25	15.75	26.25	10.5
$t = 3$	157.5	26.25	15.75	26.25	10.5
$t = 4$	147	24.5	14.7	24.5	9.8
$t = 5$	154.5	25.75	15.45	25.75	10.3
$t = 6$	139.5	23.25	13.95	23.25	9.3
$t = 7$	156	26	15.6	26	10.4
$t = 8$	136.5	22.75	13.65	22.75	9.1
$t = 9$	144	24	14.4	24	9.6
$t = 10$	136.5	22.75	13.65	22.75	9.1
$t = 11$	138	23	13.8	23	9.2
$t = 12$	159	26.5	15.9	26.5	10.6
$t = 13$	156	26	15.6	26	10.4
$t = 14$	144	24	14.4	24	9.6
$t = 15$	163.5	27.25	16.35	27.25	10.9
$t = 16$	136.5	22.75	13.65	22.75	9.1
$t = 17$	148.5	24.75	14.85	24.75	9.9
$t = 18$	147	24.5	14.7	24.5	9.8
$t = 19$	157.5	26.25	15.75	26.25	10.5
$t = 20$	159	26.5	15.9	26.5	10.6
$t = 21$	141	23.5	14.1	23.5	9.4
$t = 22$	150	25	15	25	10
$t = 23$	148.5	24.75	14.85	24.75	9.9
$t = 24$	154.5	25.75	15.45	25.75	10.3

Table A4. Tight Variable Ramp Rates at High Load Variation of $T = 24$

	P_{g_1}	P_{g_2}	P_{g_3}	P_{g_6}	P_{g_8}
$t = 1$	56.4	9.4	5.64	9.4	3.76
$t = 2$	58.2	9.7	5.82	9.7	3.88
$t = 3$	64.8	10.8	6.48	10.8	4.32
$t = 4$	58.8	9.8	5.88	9.8	3.92
$t = 5$	60.6	10.1	6.06	10.1	4.04
$t = 6$	65.4	10.9	6.54	10.9	4.36
$t = 7$	63.6	10.6	6.36	10.6	4.24
$t = 8$	61.2	10.2	6.12	10.2	4.08
$t = 9$	61.8	10.3	6.18	10.3	4.12
$t = 10$	59.4	9.9	5.94	9.9	3.96

$t = 11$	57	9.5	5.7	9.5	3.8
$t = 12$	55.8	9.3	5.58	9.3	3.72
$t = 13$	60.6	10.1	6.06	10.1	4.04
$t = 14$	59.4	9.9	5.94	9.9	3.96
$t = 15$	65.4	10.9	6.54	10.9	4.36
$t = 16$	63.6	10.6	6.36	10.6	4.24
$t = 17$	57	9.5	5.7	9.5	3.8
$t = 18$	64.8	10.8	6.48	10.8	4.32
$t = 19$	55.2	9.2	5.52	9.2	3.68
$t = 20$	55.8	9.3	5.58	9.3	3.72
$t = 21$	63.6	10.6	6.36	10.6	4.24
$t = 22$	58.8	9.8	5.88	9.8	3.92
$t = 23$	63.6	10.6	6.36	10.6	4.24
$t = 24$	61.8	10.3	6.18	10.3	4.12

Nomenclature

Abbreviations

PMU	Phasor Measurement Unit
RTU	Remote Terminal Unit
DoS attacks	Denial of Service attacks
SCADA	Supervisory Control and Data Acquisition
FDIA	False Data Injection Attack
FDIAV	False Data Injection Attack Vector
SCED	Security Constrained Economic Dispatch
SCOPF	Security Constrained Optimal Power Flow
LRA	Load Redistribution Attack
LRAV	Load Redistribution Attack Vector
GRC-LRA	Generator Ramp Constraints induced Load Redistribution Attack
GRC-LRAV	Generator Ramp Constraints induced Load Redistribution Attack Vector
BPP	Bi-level Programming Problem
MILPP	Mixed Integer Linear Programming Problem
KKT conditions	Karush-Kuhn-Tucker conditions

Symbols

P_{g_i}	Power Dispatch of i^{th} generator
L_{s_k}	Load Shedding/Curtailment of k^{th} load
ΔP_{D_k}	Load attack on k^{th} load
ΔP_{L_l}	Line attack on l^{th} generator
$\boldsymbol{R}$	Vector of attack resources
θ_{D_k}	$\begin{cases} 1 \; if \; \Delta P_{D_k} \neq 0 \\ else \; 0 \end{cases}$
θ_{D+_k}	$\begin{cases} 1 \; if \; \Delta P_{D_k} > 0 \\ else \; 0 \end{cases}$
θ_{D-_k}	$\begin{cases} 1 \; if \; \Delta P_{D_k} < 0 \\ else \; 0 \end{cases}$
θ_{L_l}	$\begin{cases} 1 \; if \; \Delta P_{L_l} \neq 0 \\ else \; 0 \end{cases}$
θ_{L+_l}	$\begin{cases} 1 \; if \; \Delta P_{L_l} > 0 \\ else \; 0 \end{cases}$
θ_{L-_l}	$\begin{cases} 1 \; if \; \Delta P_{L_l} < 0 \\ else \; 0 \end{cases}$
P_{D_k}	Load demand of k^{th} load
P_{L_l}	Power flow on l^{th} line
$R\_u_{g_i}, R\_d_{g_i}$	Up and down ramp rates of i^{th} generator
$\boldsymbol{SF}, \boldsymbol{KD}$	Shift Factor and Bus-generator incidence matrices
M, ε	Sufficiently large and sufficiently small positive numbers
τ	Attack deviation bound on load bus
$\underline{A_l}, \overline{A_l}$	Lagrange multipliers for upper and lower bounds of l^{th} transmission line
$\underline{B_i}, \overline{B_i}$	Lagrange multipliers for upper and lower bounds of i^{th} generator
$\underline{\Gamma_k}, \overline{\Gamma}_k$	Lagrange multipliers for upper and lower bounds of k^{th} load

ru_i^t, rd_i^t	Lagrange multipliers for ramp up and ramp down of i^{th} generator
$\omega_{\underline{A},l}, \omega_{\overline{A},l}$, $\omega_{\underline{B},i}, \omega_{\overline{B},i}$, $\omega_{\underline{\Gamma},k}, \omega_{\overline{\Gamma},k}$, $\omega_{ru_i^t}, \omega_{rd_i^t}$	Binary variables that represent complementary slackness conditions of l^{th} transmission line, i^{th} generator, k^{th} load and ramping of i^{th} generator
A_m, D_n	m attack and n defense strategies
P_{A_m}, P_{D_n}	Probabilities of m^{th} attack and n^{th} defense strategies