Technology and Economics of Smart Grids and Sustainable Energy (2022) 7:22
https://doi.org/10.1007/s40866-022-00131-4

ORIGINAL PAPER

# Economic Loss Utilized Probabilistic Defense against Load Redistribution Attacks by Selecting Optimal Critical Measuring Units

C Sravanthi Kommoju[1] · Mercy Rosalina Kotapuri[1]

Received: 8 November 2019 / Accepted: 19 January 2022 / Published online: 23 May 2022


## Abstract

State Estimation (SE) reflects the real time operation of power system network in the present cyber-physical power world. However, prior research works depict that bad/false undetectable data can be injected into the system on compromising measuring devices like Remote Terminal Units or Phasor Measurement Units. If an attacker intrudes into the cyber network and injects successful undetectable bad data, then that attack is popular as False Data Injection Attack (FDIA). One practical FDIA is Load Redistribution Attack (LRA), which target bus active power injections and line active power flows. LRA harms SE and subsequently disturbs Security Constrained Economic Dispatch (SCED) which result in severe rise of power generation and load shedding costs. Hence to maintain grid's security, defense is one of the optimistic options. Attacker or defender won't have access or control over all units. So, certain critical measuring units must be considered to attack or defend the system. In this research article, a procedure is developed to select optimal critical units subjected to all possible attack resources and load variations. The developed procedure is analyzed on three loading scenarios of modified IEEE-14 bus test system. These critical units are set as basis to find an optimal attack-defense strategy among possible strategies, which is accomplished by static zero-sum game theory in which economic loss is utility. This study provides an in-sight of consequences due to LRA, critical units' selection under load variations and probabilistic optimal attack-defense strategy of the modified IEEE-14 bus system at three loading conditions.

**Keywords** False Data Injection Attacks (FDIAs) · Load Redistribution Attacks (LRAs) · Security Constrained Economic Dispatch (SCED) · Economic Loss · Critical Measuring Units · Static zero-sum Game Theory

## 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 |
| BPP | Bi-level Programming Problem |
| MILPP | Mixed Integer Linear Programming Problem |
| KKT conditions | Karush-Kuhn-Tucker conditions |

### LRAV Parameters

| | |
|---|---|
| $N_d$ | Number of Load buses |
| $N_g$ | Number of generator buses |
| $N_l$ | Number of transmission lines |
| $C_{g_i}$ | Cost Coefficient of $i^{th}$ generator |

✉ Mercy Rosalina Kotapuri
kmr_eee@vignan.ac.in

C Sravanthi Kommoju
kcs_eeep@vignan.ac.in

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

| | |
|---|---|
| $k, i, l$ | Indices of load bus, generator bus and line respectively |
| $P_{g_i}$ | Power Generation Dispatch of $i^{th}$ generator |
| $C_{s_k}$ | Load Shedding Cost of $k^{th}$ load |
| $L_{s_k}$ | Load Shedding/Curtailment of $k^{th}$ load |
| $P_{D_k}$ | Load demand on $k^{th}$ load |
| $\Delta P_{D_k}$ | Load attack on $k^{th}$ load |
| $\Delta P_{L_l}$ | Line attack on $l^{th}$ line |
| $R$ | Number of attack resources |
| $\theta_{D_k}$ | $\begin{cases} 1 \; if \; \Delta P_{D_k} \neq 0 \\ else \; 0 \end{cases}$ |
| $\theta_{D+_k}$ | $\begin{cases} 1 \; if \; \Delta P_{D_k} > 0 \\ else \; 0 \end{cases}$ |
| $\theta_{D-_k}$ | $\begin{cases} 1 \; if \; \Delta P_{D_k} < 0 \\ else \; 0 \end{cases}$ |
| $\theta_{L_l}$ | $\begin{cases} 1 \; if \; \Delta P_{L_l} \neq 0 \\ else \; 0 \end{cases}$ |
| $\theta_{L+_l}$ | $\begin{cases} 1 \; if \; \Delta P_{L_l} > 0 \\ else \; 0 \end{cases}$ |
| $\theta_{L-_l}$ | $\begin{cases} 1 \; if \; \Delta P_{L_l} < 0 \\ else \; 0 \end{cases}$ |
| $P_{L_l}$ | Power flow on $l^{th}$ line |
| $SF, KD, KP$ | Shift Factor, Bus-generator and Bus-Load Incidence Matrices |
| $M, \varepsilon$ | Sufficiently large and sufficiently small positive numbers |
| $\tau$ | Attack deviation bound on load bus |
| $\lambda$ | Lagrange multiplier for power balance equality constraint |
| $\mu_l$ | Lagrange multiplier for $l^{th}$ line power flow equality constraint |
| $\underset{-l}{\mathrm{A}}, \overline{\mathrm{A}}_l$ | Lagrange multipliers for upper and lower bounds of $l^{th}$ transmission line |
| $\underset{-i}{\mathrm{B}}, \overline{\mathrm{B}}_i$ | Lagrange multipliers for upper and lower bounds of $i^{th}$ generator |
| $\underset{-k}{\Gamma}, \overline{\Gamma}_k$ | Lagrange multipliers for upper and lower bounds of $k^{th}$ load |
| $\omega_{\mathrm{A},l}, \omega_{\overline{\mathrm{A}},l}, \omega_{\mathrm{B},i}, \omega_{\overline{\mathrm{B}},i}, \omega_{\Gamma,k}, \omega_{\overline{\Gamma},k}$ | Binary variables that represent complementary slackness conditions of $l^{th}$ transmission line, $i^{th}$ generator and $k^{th}$ load |

**Defense Parameters**

| | |
|---|---|
| $A, D$ | Attacker and defender |
| $c_m$ | Number of Critical measuring units |
| $n_A, n_D$ | Number of attacker accessible and defender protectable critical resources |
| $N_{s_A}, N_{s_D}$ | Maximum no. of possible strategies for attacker and defender respectively |
| $A\_A_{space}, D\_A_{space}$ | Attacker's and defender's action spaces |
| $A_{s_a}$ | $a^{th}$ attack strategy in $A\_A_{space}$ |
| $D_{s_d}$ | $d^{th}$ defense strategy in $D\_A_{space}$ |
| $f(A, D)$ | Utility of static zero-sum game (Economic Loss) |
| $U_A, U_D$ | Utility functions of attacker and defender |
| $P_{A\_S_a}$ | Probability of $a^{th}$ attack strategy in $A\_A_{\text{space}}$ |
| $P_{D\_S_d}$ | Probability of $d^{th}$ defense strategy in $D\_A_{\text{space}}$ |

## Introduction

In the present technological society, electric power systems' security and reliability gained a significant role in driving any country's economy. Smart grid has more novel intelligent cyber networks, secured information protocols, smart meters, Phasor Measurement Units (PMUs) etc., that leads the electric network to a modern era power systems called as cyber-physical network. Deployment of advanced information technology and communication protocols to this system has made it more prone and vulnerable to cyber-attacks. Attackers can intrude in the middle of substation to control center and be able to launch man-in-middle attack for changing the state of system components [22]. Attacker can crack private keys and introduce malicious data into digital measuring devices. It is highly probable to create DoS (Denial-of-Service) attacks which target communication network [16]. So in this scenario, the cyber security has established its essentiality in cyber-physical power world.

Generally, in power systems' operation and control, bus power injections, line power flows, bus voltage vectors, line currents etc., are continuously sensed by Remote Terminal Units (RTUs)/PMUs where tracked data is transmitted to the Supervisory Control and Data Acquisition (SCADA) master at control center, then the states of the system are estimated by operator. If an attacker in the middle tries to inject bad/

false data into the system, classically, it can get detected by the operator with the help of $\chi^2-$ distribution hypothesis testing. But Liu et al. developed an undetectable False Data Injection Attack Vector (FDIAV) by using basics of Kirchoff's Current Law (KCL) and Kirchoff's Voltage Law (KVL) which is undetectable by Intrusion Detection System (IDS), but the State Estimation (SE) results in deviated estimates than actuals. Subsequently, even a trained operator can take bad decisions [13]. This in further can influence Security Constrained Economic Dispatch (SCED)/ Security Constrained Optimal Power Flow (SCOPF) and Contingency Management too, one of the important aspects in deregulated electricity market. FDIA can even lead to cascading of multiple line outages/generator outages that can create subsequent system 'blackout' [15].

Yuan et al. later came up with a practical FDIA, called Load Redistribution Attack (LRA). LRAs are developed in two forms, Immediate LRA and Delayed LRA. Immediate LRA maximizes economic loss and load shedding of the system immediately after the attack without any line outages, after performing SCED [23] and delayed LRA maximizes economic loss, load shedding and causes line outages in the system [24]. Delayed LRAs are more vulnerable than immediate LRAs. It is to be noted that attacker tries to get maximum economic loss with minimum number of resources. Maximum economic loss can be achieved by most damaging Load Redistribution Attack Vector (LRAV). Most damaging immediate LRAV of an immediate LRA can be obtained by solving a Bi-level Programming Problem (BPP) and however most damaging delayed LRAV is obtained by solving a Tri-level Programming Problem (TPP). In literature, BPP is solved by converting two-levels of BPP to single level Mixed Integer Linear Programming Problem (MILPP) using KKT (Karush-Kuhn-Tucker) conditions or duality, whereas TPP is solved by KKT conditions and duality [23]. A fast economic solution for LRA's BPP is found by framing BPP as two single-level programming problems and solved within less time that resulted in approximate solutions [12]. Moreover, multiple studies have been done on local LRAs [10, 11], coordinated cyber-physical LRAs [20, 21], system's reliability assessment after LRAs [6, 17].

Cyber-attacks directly or indirectly effect system services and make cyber-physical system vulnerable. Cyber security now finds its credit in securing the cyber network. Securing whole system is not an optimal solution as it leads to high budget allocation and it also may not be possible to protect all time, due to intelligent attacks. As per researchers, if one component in a substation/bus is compromised, the whole substation could be in their control. Defense at only one bus all time is not optimal. Defense strategies and security resources must be time changing [19]. Defense against attacks can be solved by either deterministic or probabilistic methods.

Probabilistic methods due to their advantage of randomness and uncertainties have gained their advantages in finding an optimal defense strategy. Different defense strategic methods against FDIAs have been developed by many researchers using Graphical defense method [1] and game theory methods [3–5, 7, 18]. Deng et al. have proposed a least budget defense strategy for protection against FDIAs in large scale power systems, in which critical meters are selected by modelling an MILPP, solved by Benders' Decomposition [5]. Reliable strategies for defense against targeted attacks were explored by Chen et al. on developing budget allocation analysis and two allocation algorithms [3]. Esmalifalak et al. specified that how electricity energy market prices are targetable for bad data injections. Proportional times of attack and defense actions of attacker and defender are found by zero-sum game theory [7]. Chen et al. have developed Poisson distribution probability based intrusion models for attacking and applied Markov transition game theory for defense [4].

Xiang and Wang have proposed probabilistic based static zero-sum and static non-zero sum game theories [18] and, Markov zero-sum game theory [19] concepts for optimal attacker-defender strategy considering load curtailment as utility. However, researchers in literature have considered only load shedding as utility function but not economic loss which is very severe due to LRA. The main advantage of considering economic loss as utility is, it not only involves load shedding cost but also generator operational cost when an LRA is triggered. In the previous probabilistic based defense literature, critical measuring units/nodes are considered based on entropic degree of a bus [19] or the nodes and lines operating higher or near to critical operating points [18]. This article illustrates the advantage of economic loss over load shedding after the successful intrusion of an LRA and also gives a procedure to find optimal critical units of modified IEEE-14 bus system

Main contribution of this research article are briefed as follows:

1. Maximum economic loss by most damaging LRAV of a modified IEEE-14 bus system is found by converting BPP to single-level MILPP using Karush-Kuhn-Tucker (KKT) conditions.
2. Selection of critical measuring units and their number for better attack or defense is achieved by developing an algorithm and validated by applying it to three loading scenarios of a modified IEEE-14 bus system.
3. Probabilities of optimal attack-defense strategy are found by applying static zero-sum game theory on selected critical measurements, where economic loss is considered as utility function in game theory.

This research article is organized in a way that second section deals with introduction to FDIAs and LRAs,

mathematical formulation of FDIA, LRAs' mathematical formulation and solving BPP using single-level MILPP whereas third section presents the defense methodology to find optimal critical units and static zero-sum game theory for optimal attack-defense strategy. Fourth section demonstrates three studies namely developing worst economic loss, selection of critical units at three loadings and probabilities of optimal attack-defense strategies at three load conditions. Finally, conclusions are discussed in fifth section.

## Load Redistribution Attack (LRA):

False/bad data vectors can be injected into the network measuring devices (measuring units) like RTUs/PMUs, that can observe the system all time [9]. RTUs/PMUs placed in the network can acquire (track) real-time operating data of active and reactive power measurements and communicate that data to the control center through Intelligent Electronic Devices (IEDs), Firewalls and Wide Area Networks (WANs). Then that data is communicated to Internet Cloud of Independent System Operators (ISOs)/Regional Transmission Organizations (RTOs) (Electricity Market). At the control center of ISOs/RTOs several estimation algorithms like DC state estimation, SCED, contingency analysis etc., work dependently based on communicated real-time bus active power injections and line active power flows. Classically, bad data is detected by residual detection methods, but in 2011, Liu et al. have proposed that an undetectable FDIAV can be developed by considering $a = H * c$, where $a$ is the attack vector,$H$ refers to complete network topology and $c$ is a random vector. But in practice, complete network topology can't be accessible by attacker. Moreover, to create an LRAV, active power measurements must be changed. An undetectable LRAV (bypass residual detection methods) can be structured by redistributing the zero-sum load change among the attacker's accessible measuring units of loads [23]. Hence these kind of practical FDIAs are named as Load Redistribution Attacks (LRAs) [23]. Yuan et al. have developed LRAV with some assumptions that measurement devices of load buses and lines can be attackable but not measuring units of generator or zero injection buses.

It is assumed that load can be varied by attacker only within $\pm\tau\%$ of true load demands. Line flow measurements can also be attackable as they provide assistance to inject a successful attack vector. A successful random vector injected into load and line flow measurements gets estimated to false states and false generator power dispatches on solving SE and SCED respectively. False generator dispatches obviously lead to line outages. Consequently, LRAVs results in economic loss and load shedding in case of immediate LRA whereas delayed LRAs lead to line outages too.

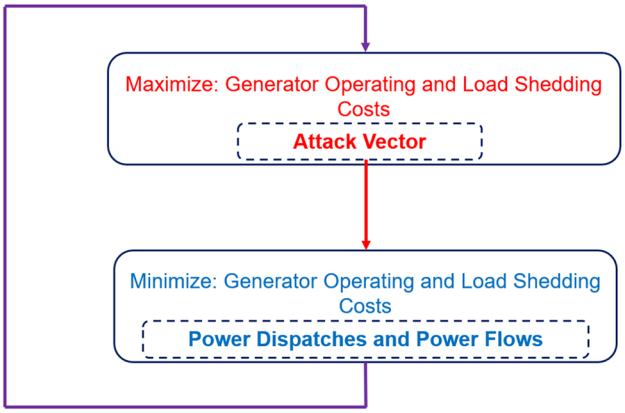


**Fig. 1** Bi-level model of an immediate LRAV

LRAV is a random attack vector that creates economic loss and load shedding which is undetectable prior to SE. Hence it is reliable to find the most damaging attack vector that causes maximum economic loss and load shedding subjected to attacker resource constraint as it helps to get notice that which measurement should be protected against LRAV. Let for one-time step attacker injects a successful LRAV into load and line flow measurements considered that in the next time step operator makes his/her decisions based on SCED injected LRAV. So, this consideration can be framed as a BPP, where upper level is dealt by attacker and lower level is tackled by operator. Attacker has his/her attack constraints like load variation, accessible buses and lines, available resources etc., and operator has basic SCED constraints. Attacker's aim is to maximize total operational cost (sum of generator operational cost and load shedding cost) and operator's goal is to minimize total operational cost. In this paper, most damaging LRAV is found by solving the bi-level optimization problem. The bi-level model to find economic loss due to most damaging LRAV is shown in Fig. 1.

BPP is expressed mathematically in upper (1)-(7) and lower (8)-(13) levels for finding the most damaging LRAV. Attacker maximizes total operational cost (1) subjected to zero-sum load redistribution (2), change in line power flow by shift factor ($SF$) and bus-load incidence ($KD$) matrices (3) and, attacker's accessible load variation tolerance (4) bounds. While (5) and (6) talk about the logical compromising of attacker with load bus and line flow measuring units and (7) deals with number of attackable resources accessible. Conversely, operator minimizes total operational cost (8) subjected to basic SCOPF constraints like power balance (9), line power flow (10), generator bounds (11), line flow limit (12) and load curtailment limits (13).

Mathematical representation of BPP in case of immediate LR attacks is given by equations (1) to (13) [23]:

**Representing Attacker:**

Attacker's Objective Function: Maximize generator operational and load shedding costs →

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

Undetectable Load Attack Vector →

$$s.t. \sum_{k=1}^{N_d} \Delta P_{Dk} = 0 \tag{2}$$

Undetectable Attack Vector of line power flows →

$$\Delta P_L = -SF.KD.\Delta P_D \tag{3}$$

Load Attack vector limit →

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

Compromising load attack measurements →

$$\Delta P_{D_k} = 0 \iff \theta_{D_k} = 0 \rightarrow \begin{cases} \Delta P_{D_k} + \tau P_{D_k} \theta_{D_k} \ge 0 \\ \Delta P_{D_k} - \tau P_{D_k} \theta_{D_k} \le 0 \\ \theta_{D+_k} + \theta_{D-_k} - 2\theta_{D_k} \le 0 \\ \Delta P_{D_k} + \left(-\tau P_{D_k} - \varepsilon\right)\theta_{D+_k} \ge -\tau P_{D_k} \\ \Delta P_{D_k} + \left(\tau P_{D_k} + \varepsilon\right)\theta_{D-_k} \le \tau P_{D_k} \\ \theta_{D+_k} + \theta_{D-_k} + \theta_{D_k} \le 2 \\ \theta_{D+_k} + \theta_{D-_k} - \theta_{D_k} \ge 0 \\ \theta_{D+_k}, \theta_{D-_k}, \theta_{D_k} \in \{0,1\} \end{cases} \tag{5}$$

Compromising line flow attack measurements →

$$\Delta P_{L_l} = 0 \iff \theta_{L_l} = 0 \rightarrow \begin{cases} \Delta P_{L_l} + M\theta_{L_l} \ge 0 \\ \Delta P_{L_l} - M\theta_{L_l} \le 0 \\ \theta_{L+_l} + \theta_{L-_l} - 2\theta_{L_l} \le 0 \\ \Delta P_{L_l} + (-M - \varepsilon)\theta_{L+_l} \ge -M \\ \Delta P_{L_l} + (M + \varepsilon)\theta_{L-_l} \le M \\ \theta_{L+_l} + \theta_{L-_l} + \theta_{L_l} \le 2 \\ \theta_{L+_l} + \theta_{L-_l} - \theta_{L_l} \ge 0 \\ \theta_{L+_l}, \theta_{L-_l}, \theta_{L_l} \in \{0,1\} \end{cases} \tag{6}$$

Attack Resources Limit →

$$\sum_{k=1}^{N_d} \theta_{D_k} + 2\sum_{l=1}^{N_l} \theta_{L_l} \le R \tag{7}$$

**Representing Operator:**

Operator's Objective function: Minimize generator operational and load shedding costs →

$$\{P_g, L_s\} = arg\left\{ \underset{P_g, L_s}{\text{Min}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i} + \sum_{k=1}^{N_d} C_{s_k} * L_{sk} \right\} \tag{8}$$

Power balance constraint →

$$\sum_{i=1}^{N_g} P_{g_i} = \sum_{k=1}^{N_d} (P_{Dk} - L_{sk}) \tag{9}$$

$$\text{Line power flow with attack vector} \rightarrow P_L = SF.KP.P_g - SF.KD.(P_D + \Delta P_D - L_s) \tag{10}$$

$$\text{Line power flow limits} \rightarrow -P_{L_l}^{max} \leq P_{L_l} \leq P_{L_l}^{max} \tag{11}$$

$$\text{Power generation limits} \rightarrow P_{g_i}^{min} \leq P_{g_i} \leq P_{g_i}^{max} \tag{12}$$

$$\text{Load shedding limits} \rightarrow 0 \leq L_{s_k} \leq P_{D_k} + \Delta P_{D_k} \tag{13}$$

BPP to find most damaging LRAV can be solved by several methods where a classical method is to convert BPP to single-level MILPP using KKT conditions. When KKT conditions are applied on the objective function of lower-level in BPP, additional constraints (14)-(17) will come into existence [23].

$$\text{Attackers Objective Function}: \text{Maximize generator operational and load shedding costs} \rightarrow \underset{\Delta P_D}{\text{Max}} \sum_{i=1}^{N_g} C_{g_i} * P_{g_i} + \sum_{k=1}^{N_d} C_{s_k} * L_{sk}$$
$$\text{Attacker and Operator Constraints} \rightarrow s.t.(2)-(7),(9)\ -(13)$$

$$\text{Optimality Feasibility Constraints} \rightarrow \begin{cases} -\vartheta_l - \underline{\mathrm{A}}_l + \overline{\mathrm{A}}_l = 0 \\ C_{g_i} - \lambda + \left(SF.KP_i\right)^T.\vartheta - \underline{B}_i + \overline{\mathrm{B}}_i = 0 \\ C_{s_k} - \lambda + \left(SF.KD_k\right)^T.\vartheta - \underline{\Gamma}_k + \overline{\Gamma}_k = 0 \end{cases} \tag{14}$$

$$\text{Non} - \text{negativity Constraints} \rightarrow \underline{\mathrm{A}}_l, \overline{\mathrm{A}}_l, \underline{\mathrm{B}}_i, \overline{\mathrm{B}}_i, \underline{\Gamma}_k, \overline{\Gamma}_k \geq 0 \tag{15}$$

$$\text{Linearized Complementary Slackness Condition} \rightarrow \begin{cases} \begin{cases} \underline{\mathrm{A}}_l \leq M\omega_{\underline{\mathrm{A}},l} \\ P_{Ll} + P_{Ll}^{max} \leq M(1-\omega_{\underline{\mathrm{A}},l}) \\ \overline{\mathrm{A}}_l \leq M\omega_{\overline{\mathrm{A}},l} \\ P_{Ll}^{max} - P_{Ll} \leq M(1-\omega_{\overline{\mathrm{A}},l}) \\ \omega_{\underline{\mathrm{A}},l} + \omega_{\overline{\mathrm{A}},l} \leq 1 \end{cases} \\ \begin{cases} \underline{\mathrm{B}}_i \leq M\omega_{\underline{\mathrm{B}},i} \\ P_{g_i} - P_{\underline{g}i}^{min} \leq M(1-\omega_{\underline{\mathrm{B}},i}) \\ \overline{\mathrm{B}}_i \leq M\omega_{\overline{\mathrm{B}},i} \\ P_{g_i}^{max} - P_{g_i} \leq M(1-\omega_{\overline{\mathrm{B}},i}) \\ \omega_{\underline{\mathrm{B}},i} + \omega_{\overline{\mathrm{B}},i} \leq 1 \end{cases} \\ \begin{cases} \underline{\Gamma}_k \leq M\omega_{\underline{\Gamma},k} \\ L_{sk} \leq M(1-\omega_{\underline{\Gamma},k}) \\ \overline{\Gamma}_k \leq M\omega_{\overline{\Gamma},k} \\ P_{Dk} + \Delta P_{Dk} - L_{sk} \leq M(1-\omega_{\overline{\Gamma},k}) \\ \omega_{\underline{\Gamma},k} + \omega_{\overline{\Gamma},k} \leq 1 \end{cases} \end{cases} \tag{16}$$

$$\omega_{\underline{\mathrm{A}},l}, \omega_{\overline{\mathrm{A}},l}, \omega_{\underline{\mathrm{B}},i}, \omega_{\overline{\mathrm{B}},i}, \omega_{\underline{\Gamma},k}, \omega_{\overline{\Gamma},k} \epsilon \{0,1\} \tag{17}$$

(9) to (13) are primal feasibility constraints, (14) to (17) are called as KKT necessary optimality feasibility constraints, (15) and (17) are non-negativity constraints and (16) are linearized expressions of complementary slackness conditions. The conversion of BPP to single-level MILPP using KKT conditions is explained briefly in Appendix-A1.

Solving the single-level MILPP comprising of (1)-(7), (9)-(13) and (14)-(17) equations, results in the most damaging LRAV ($\boldsymbol{\Delta P_D}$ *and* $\boldsymbol{\Delta P_L}$), generation power dispatches ($\boldsymbol{P_g}$), load curtailment ($\boldsymbol{L_s}$), line power flows ($\boldsymbol{P_L}$), auxiliary

binary variables, Lagrange multipliers and total operating cost. Objective function of attacker and operator is total operating cost which is sum of power generation and load shedding costs. Economic loss is nothing but the extra operational cost incurred due to LRA than the operational cost without LRA.

$$\text{Economic loss} = \text{Total operational cost due to LRA} - \text{Total operational cost without LRA}$$

The average economic loss is the ratio of sum of economic losses of all $R$ to maximum number of resources, $R_{max}$, represented in equation (18)

$$Average\ Economic\ loss = \frac{Economic\ loss_{R=1} + Economic\ loss_{R=2} + Economic\ loss_{R=3} + \cdots + Economic\ loss_{R=51}}{R_{max}} \tag{18}$$

## Defensive Methodology

Attacker always targets to maximize load shedding for creating lot of economic loss with the resources he/she has. Operator/Defender may be incapable to counter-attack to any intrusion. Hence it is recommended to safeguard the system by defending an attack. Cyber-defense is one of the better opportunities for cyber-security of any application in information processing. Cyber-defense must be provided with optimal less number of protection resources to safeguard the system such that the attacker cannot intrude into the system. Examples of cyber-defense can be frequent upgrading of firewalls, communication protocols and Intrusion Detection System (IDS). Optimal defense must be such that no random LRAV would be successful. Practically, it is not economic to protect every measurement device. Even if it is economic friendly, at such times, may any IDS can fail to operate or an LRAV intruded may not be detectable by existing log files. So it is better to select redundant critical measurements' that protect the complete system. LRAV can be framed by either with critical or non-critical measurements. If critical measurements are protected, they won't allow malicious values to enter into that measurement, this make the attackers fail to create a successful LRAV. But all critical units cannot be attacked and all critical units cannot be defended too. So, certain framework is to be followed to find optimal attack from possible attacking set and optimal defense from possible defending set. Furthermore, from each set an optimal attack-defense strategy must be found considering both attacking and defender resources. An optimal attack-defense strategy may not be a single strategy from attacker and defender sets. It can also be combination of some or all probabilities in their respective sets.

Fig. 2 shows the complete outline to find optimal attack-defense strategy against LRAs in which power systems network layer has generators, loads, their buses, lines and their measuring units. However, the measurement layer shows the enlarged view of units in network layer. Security layer has IEDs and firewalls to safeguard the system against attacks. Security layer communicates with Control Centre through Internet WAN where operator takes decisions at the control center. Decisions are sent to the cloud of ISO/RTO Market. In Fig. 2, it is also shown mixed probabilities of optimal attack-defense strategy are found by playing a static-zero-sum game of all considered strategies. Black-Hat Man's (attacker) attacking and operators defending signals are represented by red and blue lines respectively in Fig. 2.

In literature, critical measurements are selected based on entropic degree of the bus [19]. Entropic degree of a bus deals with the betweenness of the vertices (buses) and connectivity of vertices with edges (lines). It is obvious that a bus can be critical/weak if more power is injected or drawn through it (many lines are connected to it) and a line can be critical if more power flow happens through it. So, if more edges (lines) are connected to a vertex (bus) i.e., it has more betweenness, then that bus can be treated as critical one. The entropic degree of a bus $i$ is given by equation (19) [2]:

$$e_i = 1 - \sum_j w_{ij} * \log(w_{ij}) * \sum_j \tau_{ij} \tag{19}$$

where $j$ is set of to-buses if $i$ is acting as from bus and $w_{ij}$, the normalized weight of an edge represented in terms of electric betweeness of a line, $\tau_{ij}$ is equation (20)

$$\begin{aligned} w_{ij} &= \frac{\tau_{ij}}{\sum_j \tau_{ij}}\ where\ \tau_{ij} = \max(\tau^p(l), \tau^n(l))\ \forall\ l\ \epsilon\ L \\ \tau^p(l) &= \sum_{g \epsilon N_g} \sum_{k \epsilon N_d} C_g^k * f_l^{gk}, if\ f_l^{gk} > 0 \\ \tau^n(l) &= \sum_{g \epsilon N_g} \sum_{k \epsilon N_d} C_g^k * f_l^{gk}, if\ f_l^{gk} < 0 \\ and\ C_g^k &= min_{l \epsilon L} \frac{P_l^{max}}{f_l^{gk}}; f_l^{gk}\ is\ PTDF\ martix \end{aligned} \tag{20}$$

Entropic degree can state that which bus can be weaker based on the connectivity of number of lines to that bus. Entropic degree of a bus may not change with respect to load variations as it is highly dependent on power flow capacity of a line, $P_l^{max}$. So, critical measurement selection based on entropic degree of a bus may not be practical if load variations are considered.

Critical measuring units are also being selected based on higher operating points of the system. Basically, LRAV is

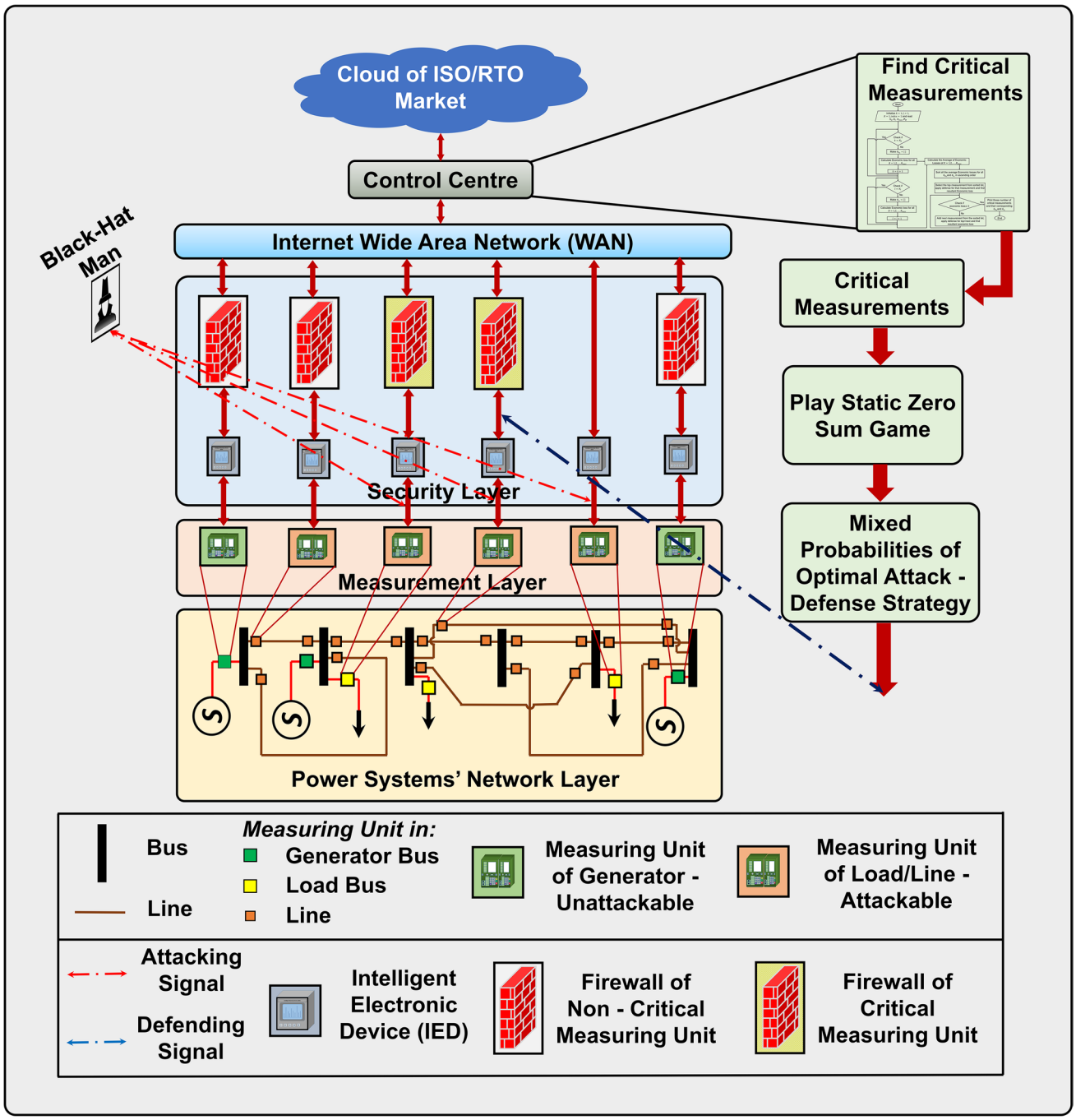


**Fig. 2** Layout to obtain probabilities of optimal attack-defense strategy

successful, if $\sum_{k=1}^{N_d} \Delta P_{Dk} = 0$. If any $\Delta P_{Dk}$'s intrusion into the system is unsuccessful means LRAV is detectable by the system operator. Also from equation (4), $\Delta P_{D_k}$ is proportional to $P_{D_k}$. So, buses or lines which are operating at high level may have the chance to get attacked with higher values. If those measurement units are defended, then the probability of defending the system is high. Hence those units which are operating at critical points can be considered as critical measurements. In reference [18], it is also considered that the buses operating at high loads and lines operating near to transmission line capacities are taken as critical units. But the main disadvantage of that consideration is that it would be applicable if the number of attack resources, $R$ is constant or if the load is constant which is not practical all time. Attacker attacks some units and defender may defend the same units or the other. It is also an unknown for

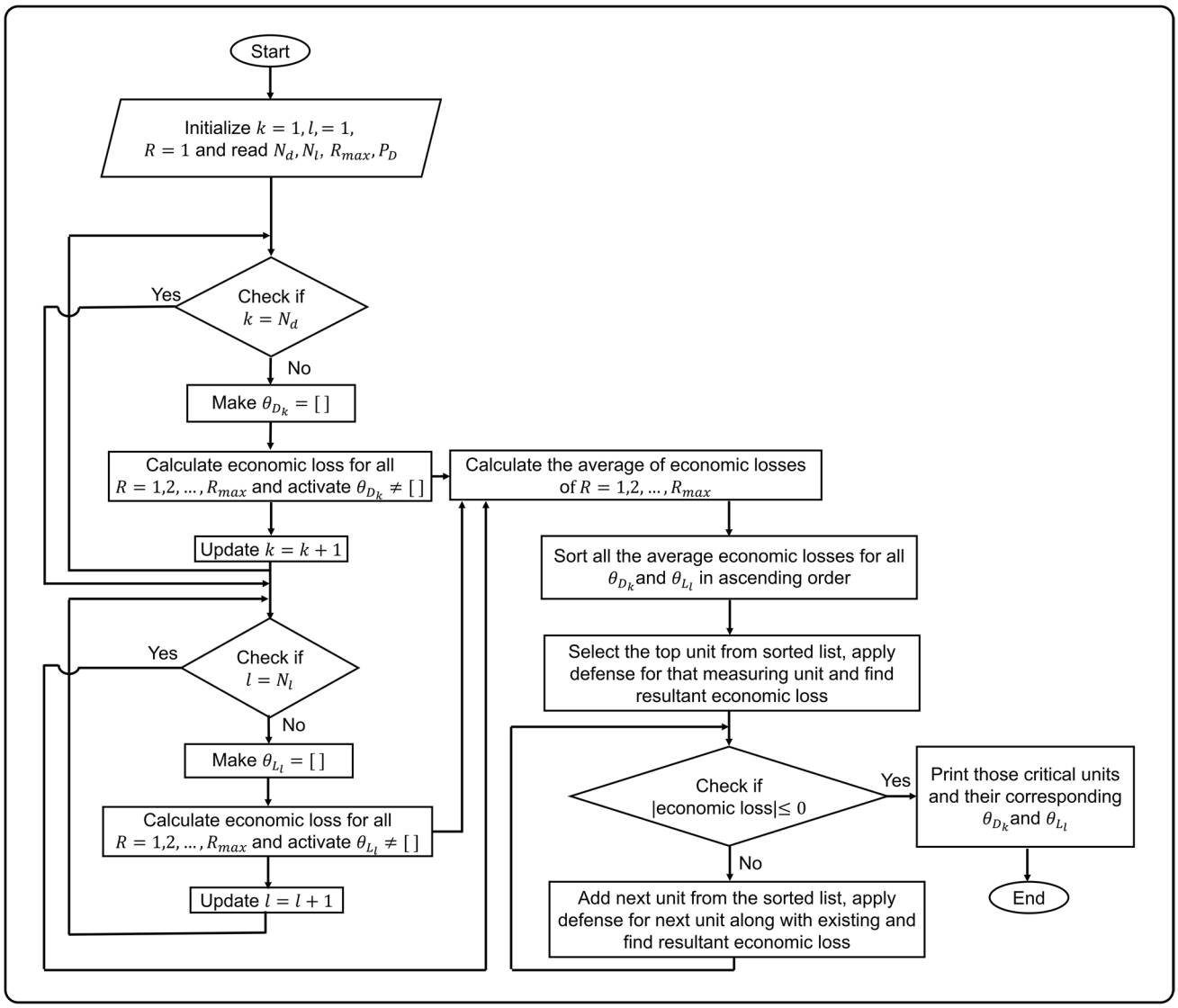


**Fig. 3** Flowchart for Selection of Critical Units

a defender that what value of $R$ is attacker's knowledge. In cyber-defense, attacker a n d defender are non-cooperative. So, a certain procedure must be framed to find the critical measurements and their number subject to considering all attack resour ce s and at an y loading conditions. In this article a procedure is developed to find the critical measurements and their number of a test system.

## Procedure to Select Optimal Critical Measuring Units

In real-time market or look-a-head electrical market, load is estimated/forecasted prior, it is assumed that $P_{D_k}$ is already known or approximately same as actual $P_{D_k}$ at one time step and let us also assume that for the next time step $P_{D_k}$ can get varied which is also approximately known for both attacker and operator.

The flowchart to select the critical units is given in Fig. 3. where $k = 1, 2, \ldots, N_d$, $l = 1, 2, \ldots, N_l$ and $R_{max}$ be the total number of attack resources, $(N_d + 2 * N_l)$. The developed algorithm to find critical measuring units is given in Step-1 to Step-13, as follows:

Step-1: Start.
Step-2: Initialize $k = 1, l = 1, R = 1$ and read $N_d$, $N_l$ *and* $\boldsymbol{P_D}$.
Step-3: For $k$, find the economic loss by making $\theta_{D_k} = []$, i.e., removing $\theta_{D_k}$ in BPP to find most damaging LRAV for all resources $R = 1, 2, \ldots, R_{max}$. Also calculate economic losses for all $R$ w.r.t. defense against $k$.

Step-4: Update $k$=$k$+$1$. Repeat Step-3, until $k = N_d$, else go to Step-5.
Step-5: For $l$, find the economic loss for each $l$ by making $\theta_{L_l} = []$ i.e., removing $\theta_{L_l}$ in BPP of most damaging LRAV for all resources $R = 1, 2, \ldots, R_{max}$. Also calculate economic losses for all $R$ w.r.t. the defense provided to $l$.
Step-6: Update $l$=$l$+$1$. Repeat Step-5, until $l = N_l$, then go to Step-7.
Step-7: Now calculate the average economic loss by considering one defense ($k$ *or* $l$) and all $R$. Hence, the total number of average economic losses be $k + l$.
Step-8: Sort all $k + l$ average economic losses in ascending order.
Step-9: Select the top measurement from the sorted list. Apply defense for that measurement (either $k$ *or* $l$) and then find the average economic loss w.r.t. that $k$ *or* $l$.
Step-10: Check if the absolute of average economic loss is approximately equal to zero. If yes go to Step-12, else go to Step-11.
Step-11: Add next top measurement to the existing top measurement and apply defense for all of them. Then find the average economic loss. Go to Step-10.
Step-12: Print the number of critical measurements and their respective $k$ *or* $l$.
Step-13: Stop.

This algorithm assumes defense as the driving parameter. But, it should be mentioned that if a unit is defended and if it results in less economic loss comparatively than other units then that unit is more capable of attacking. Means a unit which is highly attackable is the unit that is highly defendable. If the average economic loss of all attack resources (while defending each unit separately), are sorted in ascending order then that top unit in the list is highly capable to attack and highly capable to defend too.

As mentioned earlier, it is assumed that the load demand, $P_{D_k}$ is considered as known for both attacker and defender. In this procedure, it is assumed that the cost of attacking or defending a load bus meter or line meter is unity i.e., equal significance is given to all meters and the degree of difficulty of attacking or defending every unit is not considered.

Budget allocation for optimal protection problem can be solved by probabilistic or deterministic ways. To allocate budget, participation probability of specific attack and specific defense must be known. In addition to, attackers may not have access to all units and defenders also can't provide protection to all critical units. Attacker may have his/her own strategy and defender can have his/her strategy. But an optimal protection strategy is that for every attack strategy there should be a defense strategy which creates a direct/indirect interaction between them. These interactions can be framed as a game having two players, attacker and defender. Game-theoretic approach can give better solution for optimal protection against LRAV. Game-theoretic study for optimal protection involves terminology like Players, Action space, Action Strategies and Utility function which are explained as follows:

- Players: The players to find optimal attack-defense strategy's probabilities are attacker,$A$ and defender, $D$.
- Action space: Attacker may not have access to all critical units and defender also can't afford to protect all critical units. Each player in the game have their own set of accessibilities and limitations.

  Let $c_m$ be the number of critical units. Suppose that attacker has access to $n_A$ measuring units among $c_m$ and defender is able to protect $n_D$ units among $c_m$.
  Then the maximum number of possible strategies (each strategy has different combination of resources) for attacker and defender be $N_{S_A} = \binom{c_m}{n_A}$ and $N_{S_D} = \binom{c_m}{n_D}$ respectively.
  Hence the attacker's ($A$) action space and defender's ($D$) action space are $A\_A_{space}$ and $D\_A_{space}$. Let $A_{s_a}$ be the $a^{th}$ attack strategy and $D_{s_d}$ be the $d^{th}$ defense strategy where $a = 1, 2, \ldots, N_{S_A}$ and $d = 1, 2, \ldots, N_{S_D}$.

- Action Strategies: Attacker's action space, $A\_A_{space} = \{A_{s_1}, A_{s_2}, \ldots, A_{s_a}, \ldots, A_{s_{N_{S_A}}}\}$ and $D\_A_{space} = \{D_{s_1}, D_{s_2}, \ldots, D_{s_d}, \ldots, D_{s_{N_{S_D}}}\}$ is defender's action space.
- Type of game: Attacker may not know the plan of defender's strategy and defender may not have any knowledge about attacker's plan. Players in this game are non-cooperative as one player can't know others' strategies. It is also to be mentioned that for every attack strategy there would be a defense strategy or both can be applied simultaneously as there is no possibility of knowing others knowledge. Hence this game can be framed as a static game. This game can also be treated as a zero-sum static game because the cost of attacker's resources on attacking and the cost of defending resources for defense are considered as unity. Defender's utility is negation of attacker's utility.
- Utility Function: Utility function for obtaining optimal attack-defense strategy is generally the objective function of single-level MILPP. In this article, the utility is considered as economic loss. Utility function of attacker,$U_A$ is to maximize the minimum utility (economic loss) and utility function of defender,$U_D$ is to minimize the maximum utility.

  Utility function of attacker is economic loss. Prior to find economic loss, total operational cost with LRAV

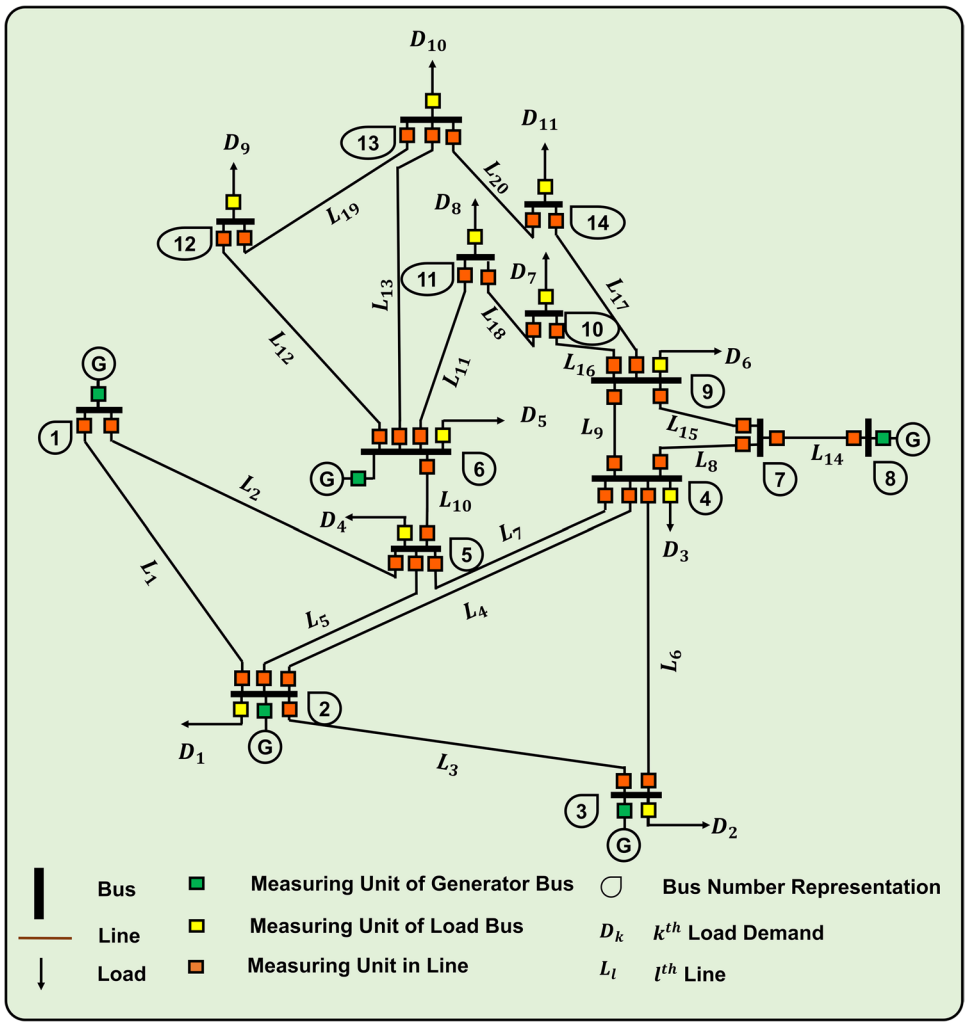


**Fig. 4** Line Diagram of modified IEEE-14 bus test system

must be known. Utility function of attacker is given by equation (21) as follows:

$$U_A = f(A,D)_{with\ LRA} - f(A,D)_{without\ LRA} \tag{21}$$

Similarly, the utility function of defender is negation of economic loss as the game is a static zero-sum game (Cost for attacking and defending resources is treated as unity):

$$U_D = f(A,D)_{without\ LRA} - f(A,D)_{with\ LRA} \tag{22}$$

Hence the objective of attacker is to maximize the minimum of $U_A$ and the objective of defender is minimize the maximum of $U_D$. Hence the optimal objective function is as follows:

$$U = max_A min_D\left(U_A\right) = min_D max_A\left(U_D\right) \tag{23}$$

To obtain an optimal attack-defense strategy, equation (23) is to be satisfied and such equilibrium point must be found such that attacker and defender can't move away from that equilibrium. Such equilibrium point in game theory is called Nash equilibrium.

- Nash equilibrium: To get an optimal attack and defense set among sets (action space) of $A\_A_{space}$ and $D\_A_{space}$, a static zero sum game is played for an equilibrium, also called Nash equilibrium. Nash equilibrium is a state where the players moving from that state may not have increase in incentives (profits).

Nash equilibrium results in either pure attack-defense strategy or mixed attack-defense strategies. A pure strategy has only one optimal attack strategy with 100% probability and also one optimal defense strategy with 100% probability. However, a mixed optimal strategy has multiple attack strategies with different probabilities and multiple defense strategies with different probabilities where the sum of attack strategic probabilities is one and sum of defense strategic probabilities is one. Let the probability of an attack strategy is $P_{A\_S_a}$ and the probability of a defense strategy is $P_{D\_S_d}$.

**Table 1** Single-level MILPP parameters

| Test System | Modified IEEE 14-bus system |
|---|---|
| Variables Number | 325 |
| Equalities' Number | 78 |
| Inequalities' Number | 492 |
| Integer Constrained Variables | 165 |
| Software Used | CPLEX interfaced with MATLAB |

## Case Studies

This article mainly demonstrates with three analyses where first one is to find maximum economic loss by most damaging LRAV of modified IEEE-14 bus test system. Second study shows a procedure to obtain critical units and validated by applying on three loading scenarios. Third aspect of this study finds the probabilities of optimal attack-defense strategy. First subsection of this section deals with the solution of single-level MILPP using CPLEX interfaced with MATLAB software to fin d the most damaging LRAV of a modified IEEE-14 bus test system [8]. It is considered that attacker has knowledge of actual load changes and let the number of attack resources be $R = 51$. However, second subsection in this section depicts the inability of entropic de gree and high operating points for finding critical measurements at load changing times. Thereafter, selection of critical units is provided in three loading conditions namely standard, high and low respectively. Further, discussions are carried out to find probabilities of optimal attack-defense strategies in all three scenarios by playing a static zero-sum game using Gambit software [14].

Data of IEEE-14 bus test system is obtained from MATPOWER software [25]. The test system, modified IEEE-14 bus test system has 20 lines and 14 buses among which 11 are load buses, 1 is zero injection bus and 5 are generator buses as shown in Fig. 4. In Fig. 4, it is also shown that each generator bus has one measuring unit (green color), one measuring unit for a zero-injection bus (orange color), every load bus has one unit (yellow color), and each line has two units (orange color) which make a total of (5+1+11+2*20) = 57 units.

**Table 2** Most damaging LRAV of a modified IEEE-14 bus system at $R = 51$

| $\Delta P_{D_k}$, MW | | $\Delta P_{L_l}$, MW | | | |
|---|---|---|---|---|---|
| **Bus Number** | **Attack Vector** | **Line Number** | **Attack Vector** | **Line Number** | **Attack Vector** |
| 2 | -10.85 | 1 | -7.7867 & 7.7867 | 11 | -1.9548 & 1.9548 |
| 3 | -47.1 | 2 | 7.7867 & -7.7867 | 12 | 9.4971 & -9.4971 |
| 4 | -23.9 | 3 | -17.8679 & 17.8679 | 13 | 28.5416 & -28.5416 |
| 5 | -3.8 | 4 | 8.2933 & -8.2933 | 14 | 0 & 0 |
| 6 | 5.6 | 5 | 12.6379 & -12.6379 | 15 | 27.7632 & -27.7632 |
| 9 | 11.4 | 6 | 29.2321 & -29.2321 | 16 | 8.2048 & -8.2048 |
| 10 | 4.5 | 7 | 17.4593 & -17.4593 | 17 | 24.3612 & -24.3612 |
| 11 | 1.75 | 8 | 27.7632 & -27.7632 | 18 | 3.7048 & -3.7048 |
| 12 | 3.05 | 9 | 16.2029 & -16.2029 | 19 | 6.4471 & -6.4471 |
| 13 | 31.9 | 10 | 41.6840 & -41.6840 | 20 | 3.0888 & -3.0888 |
| 14 | 27.45 | | | | |

**Table 3** Power Dispatches, Load Shed, Total Operational Cost and Economic Loss due to LRAV of $R = 0, R = 20, R = 35$ and $R = 51$

| Attacker Resources, $\boldsymbol{R}$ | | 0 | 20 | 35 | 51 |
|---|---|---|---|---|---|
| Power Dispatches, MW | $\boldsymbol{P}_{g_1}$ | 201.1439 | 225.8260 | 193.6778 | 201.5293 |
| | $\boldsymbol{P}_{g_2}$ | 50 | 0 | 39.4569 | 29.8950 |
| | $\boldsymbol{P}_{g_3}$ | 30 | 30 | 12.7724 | 0 |
| | $\boldsymbol{P}_{g_6}$ | 43.8394 | 46.0191 | 50 | 50 |
| | $\boldsymbol{P}_{g_8}$ | 20 | 20 | 13.2765 | 6.6998 |
| Load Shed w.r.t. bus, MW | | 0 | 22.8567 (Bus-2) 4.5981 (Bus-13) | 40.1164 (Bus-13) | 1.1117 (Bus-6) 9.1500 (Bus-12) 50.9142 (Bus-13) |
| Total Load Shed, MW | | 0 | 27.4548 | 40.1164 | 61.1759 |
| Total Operational Cost, $/MWh | | 10046.52 | 11462.96 | 12544.74 | 13779.52 |
| Economic Loss, $/MWh | | 0 | 1416.4 | 2498.2 | 3733 |

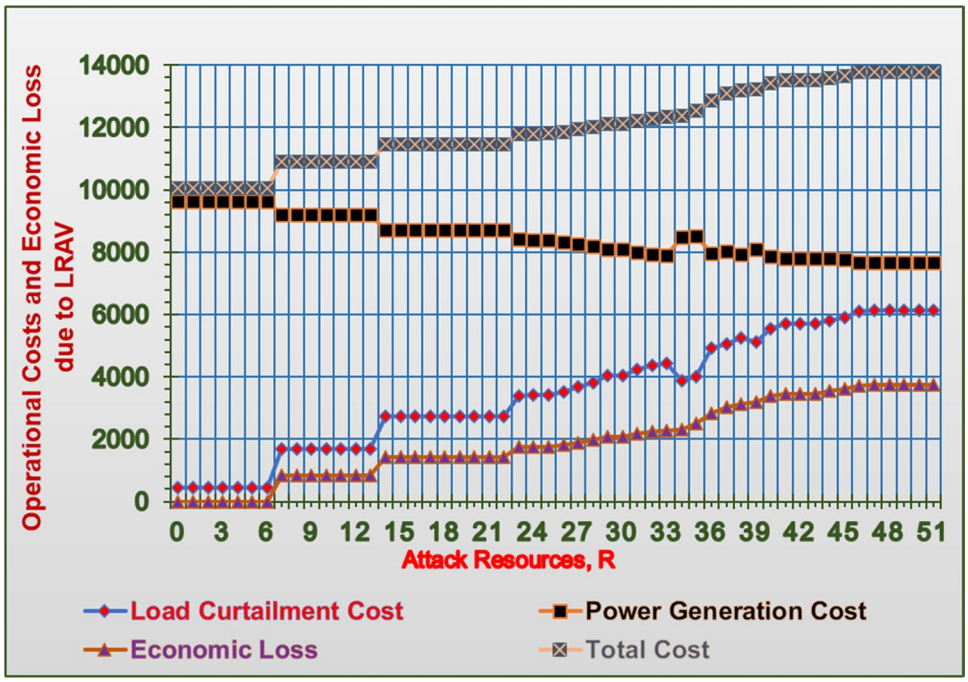


**Fig. 5** Operational Costs and Economic Loss due to LRAV versus Attack Resources,$R$ of modified IEEE-14 bus system

## Most Damaging Successful LRAV:

For each load bus, there exist each measurement device and for each line, two measuring units are on either sides. Hence the maximum number of attackable resources be (11+(2*20)) = 51. In this article, the cost of load shedding is considered as $c_s = 100\$/MWh$ and attacker's load redistribution limit, $\tau = \pm 50\%$. Single-level MILPP parameters of modified IEEE-14 bus test system to obtain maximum economic loss by most damaging LRAV are shown in Table 1 [23].

Most damaging LRAV at standard loading conditions in case of $R = 0$ results in $\Delta P_{D_k} = 0,\ \forall\ k$ and $\Delta P_{L_l} = 0,\ \forall\ l$. But if $R = 51$, i.e., the attacker has access to all attackable resources then the most damaging LRAV is shown in Table 2.

Power generation dispatches, bus wise load shedding, total load shed, power generation cost, load curtailment cost and finally economic loss if $R = 0, R = 20, R = 35$ and $R = 51$ are given in Table 3. It can be clearly observed that as if $R$ is increased then economic loss is also increased which is given in Table 3.

Economic loss is the extra cost that should be incurred when an undetectable most damaging LRAV is intruded, which is nothing but economic loss = total cost at $R \geq 0$ – total cost at $R = 0$, where total operational cost is power generation and load shedding cost. Maximum economic loss of a modified IEEE-14 bus system at $R = 51$ is 3733$/MWh.

Fig. 5 shows a graph which is plotted considering load curtailment cost, power generation cost, total operating cost and economic loss versus attack resources, $R = \{0, 1, \ldots, 51\}$. As power generation and load shedding costs are considered as objective function given in equation (1), at some resources of $R = 34, R = 35$ and $R = 39$, power generation cost is dominating than load shedding cost whereas at remaining attack resources, load shedding cost is dominating than power generation cost. This issue exists if the objective function of BPP is total operating cost and doesn't exist if the objective is only load shedding. So, in this aspect the driving parameter can be economic loss but not load shedding.

## Selection of Critical Measuring Units of a Modified IEEE-14 Bus System

For an optimal attack or optimal defense, it is better to know the critical (weak) units of the test system. Researchers, basically selected the critical units based on entropic degree or higher operating nodes and critical lines but those methods are deficient for any number of attack resources or at load varying conditions [18, 19].

Selection of critical units can be done based on entropic degree. Based on equations (19) and (20), the bus entropic degrees of a modified IEEE-14 bus test system are given in Table 4.

From Table 4, entropic degree of bus-2 is high, which shows that the connectivity of bus-2 to various edges (lines) is high. But in case of most damaging LRAV, bus-3 is given more importance than bus-2. Even, if bus-2 is defended then average economic loss w.r.t. all resources resulted is 611.16MW and if bus-3 is defended, then average economic loss w.r.t. all $R$ is 127.66MW. From this it can be depicted that entropic degree may not be able to provide the best

**Table 4** Bus entropic degrees of modified IEEE-14 bus test system

| Bus Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Load, MW | 0 | 21.7 | 94.2 | 47.8 | 7.6 | 11.2 | 0 | 0 | 29.5 | 9 | 3.5 | 6.1 | 13.5 | 14.9 |
| Entropic Degree | 2174.5 | 2931.9 | 858.1 | 2666.9 | 1153.4 | 2574.4 | 2338.4 | 0 | 1680.8 | 459.4 | 0 | 238.5 | 384.8 | 0 |
| Degree Ranking | V | I | VIII | II | VII | III | IV | XII | VI | IX | XII | XI | X | XII |

critical measurements all time. The other disadvantage is entropic degree of a bus is dependent on power flow capacities and independent on load variations.

From literature, the buses and lines operating at higher points are considered as critical measuring units. But if the load changes, the number of critical units can also change [18].

In this section, a developed procedure to select the number of critical units is applied on the modified IEEE-14 bus test system and compared with other two methods. Consider the three loading scenarios, one is standard test system loading and the other two are high loading and low loading conditions.

### Scenario-1: Standard Loading Condition of Modified IEEE-14 Bus Test System

The standard load data of IEEE-14 bus test system obtained from MATPOWER is given in Table 5 and let the maximum power flow capacities be 160MW for line-1 and 60MW for remaining 19 lines [23].

The maximum number of attack resources of the 14 bus test system is $R_{max} = 11 + 2 * 20 \Rightarrow R_{max} = 51$ and the maximum number of defendable resources be $11 + 20 = 31$ as safeguarding one measuring unit of a line is sufficient. Here $k = \{1, 2, \ldots, 11\}, l = \{1, 2, \ldots., 20\}$ and $R = \{1, 2, \ldots, 51\}$.

Based on procedure presented in third section, if one unit is defended considering all 50 (one used for defense) possibilities of attack resources, then the average economic losses of 31 units is given in Table 6.

After sorting is done, based on Fig. 2. Select the top measuring units which can have more capacity to attack or to defend. As mentioned in third section the unit which gives less average economic loss when defended is obviously the most vulnerable unit.

Now consider the top unit in the sorted order given in Table 6, $P_{L_6}$, and when it is defended it results in average economic loss w.r.t. all $R$(s), 127.6562MW. By considering only $P_{L_6}$, average economic loss is not zero and then consider the next one from top i.e., $P_{D_2}$. If $P_{L_6}$ and $P_{D_2}$ are both safeguarded, then the average economic loss is 70.7955MW which is even not less than or equal to zero. Repeat the process again and select $P_{L_3}$ in the next step where the economic loss of defending $P_{L_6}, P_{D_2}$ and $P_{L_3}$ is even 70.7955MW. So safeguarding $P_{L_3}$ has not provided any advantage than $P_{L_6}$ and $P_{D_2}$. However in case of attacking, $P_{L_3}$ plays a crucial role from $R = \{7, 8, \ldots, 36\}$ whereas from $R = \{37, 38, \ldots, 51\}$, the attacking impact of $P_{L_3}$ is less comparatively. So from attacker's view, $P_{L_3}$ can be treated as a critical unit. Now defending the next unit $P_{L_2}$ in addition to existing set ($P_{L_6}, P_{D_2}$ and $P_{L_3}$), then the absolute of average economic loss is 2.2367E-7 $\cong 0$. Hence in case of standard loading conditions of modified IEEE-14 bus test system, the

**Table 5** Standard load data of modified IEEE-14 bus test system

| Bus Number | 2 | 3 | 4 | 5 | 6 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Load, MW | 21.7 | 94.2 | 47.8 | 7.6 | 11.2 | 29.5 | 9 | 3.5 | 6.1 | 13.5 | 14.9 |

**Table 6** Average economic losses unsorted and sorted in ascending order while defending each measuring unit at standard loading conditions

| S. No. | Unsorted | | | Sorted in Ascending Order | |
|---|---|---|---|---|---|
| | Bus Number or Line number and Measurement unit Defended | | Average Economic loss w.r.t. all $R$ | Measurement unit Defended | Average Economic loss w.r.t. all $R$ |
| 1 | Bus-2 | $P_{D_1}$ | 611.1637422 | $P_{L_6}$ | 127.6562 |
| 2 | Bus-3 | $P_{D_2}$ | 132.1625192 | $P_{D_2}$ | 132.1625 |
| 3 | Bus-4 | $P_{D_3}$ | 610.9258262 | $P_{L_3}$ | 151.0537 |
| 4 | Bus-5 | $P_{D_4}$ | 877.1357525 | $P_{L_2}$ | 272.4504 |
| 5 | Bus-6 | $P_{D_5}$ | 892.1556554 | $P_{L_5}$ | 272.4504 |
| 6 | Bus-9 | $P_{D_6}$ | 905.597101 | $P_{L_1}$ | 272.4504 |
| 7 | Bus-10 | $P_{D_7}$ | 970.1407314 | $P_{L_4}$ | 435.979 |
| 8 | Bus-11 | $P_{D_8}$ | 970.6694866 | $P_{D_3}$ | 610.9258 |
| 9 | Bus-12 | $P_{D_9}$ | 967.4227919 | $P_{D_1}$ | 611.1637 |
| 10 | Bus-13 | $P_{D_{10}}$ | 962.7633407 | $P_{L_{10}}$ | 846.8893 |
| 11 | Bus-14 | $P_{D_{11}}$ | 966.1615724 | $P_{L_8}$ | 855.7738 |
| 12 | Line-1 | $P_{L_1}$ | 272.4504036 | $P_{L_{15}}$ | 870.9924 |
| 13 | Line-2 | $P_{L_2}$ | 272.4504017 | $P_{L_9}$ | 870.9924 |
| 14 | Line-3 | $P_{L_3}$ | 151.0536627 | $P_{D_4}$ | 877.1358 |
| 15 | Line-4 | $P_{L_4}$ | 435.9790158 | $P_{D_5}$ | 892.1557 |
| 16 | Line-5 | $P_{L_5}$ | 272.4504019 | $P_{D_6}$ | 905.5971 |
| 17 | Line-6 | $P_{L_6}$ | 127.6562406 | $P_{L_7}$ | 931.2359 |
| 18 | Line-7 | $P_{L_7}$ | 931.2359113 | $P_{L_{13}}$ | 956.5407 |
| 19 | Line-8 | $P_{L_8}$ | 855.7737836 | $P_{L_{12}}$ | 961.4617 |
| 20 | Line-9 | $P_{L_9}$ | 870.992377 | $P_{D_{10}}$ | 962.7633 |
| 21 | Line-10 | $P_{L_{10}}$ | 846.8893086 | $P_{L_{17}}$ | 965.099 |
| 22 | Line-11 | $P_{L_{11}}$ | 970.231284 | $P_{D_{11}}$ | 966.1616 |
| 23 | Line-12 | $P_{L_{12}}$ | 961.4617203 | $P_{D_9}$ | 967.4228 |
| 24 | Line-13 | $P_{L_{13}}$ | 956.54073 | $P_{L_{16}}$ | 969.8887 |
| 25 | Line-14 | $P_{L_{14}}$ | 971.7764965 | $P_{L_{19}}$ | 969.9724 |
| 26 | Line-15 | $P_{L_{15}}$ | 870.9923769 | $P_{D_7}$ | 970.1407 |
| 27 | Line-16 | $P_{L_{16}}$ | 969.888697 | $P_{L_{11}}$ | 970.2313 |
| 28 | Line-17 | $P_{L_{17}}$ | 965.0989966 | $P_{L_{20}}$ | 970.2726 |
| 29 | Line-18 | $P_{L_{18}}$ | 971.7635006 | $P_{D_8}$ | 970.6695 |
| 31 | Line-19 | $P_{L_{19}}$ | 969.9724343 | $P_{L_{18}}$ | 971.7635 |
| 31 | Line-20 | $P_{L_{20}}$ | 970.2725635 | $P_{L_{14}}$ | 971.7765 |

optimal number of critical measurements be 4 ($P_{L_6}, P_{D_2}, P_{L_3}$ and $P_{L_2}$). If for a known standard load, if these four measurements are completely attacked or completely defended, the economic loss resulted would be maximum and minimum respectively for any value of $R$, where $R = \{1, 2, \ldots, 51\}$. Fig. 6 also shows the diagrammatical representation of critical measuring units of modified IEEE-14 bus test system at standard loading conditions. Measuring unit of $L_6$ is marked with a blue colored star mark, which shows, that measuring unit is a critical unit. Four stars are represented with numbers marked as 1,2,3,4. From Fig. 6, star with 1 shows, that respective unit is top in sorted list (average economic loss w.r.t. all $R$(s) while defending critical unit of $L_6$ is minimum).

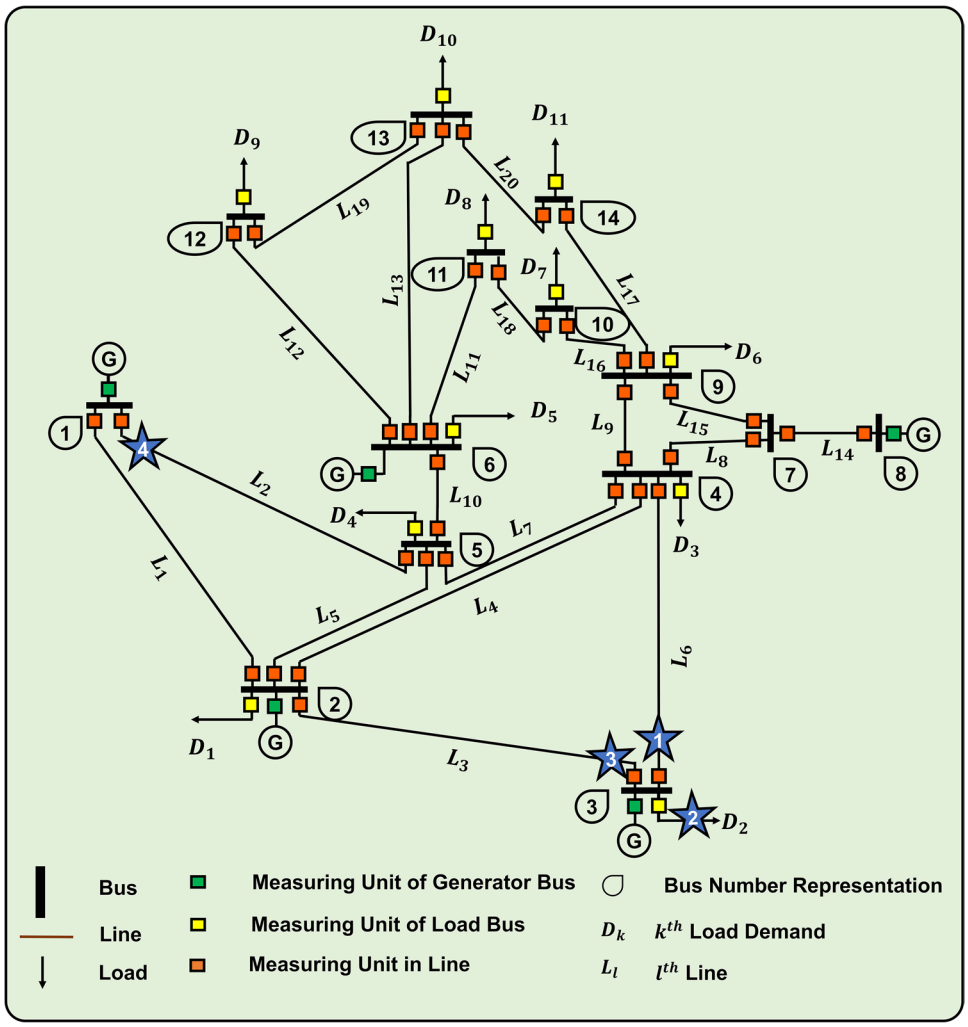


**Fig. 6** Critical measuring units of modified IEEE-14 bus test system at standard loading conditions

**Table 7** High loading condition of modified IEEE-14 bus test system

| Bus Number | 2 | 3 | 4 | 5 | 6 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Load, MW | 21.7 | 94.2 | 47.8 | 7.6 | 11.2 | 29.5 | 9 | 3.5 | 6.1 | **63.8** | **54.9** |

### Scenario-2: High Loading Condition of Modified IEEE-14 Bus Test System

Consider the load just higher than the standard loading of modified IEEE-14 bus test system where load at bus-13 is increased to 63.8MW and load at bus-14 is increased to 54.9MW as mentioned in Table 7 and let the maximum power flow capacities be 160MW for line-1, 70MW for line-2 and 60MW for remaining 18 lines [18].

Based on procedure presented in third section, if defense is provided to each unit individually for all attack resources, at one go, then the sorted average economic losses of 31 units is given in Table 8.

Based on the procedure developed, select the top unit in the sorted list and go on until economic loss is less than or equal to zero.

- Defending $P_{D_2}$, then |*average economic loss*| is 1192.8$/MWh,
- Defending $P_{D_2}$ and $P_{L_6}$, then |*average economic loss*| is 1162.0$/MWh,
- Defending $P_{D_2}$, $P_{L_6}$ and $P_{L_3}$, then |*average economic loss*| is 1162.0$/MWh,
- Defending $P_{D_2}$, $P_{L_6}$, $P_{L_3}$ and $P_{L_{13}}$, then |*average economic loss*| is 197.9386$/MWh,
- Defending $P_{D_2}$, $P_{L_6}$, $P_{L_3}$, $P_{L_{13}}$ and $P_{D_3}$, then |*average economic loss*| is 41.9726$/MWh,

**Table 8** Sorted average economic losses when defending each measuring unit at high loading conditions

| High Load Conditions | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Defended Measurement Unit | $P_{D_2}$ | $P_{L_6}$ | $P_{L_5}$ | $P_{L_{13}}$ | $P_{D_3}$ | $P_{D_1}$ | $P_{L_{12}}$ | $P_{D_{10}}$ | $P_{L_{19}}$ | $P_{L_4}$ | $P_{L_5}$ |
| Sorted Average Economic loss, $/MWh | 1192.793 | 1198.803 | 1214.086 | 1346.557 | 1378.486 | 1418.649 | 1436.894 | 1439.02 | 1456.379 | 1482.097 | 1500.283 |
| Defended Measurement Unit | $P_{L_2}$ | $P_{L_1}$ | $P_{L_{10}}$ | $P_{L_8}$ | $P_{L_9}$ | $P_{L_{15}}$ | $P_{D_{11}}$ | $P_{L_7}$ | $P_{L_{17}}$ | $P_{D_6}$ | $P_{D_5}$ |
| Sorted Average Economic loss, $/MWh | 1500.283 | 1500.283 | 1530.533 | 1560.195 | 1560.195 | 1560.195 | 1574.774 | 1589.327 | 1590.454 | 1704.672 | 1766.358 |
| Defended Measurement Unit | $P_{L_{14}}$ | $P_{D_4}$ | $P_{L_{18}}$ | $P_{L_{16}}$ | $P_{L_{11}}$ | $P_{D_7}$ | $P_{D_9}$ | $P_{D_8}$ | $P_{L_{14}}$ | | |
| Sorted Average Economic loss, $/MWh | 1769.409 | 1781.797 | 1803.179 | 1803.708 | 1806.504 | 1836.327 | 1853.666 | 1858.785 | 1862.382 | | |

- Defending $P_{D_2}$, $P_{L_6}$, $P_{L_3}$, $P_{L_{13}}$, $P_{D_3}$ and $P_{D_1}$, then |*average economic loss*| is 7.6831E-7$/MWh ≅ 0$/MWh.

Then the maximum number of critical units be 6 ($P_{D_2}$, $P_{L_6}$, $P_{L_3}$, $P_{L_{13}}$, $P_{D_3}$ and $P_{D_1}$) in case of high loading. In reference [18], the loads and lines operating at higher values are considered as critical units. There it is considered that, measuring units on bus-13 and bus-14 are critical measurements. But the average economic loss when defending units on bus-13 and bus-14 are 1439MW and 1574.8MW respectively which are not optimal to select them as critical measurements. Critical measuring units of the test system at high loading conditions are marked in Fig. 7.

### Scenario-3: Low Loading Condition of Modified IEEE-14 Bus Test System

Let us consider the load which is just lower than the standard load of IEEE-14 bus test system where load at bus-3 is reduced from 94.2MW to 64.2MW, given in Table 9. Let the maximum power flow capacities be 160MW for line-1 and 60MW for remaining 19 lines.

Based on procedure presented in third section , if defense is provided to each unit individually, considering all attack resources at one go, then the sorted average economic losses of 31 units is given in Table 10.

Based on the procedure developed, select the top measurement in the sorted list.

- Defending $P_{L_2}$, then |*average economic loss*| is 19.2699$/MWh,
- Defending $P_{L_2}$ and $P_{L_5}$, then |*average economic loss*| is 19.2944$/MWh,
- Defending $P_{L_2}$, $P_{L_5}$ and $P_{L_1}$, then |*average economic loss*| is 19.2904$/MWh,
- Defending $P_{L_2}$, $P_{L_5}$, $P_{L_1}$ and $P_{L_4}$, then |*average economic loss*| is 9.9780$/MWh,
- Defending $P_{L_2}$, $P_{L_5}$, $P_{L_1}$, $P_{L_4}$ and $P_{L_6}$, then |*average economic loss*| is 2.9425E-11$/MWh ≅ 0$/MWh.

Defending $P_{L_2}$ or $P_{L_5}$ or $P_{L_1}$, the |average economic loss| is 19.3$/MWh. So selecting one measurement among them is sufficient. Then the maximum number of critical measurements be 3 ($P_{L_2}$, $P_{L_4}$ and $P_{L_6}$) in case of low loading condition. Fig. 8 highlights the critical units if the test system operates in Scenario-3 i.e., low loading conditions.

From Figs. 6, 7 and 8, it can be inferred that critical units vary with all number of attack resources considered and load variations happened.

As the load demand in three scenarios is considered varying, simulation time for one set of attack-resources provided with one-set of defense resources in three scenarios is 2.20s,

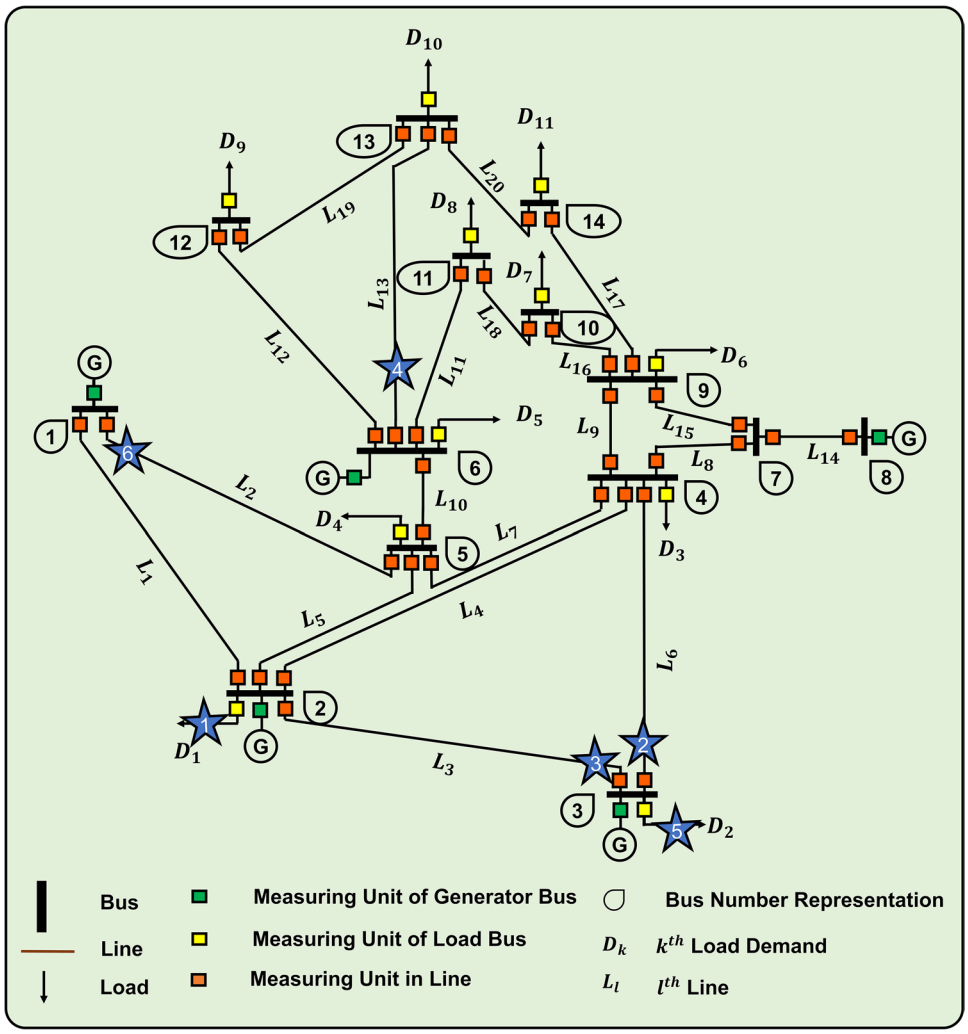


**Fig. 7** Critical measuring units of modified IEEE-14 bus test system at high loading conditions

**Table 9** Low loading demand of modified IEEE-14 bus test system

| Bus Number | 2 | 3 | 4 | 5 | 6 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Load, MW | 21.7 | **64.2** | 47.8 | 7.6 | 11.2 | 29.5 | 9 | 3.5 | 6.1 | 13.5 | 14.9 |

2.37s and 1.04s. However, execution time of multiple sets of attack resources with one set of defense resources is 83.13s (1.39 m), 195.91s (3.27 m) and 53.45s (0.89 m). Time taken to compute the solution of BPP with all attack resources and all defense resources in three load changing conditions is 1115.42s (18.59m), 5030.47s (83.84m) and 574.9s (9.5817m). Computational time (in seconds and minutes) in all three scenarios is given in Table 11.

## Optimal Attack-Defense Strategy by Static-Zero Sum Game Theory:

Providing defense is protecting redundant critical measurement devices in the system such that any random LRAV could become unsuccessful i.e. the attacker can't intrude into the system. Perhaps, malicious data which can even enter into the system by means of non-critical units can't built successful LRAV and won't impact the system's vulnerability. Attacker won't have access to all resources and the defender too can't protect all, then where critical units of the network must be considered. As it can be depicted from section of "Selection of Critical Units", the critical units cannot be selected based on entropic degree of a bus or lines/loads operating at critical points. In this section, an optimal attack-defense strategy by using static zero-sum game theory is found at all the three loading scenarios considering optimal critical units.

**Table 10** Sorted average economic losses when defending each measuring unit at low loading conditions

| Low Loading Conditions | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Defended Measurement Unit | $P_{L_2}$ | $P_{L_5}$ | $P_{L_1}$ | $P_{L_4}$ | $P_{L_6}$ | $P_{D_2}$ | $P_{L_3}$ | $P_{D_1}$ | $P_{L_{10}}$ | $P_{D_3}$ | $P_{L_8}$ |
| Sorted Average Economic loss, $/MWh | 19.26985 | 19.29564 | 19.2967 | 71.39181 | 106.6713 | 111.2171 | 126.1233 | 138.3721 | 154.7766 | 166.9013 | 176.2052 |
| Defended Measurement Unit | $P_{L_{15}}$ | $P_{L_9}$ | $P_{L_7}$ | $P_{D_5}$ | $P_{D_4}$ | $P_{D_6}$ | $P_{L_{13}}$ | $P_{L_{12}}$ | $P_{D_{10}}$ | $P_{L_{17}}$ | $P_{D_{11}}$ |
| Sorted Average Economic loss, $/MWh | 176.2052 | 176.2052 | 176.7906 | 181.1438 | 188.1605 | 192.2286 | 195.9092 | 199.2969 | 199.7672 | 201.6938 | 202.3969 |
| Defended Measurement Unit | $P_{D_9}$ | $P_{L_{19}}$ | $P_{L_{20}}$ | $P_{L_{16}}$ | $P_{L_{11}}$ | $P_{D_7}$ | $P_{D_8}$ | $P_{L_{18}}$ | $P_{L_{14}}$ | | |
| Sorted Average Economic loss, $/MWh | 202.6881 | 204.5914 | 204.7301 | 204.9027 | 204.9723 | 205.0838 | 205.3701 | 205.7813 | 205.8653 | | |

### Optimal Attack-Defense Strategy in Scenario-1- Standard Loading Condition

The optimal number of critical units is 4 ($P_{L_6}, P_{D_2}, P_{L_3}$ and $P_{L_2}$) in case of standard loading conditions of modified IEEE-14 bus test system. Let attacker has access to 2 critical measurements among total four and defender can protect only one among four, then $N_{S_A} = \binom{4}{2} \Rightarrow N_{S_A} = 6$ and $N_{S_D} = \binom{4}{1} \Rightarrow N_{S_D} = 4$. Except defended critical units and non-attacked critical units, all non-critical units are attackable i.e., among 11 load and 40-line flow measurements, if one critical measurement is non-attacked and one is defended then the remaining 49 measurements are all attackable.

The critical units at standard loading conditions are $P_{L_6}, P_{D_2}, P_{L_3}$ and $P_{L_2}$. Then the attacker's action space,$A\_A_{space}$ has 6 attack strategies and defenders' action space,$D\_A_{space}$ has 4 defense strategies as shown in Table 12. The utilities are found by solving single-level MILPP using CPLEX interfaced with MATLAB and are all tabulated in Table 12. The average economic loss is considered as utility.

In this article, utility is economic loss. Economic loss is advantageous for attackers and loss for defenders/operators. Utility for attacker is economic loss $f(A, V)$ (objective of most damaging LRAV) and utility for defender is $-f(A, V)$. From these discussions, it can be depicted that attacker's loss is defender's gain and vice versa. Hence attacker's utility is 70.7955$/MWh and defender's utility is -70.7955$/MWh as shown in Table 13. As per the utilities of all 2*(6*4) = 48 possible attacker and defender strategies (shown in Table 13), a static zero-sum game is solved by using Gambit software. Gambit software's introduction and its application to attack-defense strategic game is given in Appendix-A2.

On applying zero-sum game theory on all 24*2 strategies in Table 13, an optimal Nash equilibrium point is found using simplicial subdivision method in Gambit software.

The probabilities of optimal attack-defense strategy are given in Table 14. The sum of probabilities of attack and defense strategies is 1 and 1 respectively, also shown in Table 14. From Table 14, optimal attack-defense strategy's probabilities are not pure but mixed. At the point of Nash equilibrium, probability of $A_{s_3}$ is 0.1382 (13.82%), probability of $A_{s_4}$ is 0.8618 (86.18%) and the attack probabilities of remaining four strategies is 0. However, at Nash equilibrium, probability of $D_{s_2}$ is 0.1382 (13.82%), probability of $D_{s_4}$ is 0.8618 (86.18%) and the defense probabilities of remaining two strategies is 0.

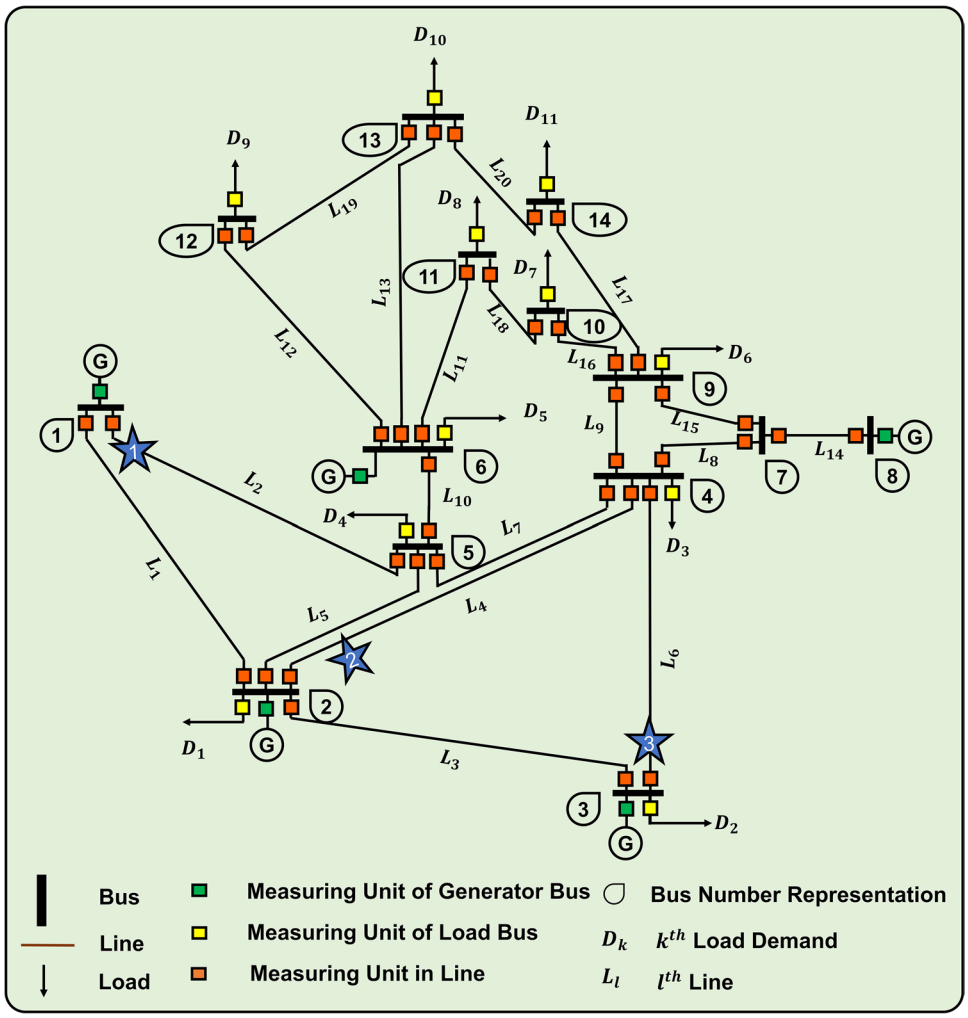


**Fig. 8** Critical units of modified IEEE-14 bus system at low loading conditions

**Table 11** Computational time in three loading scenarios

| Attack and defense resources at one execution run | Computational Time | | | | | |
|---|---|---|---|---|---|---|
| | Scenario-1: Standard Load | | Scenario-2: High Load | | Scenario-3: Low Load | |
| | Seconds | Minutes | Seconds | Minutes | Seconds | Minutes |
| One attack one defense | 2.200 | 0.037 | 2.369 | 0.039 | 1.045 | 0.017 |
| All attacks one defense | 83.128 | 1.385 | 195.912 | 3.265 | 53.446 | 0.891 |
| All attacks all defenses | 1115.424 | 18.590 | 5030.474 | 83.841 | 574.901 | 9.582 |

**Table 12** Average economic loss in possible attack and defense strategies at standard loading conditions

| Attack Strategies, \$/MWh | Defense Strategies, \$/MWh | | | |
|---|---|---|---|---|
| | $D_{s_1} \Rightarrow P_{L_6}, P_{D_2}$ | $D_{s_2} \Rightarrow P_{D_2}$ | $D_{s_3} \Rightarrow P_{L_3}$ | $D_{s_4} \Rightarrow P_{L_2}$ |
| $A_{s_1} \Rightarrow P_{L_6}, P_{D_2}$ | 0 | 0 | 0 | 0 |
| $A_{s_2} \Rightarrow P_{L_6}, P_{L_3}$ | 0 | 5.7817 | 0 | 5.7817 |
| $A_{s_3} \Rightarrow P_{L_6}, P_{L_2}$ | 70.7955 | 70.7955 | 70.7955 | 0 |
| $A_{s_4} \Rightarrow P_{D_2}, P_{L_3}$ | 11.3552 | 0 | 0 | 11.3552 |
| $A_{s_5} \Rightarrow P_{D_2}, P_{L_2}$ | 70.7955 | 70.7955 | 70.7955 | 0 |
| $A_{s_6} \Rightarrow P_{L_3}, P_{L_2}$ | 70.7955 | 70.7955 | 70.7955 | 0 |

### Optimal Attack-Defense Strategy in Scenario-2-High Load Condition

The optimal number of critical units in scenario-2 is 6 ($P_{D_2}$, $P_{L_6}$, $P_{L_3}$, $P_{L_{13}}$, $P_{D_3}$ and $P_{D_2}$). Let attacker has access to 5 critical units among six and defender can protect one among six, then $N_{S_A} = \binom{6}{5} \Rightarrow N_{S_A} = 6$ and $N_{S_D} = \binom{6}{1} \Rightarrow N_{S_D} = 6$. Attacker's action space,$A\_A_{space}$ has 6 attack strategies and defenders' action space,$D\_A_{space}$ has 6 defense strategies as shown in Table 15.

**Table 13** Utility table of static zero-sum game at standard load demand at standard loading conditions

| Attack Strategies, $/MWh | Defense Strategies, $/MWh | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | $D_{s_1}$ | | $D_{s_2}$ | | $D_{s_3}$ | | $D_{s_4}$ | |
| | *A* | *D* | *A* | *D* | *A* | *D* | *A* | *D* |
| $A_{s_1}$ | 0 | -0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $A_{s_2}$ | 0 | -0 | 5.7817 | -5.7817 | 0 | 0 | 5.7817 | -5.7817 |
| $A_{s_3}$ | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 0 | 0 |
| $A_{s_4}$ | 11.3552 | -11.3552 | 0 | 0 | 0 | 0 | 11.3552 | -11.3552 |
| $A_{s_5}$ | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 0 | 0 |
| $A_{s_6}$ | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 70.7955 | -70.7955 | 0 | 0 |

**Table 14** Optimal attack and defense probabilities at Nash equilibrium on standard loading conditions

| Attack Probabilities,$P_{A\_S_a}$ | | Defense Probabilities,$P_{D\_S_d}$ | |
|---|---|---|---|
| $P_{A\_S_1}$ | 0 | $P_{D\_S_1}$ | 0 |
| $P_{A\_S_2}$ | 0 | $P_{D\_S_2}$ | 0.1382 |
| $P_{A\_S_3}$ | 0.1382 | $P_{D\_S_3}$ | 0 |
| $P_{A\_S_4}$ | 0.8618 | $P_{D\_S_4}$ | 0.8618 |
| $P_{A\_S_5}$ | 0 | $\sum_{i=1}^{N_{s_D}} P_{D\_S_i} = 0.1382 + 0.8618 \rightarrow \sum_{i=1}^{N_{s_D}} P_{D\_S_i} = 1$ | |
| $P_{A\_S_6}$ | 0 | | |
| $\sum_{i=1}^{N_{s_A}} P_{A\_S_i} = 0.1382 + 0.8618 \rightarrow \sum_{i=1}^{N_{s_A}} P_{A\_S_i} = 1$ | | | |

**Table 15** Average economic loss in possible attack-defense strategies at high loading conditions

| Attack Strategies, $/MWh | Defense Strategies, $/MWh | | | | | |
|---|---|---|---|---|---|---|
| | $D_{s_1} \Rightarrow P_{D_2}$ | $D_{s_2} \Rightarrow P_{L_6}$ | $D_{s_3} \Rightarrow P_{L_3}$ | $D_{s_4} \Rightarrow P_{L_{13}}$ | $D_{s_5} \Rightarrow P_{D_3}$ | $D_{s_6} \Rightarrow P_{D_1}$ |
| $A_{s_1} \Rightarrow P_{D_2}$ | 1192.8 | 1162.0 | 1162.1 | 361.9888 | 921.1912 | 970.5347 |
| $A_{s_2} \Rightarrow P_{L_6}$ | 1162.0 | 1198.8 | 1162.1 | 332.4115 | 920.3664 | 1003.0 |
| $A_{s_3} \Rightarrow P_{L_3}$ | 1162.1 | 1162.1 | 1162.1 | 418.3842 | 966.1590 | 974.1143 |
| $A_{s_4} \Rightarrow P_{L_{13}}$ | 361.9888 | 332.4115 | 418.3842 | 1348.9 | 884.3864 | 822.3519 |
| $A_{s_5} \Rightarrow P_{D_3}$ | 921.1912 | 920.3664 | 966.1590 | 884.3864 | 1378.5 | 1196.4 |
| $A_{s_6} \Rightarrow P_{D_1}$ | 970.5347 | 1003.0 | 974.1143 | 822.3519 | 1196.4 | 1405.7 |

**Table 16** Optimal attack and defense probabilities at Nash equilibrium on high loading conditions

| Attack Probabilities,$P_{A\_S_a}$ | | Defense Probabilities,$P_{D\_S_d}$ | |
|---|---|---|---|
| $P_{A\_S_1}$ | 0 | $P_{D\_S_1}$ | 0.0619 |
| $P_{A\_S_2}$ | 0 | $P_{D\_S_2}$ | 0.3812 |
| $P_{A\_S_3}$ | 0 | $P_{D\_S_3}$ | 0 |
| $P_{A\_S_4}$ | 0.0427 | $P_{D\_S_4}$ | 0.5570 |
| $P_{A\_S_5}$ | 0.8957 | $P_{D\_S_5}$ | 0 |
| $P_{A\_S_6}$ | 0.0616 | $P_{D\_S_6}$ | 0 |
| $\sum_{i=1}^{N_{s_A}} P_{A_{S_i}} = 0.0427 + 0.8957 + 0.0616 \Rightarrow \sum_{i=1}^{N_{s_A}} P_{A\_S_i} = 1$ | | $\sum_{i=1}^{N_{s_D}} P_{D_{S_i}} = 0.0619 + 0.3812 + 0.5570 \Rightarrow \sum_{i=1}^{N_{s_D}} P_{D\_S_i} = 1$ | |

On applying zero-sum game theory on all 36 strategies in Table 15, the Nash equilibrium is found using simplicial subdivision method in Gambit software as shown in Table 16.

From Table 16, at the point of Nash equilibrium, probability of $A_{s_4}$ is 0.0427 (4.27%), probability of $A_{s_5}$ is 0.8957 (89.57%), probability of $A_{s_6}$ is 0.0616 (6.16%) and attack probabilities of remaining three strategies is 0. However,

**Table 17** Average Economic loss regarding possible strategies at low loading

| Attack Strategies, $/MWh | Defense Strategies, $/MWh | | |
|---|---|---|---|
| | $D_{s_1} \Rightarrow P_{L_2}$ | $D_{s_2} \Rightarrow P_{L_4}$ | $D_{s_3} \Rightarrow P_{L_6}$ |
| $A_{s_1} \Rightarrow P_{L_2}$ | 19.2699 | 9.9780 | 0 |
| $A_{s_2} \Rightarrow P_{L_4}$ | 9.9780 | 71.3918 | 62.5574 |
| $A_{s_3} \Rightarrow P_{L_6}$ | 0 | 62.5574 | 106.6713 |

at Nash equilibrium, probability of $D_{s_1}$ is 0.0619 (6.19%), probability of $D_{s_2}$ is 0.3812 (38.12%), probability of $D_{s_4}$ is 0.5570 (55.70%) and defense probabilities of remaining three strategies is 0.

### Optimal Attack-Defense Strategy in Scenario-3-Low Load Condition

The optimal number of critical units in scenario-3 is 3 ($P_{L_2}$, $P_{L_4}$ and $P_{L_6}$). Let attacker has access to 2 critical units among total three and defender can protect one among three, then $N_{S_A} = \binom{3}{2} \Rightarrow N_{S_A} = 3$ and $N_{S_D} = \binom{3}{1} \Rightarrow N_{S_D} = 3$. Attacker's action space,$A\_A_{space}$ has 3 attack strategies and defenders' action space,$D\_A_{space}$ has 3 defense strategies as shown in Table 17.

On applying zero-sum game theory on all 9*2 strategies in Table 17, the Nash equilibrium is found using simplicial subdivision method in Gambit software and the optimal attack-defense probabilities at Nash equilibrium are given in Table 18.

From Table 18, at the point of Nash equilibrium, probability of $A_{s_1}$ is 0.7318 (73.18%), probability of $A_{s_2}$ is 0.2682 (26.82%) and attack probability of remaining one strategy is 0. However, at Nash equilibrium, probability of $D_{s_1}$ is 0.8707 (87.07%), probability of $D_{s_2}$ is 0.1293 (12.93%) and defense probability of remaining one strategy is 0.

From the above analysis, if all the critical units are used for attacking and defending, economic loss will be maximum and minimum (zero) respectively. But due to budget issues on both attacker and defender side, only some critical units can be attacked and some can be defended. So, an optimal attack-defense strategy can be obtained with suitable critical units, found using static zero sum game theory. Hence from these discussions, it can be depicted that for such percentage of attacking probability, the defense budget can be shared proportionally based on the defense probabilities. If the defense probability for a strategy is maximum, the budget allocated for upgrading of those units' firewalls in that defense strategy will be high.

## Conclusions

Cyber defense is a key aspect that require upgrading or updating of power system to safeguard against bad/false data intrusions. Researchers have modelled many intelligent undetectable attacks like FDIAVs. However, in practical, LRAV can directly target bus active power injections and line active power flows. In this article, three aspects are mainly dealt. The first aspect is obtaining maximum economic loss due to the most damaging LRAV of modified IEEE-14 bus test system where loss is found by converting BPP to single-level MILPP and then computed in MATLAB integrated with MATPOWER and CPLEX. Table 3 and Fig. 5 shows the proportionality of economic loss with respect to attack resources. For attack resources $R = 0$ to $R = 51$, the economic loss is increased from 0$/MWh to 3733$/MWh and load shedding is increased from 0MW to 61.1759MW which are shown in Table 3. So, it is a mandate to suppress these undesirables.

Cyber defense is superior to counter attacking in the present scenario, so that attacker can't intrude into the system completely and inject successful vectors. Before finding an optimal defense strategy, it is mandate to find optimal attack strategy and critical units. From selection of critical measuring units section, it is clear that optimal critical units may not be satisfactory by entropic degree method or by highly operating points. Hence the second aspect in this article is development of a procedure to find critical units, even if load varies or number of attack resources is unaware. Fig. 2 shows the developed procedure which is validated on the test system at standard, high and low loading conditions subjected to all possible attack resources. Figs. 6, 7 and 8 show the details of critical units at standard, high and low loading conditions.

**Table 18** Optimal Attack and Defense Probabilities at Nash Equilibrium on low loading conditions

| Attack Probabilities,$P_{A\_S_a}$ | | Defense Probabilities,$P_{D\_S_d}$ | |
|---|---|---|---|
| $P_{A\_S_1}$ | 0.7318 | $P_{D\_S_1}$ | 0.8707 |
| $P_{A\_S_2}$ | 0.2682 | $P_{D\_S_2}$ | 0 |
| $P_{A\_S_3}$ | 0 | $P_{D\_S_3}$ | 0.1293 |
| $\sum_{i=1}^{N_{S_A}} P_{A\_S_i} = 0.7318 + 0.2682 \Rightarrow \sum_{i=1}^{N_{S_A}} P_{A\_S_i} = 1$ | | $\sum_{i=1}^{N_{S_D}} P_{D\_S_i} = 0.8707 + 0.1293 \Rightarrow \sum_{i=1}^{N_{S_D}} P_{D\_S_i} = 1$ | |

| | 1 | | 2 | | 3 | | 4 | |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 57817/10000 | -57817/10000 | 0 | 0 | 57817/10000 | -57817/10000 |
| 3 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 0 | 0 |
| 4 | 7097/625 | -7097/625 | 0 | 0 | 0 | 0 | 7097/625 | -7097/625 |
| 5 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 0 | 0 |
| 6 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 141591/2000 | -141591/2000 | 0 | 0 |

**Fig. 9** Utility Table in Gambit (Data from Table 13)

The third aspect discusses the probabilities of optimal attack-defense strategies at three loading conditions. Optimal probabilities are acquired by playing a static-zero sum game. Economic loss is considered as utility rather than load shedding as economic loss has both power generation and load shedding costs [18, 19]. Optimal attack-defense probabilities at Nash equilibrium in all three loadings are given in Table 14, Table 16 and Table 18 respectively. Hence this work provides some knowledge, that which measuring unit has to be treated as critical and among the selected critical devices, which device has to be defended/protected against LRA.

## Appendix 1

The Lagrangian function of the lower level of BPP is given as:

$$\begin{aligned}\mathcal{L}\left(\Delta P_D, P_{g_i}, L_{s_k}\right) = &\sum_{i=1}^{N_g} C_{g_i} * P_{g_i} + \sum_{k=1}^{N_d} C_{s_k} * L_{sk} \\ &- \lambda * \left\{\sum_{i=1}^{N_g} P_{g_i} - \sum_{k=1}^{N_d}(P_{Dk} - L_{sk})\right\} \\ &- \mu_l * \left\{\boldsymbol{P_L} - \boldsymbol{SF.KP.P_g} + \boldsymbol{SF.KD.}(\boldsymbol{P_D} + \Delta\boldsymbol{P_D} - \boldsymbol{L_s})\right\} \\ &- \underline{\mathrm{A}}_l * \left\{P_{L_l} + P_{L_l}^{max}\right\} - \overline{\mathrm{A}}_l * \left\{P_{L_l}^{max} - P_{L_l}\right\} - \underline{\mathrm{B}}_i * \left\{P_{g_i} - P_{g_i}^{min}\right\} \\ &- \overline{\mathrm{B}}_i\left\{P_{g_i}^{max} - P_{g_i}\right\} - \underline{\Gamma}_k\left\{L_{s_k}\right\} - \overline{\Gamma}_k\left\{P_{D_k} + \Delta P_{D_k} - L_{s_k}\right\}\end{aligned} \tag{24}$$

KKT necessary optimality conditions of the lower level BPP is as follows:

$$\frac{\partial \mathcal{L}}{\partial P_{g_i}} = 0 \rightarrow C_{g_i} - \lambda + \left(SF.KP_{g_i}\right)^T * \mu - \underline{\mathrm{B}}_i + \overline{\mathrm{B}}_i = 0 \tag{25}$$

$$\frac{\partial \mathcal{L}}{\partial L_{s_k}} = 0 \rightarrow C_{s_d} - \lambda + \left(SF.KD_{s_d}\right)^T * \mu - \underline{\Gamma}_d + \overline{\Gamma}_d = 0 \tag{26}$$

$$\frac{\partial \mathcal{L}}{\partial P_L} = 0 \rightarrow \mu_l - \underline{\mathrm{A}}_l + \overline{\mathrm{A}}_l = 0 \tag{27}$$

$$\underline{\mathrm{A}}_l, \overline{\mathrm{A}}_l, \underline{\mathrm{B}}_i, \overline{\mathrm{B}}_i, \underline{\Gamma}_k, \overline{\Gamma}_k \geq 0 \tag{28}$$

$$\underline{\mathrm{A}}_l * \left(P_{L_l} + P_{L_l}^{max}\right) = 0 \tag{29}$$

$$\overline{\mathrm{A}}_l * \left(P_{L_l}^{max} - P_{L_l}\right) = 0 \tag{30}$$

$$\underline{\mathrm{B}}_i * \left\{P_{g_i} - P_{g_i}^{min}\right\} = 0 \tag{31}$$

$$\overline{\mathrm{B}}_i\left\{P_{g_i}^{max} - P_{g_i}\right\} = 0 \tag{32}$$

$$\underline{\Gamma}_k\left\{L_{s_k}\right\} = 0 \tag{33}$$

$$\overline{\Gamma}_k\left\{P_{D_k} + \Delta P_{D_k} - L_{s_k}\right\} = 0 \tag{34}$$

(28) represents the non-negativity constraints and (28)-(34) are complementary slackness conditions which are non-linear equations. These complementary slackness non-linear conditions can be linearized. Let $\pi f = 0$ be the complementary slackness condition where $\pi$ be a non-negative Lagrange multiplier and $f$ be a continuous function which can be represented into two linear inequalities like $\pi \leq M\omega$ and $f \leq M(1-\omega)$. $M$ represents sufficiently large positive constant and $\omega$ is a new binary variable. Then (28)-(34) can be represented in the form of linear equations as follows:

$$\underline{\mathrm{A}}_l * \left(P_{L_l} + P_{L_l}^{max}\right) = 0 \rightarrow \begin{matrix}\underline{\mathrm{A}}_l \leq M\omega_{\underline{\mathrm{A}},l} \\ P_{Ll} + P_{Ll}^{max} \leq M(1-\omega_{\underline{\mathrm{A}},l})\end{matrix} \tag{35}$$

$$\overline{\mathrm{A}}_l * \left(P_{L_l} + P_{L_l}^{max}\right) = 0 \rightarrow \begin{matrix}\overline{\mathrm{A}}_l \leq M\omega_{\overline{\mathrm{A}},l} \\ P_{Ll}^{max} - P_{Ll} \leq M(1-\omega_{\overline{\mathrm{A}},l})\end{matrix} \tag{36}$$

$$\underline{\mathrm{B}}_i * \left\{P_{g_i} - P_{g_i}^{min}\right\} = 0 \rightarrow \begin{matrix}\underline{\mathrm{B}}_i \leq M\omega_{\underline{\mathrm{B}},i} \\ P_{g_i} - P_{g_i}^{min} \leq M(1-\omega_{\underline{\mathrm{B}},i})\end{matrix} \tag{37}$$

$$\overline{\mathrm{B}}_i\left\{P_{g_i}^{max}-P_{g_i}\right\}=0\Rightarrow\begin{array}{c}\overline{\mathrm{B}}_i\le M\omega_{\overline{\mathrm{B}},i}\\ P_{g_i}^{\ max}-P_{g_i}\le M(1-\omega_{\overline{\mathrm{B}},i})\end{array}\tag{38}$$

$$\underline{\Gamma}_k\left\{L_{s_k}\right\}=0\rightarrow\begin{array}{c}\underline{\Gamma}_k\le M\omega_{\underline{\Gamma},k}\\ L_{sk}\le M(1-\omega_{\underline{\Gamma},k})\end{array}\tag{39}$$

$$\overline{\Gamma}_k\left\{P_{D_k}+\Delta P_{D_k}-L_{s_k}\right\}=0\rightarrow\begin{array}{c}\overline{\Gamma}_k\le M\omega_{\overline{\Gamma},k}\\ P_{Dk}+\Delta P_{Dk}-L_{sk}\le M(1-\omega_{\overline{\Gamma},k})\end{array}\tag{40}$$

## Appendix 2

Gambit Software: Gambit is an open source software which is used to solve an optimal solution for player games. The main advantage of Gambit software is it is a Graphical User Interface and the other advantage of it is it helps to find equilibrium points in a game and dominance of players in a game. In this article, Gambit is used to find the Nash equilibrium of static-zero sum attack-defense game. The utility values table with different strategies can be easily given to Gambit such that Nash equilibrium can be obtained within less time. Gambit also has other advantage that it gives not only single Nash equilibrium but also multiple Nash equilibria. The data from Table 13 is taken and can be directly entered in Gambit GUI is shown in Fig. 9. After entering the values, using "Tools" in Gambit, Nash equilibrium using "by solving a linear program" method is used and the result is nothing but the probabilities of attack and defense strategies. The probabilities after Nash equilibrium (Optimal attack-defense strategy) is shown in Fig. 10.

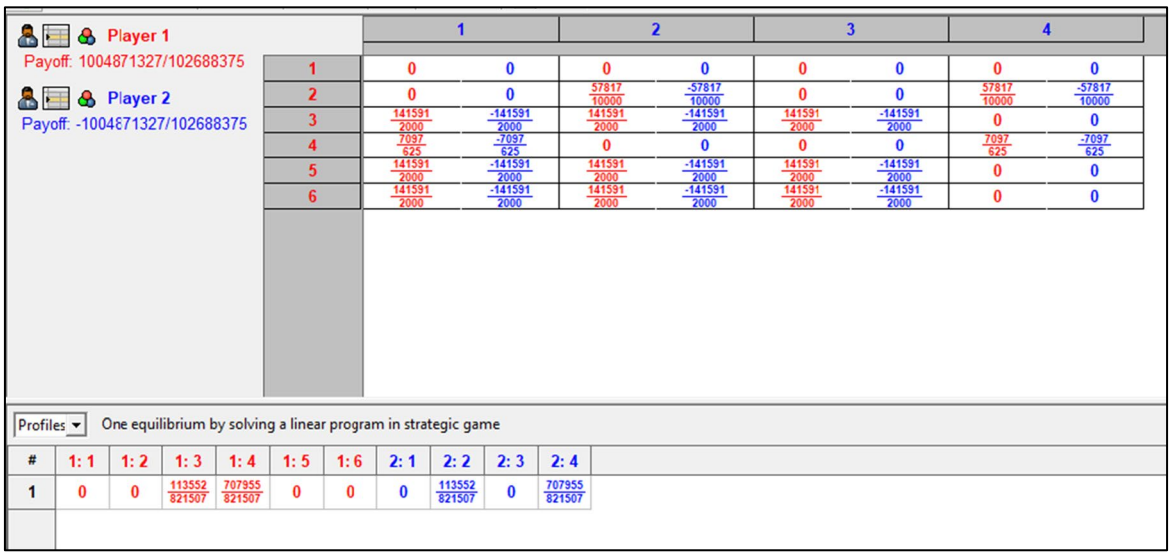


**Fig. 10** Probabilities of optimal attack-defense strategy at standard load of test system

**Acknowledgements** 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. Bi S, Zhang YJ (2014) Graphical methods for defense against false-data injection attacks on power system state estimation. IEEE Trans on Smart Grid 5(3):1216–1227. https://doi.org/10.1109/TSG.2013.2294966
2. Wu C, Wang X, Xue F, Xu X, Lu S, Zhai Y, Jiang L (2018) Evaluation of Buses in Power Grids by Extended Entropic Degree. In: 2018 IEEE 37th Chinese Control Conference (CCC), pp. 1092-1097. https://doi.org/10.23919/ChiCC.2018.8482984
3. Chen G, Dong ZY, Hill DJ, Xue YS (2010) Exploring reliable strategies for defending power systems against targeted attacks. IEEE Trans on Power Syst 26(3):1000–1009. https://doi.org/10.1109/TPWRS.2010.2078524
4. Chen Y, Hong J, Liu CC (2016) Modeling of intrusion and defense for assessment of cyber security at power substations. IEEE Trans on Smart Grid 9(4):2541–2552. https://doi.org/10.1109/TSG.2016.2614603

5. Deng R, Xiao G, Lu R (2017) Defending against false data injection attacks on power system state estimation. IEEE Trans on Ind Inform 13(1):198–207. https://doi.org/10.1109/TII.2015.2470218
6. Ding Z, Xiang Y, Wang L (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. https://doi.org/10.1109/PESGM.2016.7741526
7. Esmalifalak M, Shi G, Han Z, Song L (2013) Bad data injection attack and defense in electricity market using game theory study. IEEE Trans on Smart Grid 4(1):160–169. https://doi.org/10.1109/TSG.2012.2224391
8. Cplex II. V12. 1: User's Manual for CPLEX. International Business Machines Corporation. 2009;46(53):157. Available: https://www.ibm.com/in-en/products/ilog-cplex-optimization-studio
9. Krishna KB, Rosalina KM, Ramaraj N (2018) Complete and incomplete observability analysis by optimal PMU placement techniques of a network. J of Electr Eng and Technol 13(5):1814–1820. https://doi.org/10.5370/JEET.2018.13.5.1814
10. Liu X, Li Z (2014) Local load redistribution attacks in power systems with incomplete network information. IEEE Trans on Smart Grid 5(4):1665–1676. https://doi.org/10.1109/TSG.2013.2291661
11. Liu X, Li Z (2017) Local topology attacks in smart grids. IEEE Trans on Smart Grid 8(6):2617–2626. https://doi.org/10.1109/TSG.2016.2532347
12. Liu X, Li Z, Shuai Z, Wen Y (2017) Cyber attacks against the economic operation of power systems: A fast solution. IEEE Trans on Smart Grid 8(2):1023–1025. https://doi.org/10.1109/TSG.2016.2623983
13. Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans on Inf and Sys Secur 14(1):1–33. https://doi.org/10.1145/1952982.1952995
14. McKelvey RD, McLennan AM, Turocy TL (2014) Gambit: Software tools for game theory, Version 15.1.1. http://www.gambit-project.org
15. Mishra A, Gundavarapu VN (2015) Contingency management of power system with interline power flow controller using real power performance index and line stability index. Ain Shams Eng J 7(1):209–222. https://doi.org/10.1016/j.asej.2015.11.004
16. Shen Y, Fei M, Du D (2019) Cyber security study for power systems under denial of service attacks. Trans of the Inst of Meas and Control 41(6):1600–1614. https://doi.org/10.1177/0142331217709528
17. Xiang Y, Ding Z, Zhang Y, Wang L (2017) Power system reliability evaluation considering load redistribution attacks. IEEE Trans on Smart Grid 8(2):889–901. https://doi.org/10.1109/TSG.2016.2569589
18. Xiang Y, Wang L (2015) A game-theoretic approach to optimal defense strategy against load redistribution attack. In: 2015 IEEE Power & Energy Society General Meeting, pp. 1-5. https://doi.org/10.1109/PESGM.2015.7286529
19. Xiang Y, Wang L (2017) A game-theoretic study of load redistribution attack and defense in power systems. Electr Power Syst Res 151:12–25. https://doi.org/10.1016/j.epsr.2017.05.020
20. Xiang Y, Wang L, Liu N (2017) A framework for modeling load redistribution attacks coordinating with switching attacks. In: 2017 IEEE Power & Energy Society General Meeting, pp 1-5. https://doi.org/10.1109/PESGM.2017.8274621
21. Xiang Y, Wang L, Yu D, Liu N (2015) Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks. In: 2015 IEEE Power & Energy Society General Meeting, pp 1-5. https://doi.org/10.1109/PESGM.2015.7286402
22. Yang Y, McLaughlin K, Littler T, Sezer S, Eul Gyu Im, Yao ZQ, Pranggono B, Wang HF (2012) Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems. In: 2012 International Conference on Sustainable Power Generation and Supply (SUPERGEN-2012), pp 1-8. https://doi.org/10.1049/cp.2012.1831
23. Yuan Y, Li Z, Ren K (2011) Modeling load redistribution attacks in power systems. IEEE Trans on Smart Grid 2(2):382–390. https://doi.org/10.1109/TSG.2011.2123925
24. Yuan Y, Li Z, Ren K (2012) Quantitative analysis of load redistribution attacks in power systems. IEEE Trans on Parallel and Distrib Sys 23(9):1731–1738. https://doi.org/10.1109/TPDS.2012.58
25. Zimmerman RD, Murillo-Sánchez CE, Thomas RJ (2011) MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans on Power Syst 26(1):12–19. https://doi.org/10.1109/TPWRS.2010.2051168