frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 25 September 2023
DOI 10.3389/fenrg.2023.1242047

OPEN ACCESS

EDITED BY
Mingfei Ban,
Northeast Forestry University, China

REVIEWED BY
Yushuai Li,
University of Oslo, Norway
Mingyu Yan,
Huazhong University of Science and Technology, China
Zhenjie Li,
Northeast Forestry University, China
Yingjun Wu,
Hohai University, China

*CORRESPONDENCE
Weiyu Wang,
wywang@csust.edu.cn

RECEIVED 18 June 2023
ACCEPTED 07 September 2023
PUBLISHED 25 September 2023

CITATION
Shi X, Guo H, Wang W, Yin B and Cao Y (2023), Modeling and assessing load redistribution attacks considering cyber vulnerabilities in power systems. *Front. Energy Res.* 11:1242047. doi: 10.3389/fenrg.2023.1242047

Modeling and assessing load redistribution attacks considering cyber vulnerabilities in power systems

Xingyu Shi, Huan Guo, Weiyu Wang*, Banghuang Yin and Yijia Cao

School of Electrical and Information Engineering, Changsha University of Science and Technology, Changsha, China

Introduction: Load Redistribution (LR) attacks, as a common form of false data injection attack, have emerged as a significant cybersecurity threat to power system operations by manipulating load buses' measurements at substations. Existing LR attack methods typically assume that any substation can be equally attacked, contributing to the analysis of LR attacks in power systems. However, the diversity of cyber vulnerabilities in substation communication links implies varying costs associated with falsifying load buses' measurements. Thus, quantitatively evaluating these costs and analyzing the impact of LR attacks on power systems within cost constraints holds practical significance.

Methods: In this paper, we employ a Bayesian attack graph model to characterize the intrusion process through cyber vulnerabilities. The costs of falsifying load buses' measurements at substations are quantitatively evaluated using the mean time-to-compromise model. Subsequently, from the attacker's perspective, we propose a bi-level optimization model for LR attacks, considering the mean time to compromise in conjunction with limited attack resources and power flow constraints.

Results: Simulations conducted on the IEEE 14-bus system illustrate the influence of cyber vulnerabilities on LR attacks within power systems. Furthermore, we verify that the attack scenario of the existing LR attack model aligns with a case of the proposed bi-level LR attack model when there is sufficient attack time to compromise all communication links.

Discussion: The findings of this research demonstrate that the impact of cyber vulnerabilities on LR attacks can be quantified by assessing the attack costs. Effective management of LR attacks can be achieved under cost constraints through optimization methods. These insights contribute to enhancing network security strategies for power systems, mitigating potential threats posed by LR attacks in power system operations.

KEYWORDS

cyber-physical systems, false data injection attacks, load redistribution attack, Bayesian attack graph model, mean time to compromise, bi-level model, common vulnerability scoring system

1 Introduction

The cyber-physical power system has become the main feature of modern power systems and attracts countries to compete to develop such a power system (Pliatsios et al., 2020; Liu et al., 2022). The cyber system brings flexibility to the operation of power grids. However, the complex cyber-enabled technologies and communication networks will profoundly impact the physical process of power systems, bringing more cyber security problems to the power system (Xiang et al., 2016; Zhang and Yang, 2022).

In recent years, the militarization of global cyberspace has accelerated, and cyberattacks targeting critical core infrastructure have developed into real threats. Many information technologies were deployed in the power system to defend against cyberattacks. The state estimation has been widely used by energy management systems (EMSs) to filter the measurement noise and detect gross errors. Information encryption technology, network address locking, and modifying defense equipment are used to enhance the security of the power system. However, intruders can still launch various malicious attacks to compromise the power data integrity by exploiting the vulnerabilities and social engineering access to a target network authority. Attackers can mislead the operator to conduct uneconomical power system operations, obtain economic benefits, and even disrupt the stability of the power system (Yuan et al., 2011; Tan et al., 2016; Zhang and Yang, 2022).

Cyberattacks on power systems can be divided into man-in-the-middle (MITM) attacks, replay attacks, and false data injection (FDI) attacks (Deng et al., 2016). Among them, the FDI attack refers to injecting falsified measurements, inducing uneconomic, non-optimal, or even harmful decisions on power dispatch based on security-constrained economic dispatch (SCED). Load redistribution (LR) attacks are typical FDI attacks, which mislead operators by injecting falsified load values (Liang et al., 2016).

In the LR attack model, extensive attention has been paid to constructing a representative attack vector and investigating the system response (Yuan et al., 2011; Liu et al., 2015; Gao et al., 2022). LR attack against state estimation was first proposed by Liu et al. ((2011), which is a coordinated cyberattack against state estimation. In the work of Liu and Li (2014) and Liu and Li (2016), the concept of an attack zone is introduced, and the regional LR attack model is proposed. In the work of Gao et al. (2022), an LR attack model was built based on pre- and post-dispatch, which can lead the system to an uneconomic and insecure operating state. In the work of Liu et al. (2016), a simple approach was used to determine an effective attack vector to change the load data sent to the control center.

The abovementioned works contributed to analyzing the impact of LR attacks in power systems, given that load buses' measurements of substations are equally attackable. However, cyber vulnerabilities in communication links of substations are diverse, and therefore, the feasibility of injecting falsified measurements of different load buses has a significant difference, which will affect the impact of LR attacks on power systems. Hence, assessing LR attacks with cyber vulnerabilities has become non-negligible work.

In the literature, different vulnerability evaluation models have been developed to address cyber security issues of power grids. The Petri net was first proposed by Ten et al. (2008), which can assess the cyber vulnerabilities in power systems and quantify the potential harm cyberattacks may cause. In the work of Bahrami et al. (2020), Petri nets are used to simulate possible intrusion scenarios into substation networks, and a multi-state Markov model is proposed to identify the consequences of cyberattacks on protective devices. However, the abovementioned probabilistic model cannot estimate the attack time that will impact the result of the LR attack. The mean time-to-compromise (MTTC) model is a meaningful way to quantitatively estimate the time intervals of successful attacks on the target cyber components of the SCADA system (Zhang et al., 2015). The MTTC model also was applied to assess the reliability of the wind farm energy management systems (Zhang et al., 2017).

In the paper, the intruding process through cyber vulnerabilities is modeled, and the costs to intrude communication links between substations and the control center are quantitatively evaluated. Then, a bi-level model of LR attack considering cyber vulnerabilities is proposed. The main works of the paper are as follows:

1) This paper introduces a Bayesian attack graph model to simulate the process of intruding communication links between substations and the control center through cyber vulnerabilities. Subsequently, the intruding time is quantitatively assessed through the MTTC model.
2) A bi-level LR attack model is proposed, considering the MTTC, limited attack resources, and power flow constraints, to identify the most damaging LR attack. The upper-level constructs an attack vector to maximize the operation cost of the power system. The lower-level employs the SCED to model the operator response after the LR attack.
3) The IEEE 14-bus system is adopted to test the proposed LR attack model. The MTTC of intruding communication links through cyber vulnerabilities between the substations and the control center is quantitatively evaluated. Then, the impact of the LR attack on operation cost is analyzed with different available attack resources and time.
4) Results show that cyber vulnerabilities will significantly impact the LR attack on power systems. Furthermore, it can be found that the most damaging scenario in the traditional LR attack may not be achieved due to the limited attacking time unable to intrude necessary communication links, and the scenario is just a case in the proposed bi-level LR attack model with the sufficient attack time to intrude all communication links between the substations and the control center.

The remainder of this paper is organized as follows. The evaluation of cyber vulnerabilities is introduced in Section 2. The LR attack model considering cyber vulnerabilities is given in Section 3, Section 4 presents the quantitative analysis, and Section 5 concludes the paper.

2 Cost evaluation of LR attacks on communication links through cyber vulnerabilities

Cyberattacks weaken or destroy the secondary system operation of power systems. Information is interrupted, delayed, or tampered with if the secondary system suffers malicious attacks, such as SCADA, WAMS, and AMI systems (Yang et al., 2022). The control center may give wrong instructions, and the decision-making units misoperate or quit the operation (Che et al., 2019).

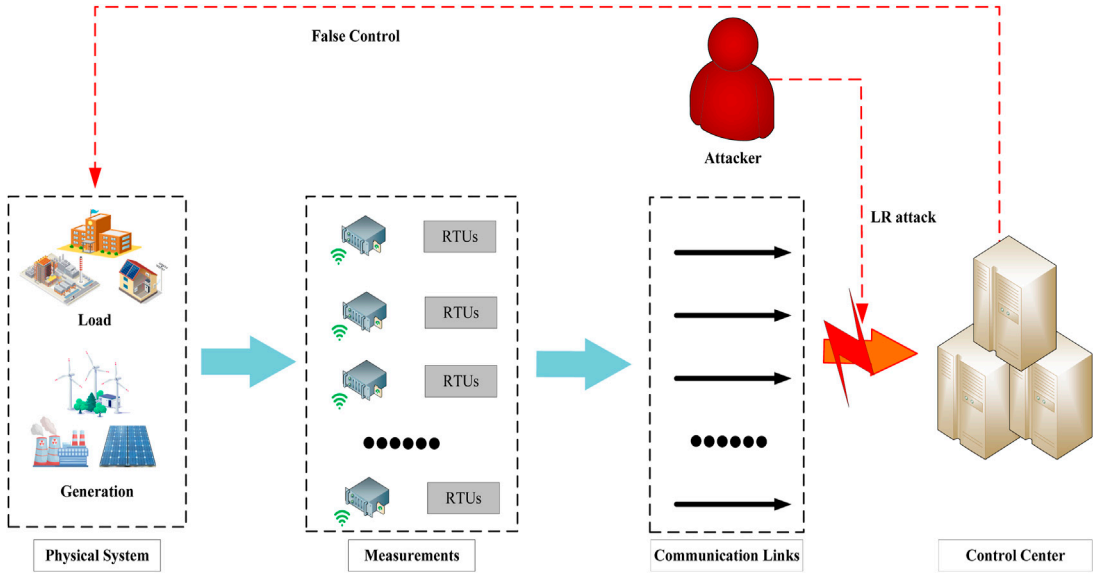

FIGURE 1
LR attacks in cyber-physical systems.

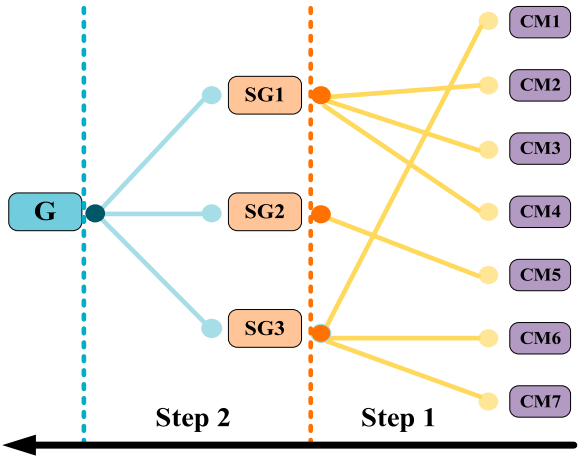

FIGURE 2
Bayesian attack graph model of LR attacks on communication links.

The measured power systems states, such as voltage amplitude, bus load, line state, and transmission line power flow, are transmitted through communication links between the substations and the control center. Power system communication links are easily intercepted and forged (Liang et al., 2016; Li et al., 2022), and an attacker can inject falsified measurements to mislead power system operators (Liu et al., 2016). Therefore, cyberattacks oriented to communication links are more threatening and have practical significance (Liu et al., 2016; Li et al., 2019).

Figure 1 shows LR attacks in cyber-physical systems. Based on measurements through communication links, the power system operator conducts unified scheduling of power generations and consumers according to security-constrained economic dispatch (SCED). Although countermeasures are deployed in power systems, attackers can manipulate measurements by intruding communication links through cyber vulnerabilities of known and zero vulnerabilities in the cyber system of power systems. The manipulated measurements, carefully calculated to avoid being identified as malicious data, mislead SCED to bring the system into an insecure and non-optimal operating condition.

2.1 Modeling intruding process on communication links through cyber vulnerabilities

Inspired by the work of Sommestad et al. (2009), a three-layer structure is employed to model the cyber intrusion of communication links between the targeted substation and the control center, as shown in Figure 2. The right side consists of power system countermeasures. The middle and left parts are the sub-goals and the goal of the LR attack, respectively. Table 1 lists the countermeasures of substations and sub-goals and goal of the LR attack.

To reach the second layer SG_j, for ($j \in \mathcal{J}$), where $\mathcal{J}$ is the set of the LR attack sub-goals, the intruder must first bypass one of the countermeasures CM_i, for $CM_i \in \mathcal{I}$ (SG_j), where $\mathcal{I}$ (SG_j) means the set of countermeasures related with SG_j. When all sub-goals are satisfied, the intruder can inject manipulated data into communication links.

Attackers intrude communication links through cyber vulnerabilities of known and zero vulnerabilities in countermeasures. Without loss of generality, it is assumed that the known and zero-day vulnerabilities are randomly distributed in countermeasures (Zhang et al., 2017). The CVSS scores reflect countermeasures' known and zero-day vulnerabilities from 0 to 10. The details of evaluating CVSS scores can be seen in the work of Zieger et al. (2018).

TABLE 1 Countermeasures, sub-goals, and overall goals.

Node label	Node usage	Node label	Node usage
CM1	Message encryption	CM7	Remote password
CM2	Medium type	SG1	Obtain network connection
CM3	Network address locking	SG2	Interpret message structure
CM4	Physical link protection	SG3	Generate valid data
CM5	Protocol non-public	G	Inject manipulated data
CM6	Signature cryptography		

According to Figure 2, the LR attack probability model can be obtained by the following equations:

$$p_d(CM_i) = \begin{cases} \frac{CVSS_i}{10} \times U(0,1), CM_i \text{ with Known vulnerability} \\ 0.008 \times U(0,1), CM_i \text{ with zero} - \text{day vulnerability} \end{cases}, \quad (1)$$

$$p_d\left(CM_i \wedge SG_j\right) = p_d(CM_i) \times p_d\left(SG_j \mid CM_i\right), \forall i \in \mathcal{I}\left(SG_j\right), \quad (2)$$

$$p_d\left(SG_j\right) = \sum p_d\left(CM_i \wedge SG_j\right), \forall i \in \mathcal{I}\left(SG_j\right), \forall j \in \mathcal{J}, \quad (3)$$

$$p_d(G) = \prod_{j=1}^{\mathcal{J}} p_d\left(SG_j\right), \forall j \in \mathcal{J}. \quad (4)$$

Equation (1) represents the probability of exploiting the known and zero-day vulnerabilities, where $CVSS_i$ indicates the bass score corresponding to known vulnerabilities in CM_i and U (0,1) is the uniform distribution corresponding with three preconditions of service, connection, and privilege to complete vulnerability exploitation. Equation (2) represents the probability of achieving SG_j through CM_i, for $i \in \diamondsuit$ (SG_j), where $p_d(SG_j|CM_i)$ is the conditional probability following a uniform distribution U (0.8, 1) of substation d. Equation (3) is the overall probability of reaching the sub-goal SG_j, for $j \in \mathcal{I}$. Equation (4) represents the probability of reaching the goal G of injecting manipulated data. In order to achieve G, SG_1, SG_2, and SG_3 should be reached.

2.2 Quantitatively evaluating the LR attack cost of intruding communication links

2.2.1 Compromise time model of vulnerabilities

The compromise time $T_{d,\ i}(v_i)$ is a metric to estimate the mean time to compromise vulnerabilities in the CM_i of the communication link of the substation at bus d, where v_i is the number of known or zero-day vulnerabilities in CM_i. $T_{d,\ i}(v_i)$ can be modeled as a stochastic process consisting of the following three sub-processes depending on the nature of the vulnerability and the attacker's skill level.

Process 1 means at least a known vulnerability on CM_i, which can be exploited to launch an attack. Process 2 means that no vulnerability can be exploited to launch an attack, though there is at least a known vulnerability in CM_i. Process 3 means that no known vulnerability can be exploited. Furthermore, new vulnerabilities must be searched for or developed. The $\{t_1, t_2, \text{and } t_3\}$ and $\{P_1, P_2, \text{and } P_3\}$ are the three sub-processes' mean times and probabilities, respectively.

We can see that processes 1 and 2 are mutually exclusive. Process 3 runs continuously and in parallel with processes 1 and 2. For the calculation feasibility of $T_{d,i}$, we assume that process 3 only occurs when processes 1 and 2 are inactive (Lau et al., 2021).

The calculation of $T_{d,\ i}(v_i)$ is as follows:

$$T_{d,i}(v_i) = \int_0^1 t^*(v_i, s, \sigma)^* Beta_{\varepsilon,\theta}(s) ds, \quad (5)$$

subject to

$$t^* = t_1 P_1 + t_2 P_2 + t_3 P_3, \quad (6)$$

$$\begin{cases} P_1 = 1 - e^{-v_i * \frac{m(s)}{\sigma}} \\ P_2 = (1 - P_1)(1 - u), \\ P_3 = 1 - P_1 - P_2 \end{cases} \quad (7)$$

$$\begin{cases} t_1 = 1 \\ t_2 = 5.8E(s, v_i) \\ \begin{cases} t_3 = \left(\frac{1}{f(s)} - 0.5\right)30.42 + 5.8, \text{CM}_i \text{ with known vulnerability} \\ t_3 = \left(\frac{1}{f(s)} - 0.5\right)65 + 32, \text{CM}_i \text{ with zero} - \text{day vulnerability} \end{cases} \end{cases}, \quad (8)$$

$$\begin{cases} m(s) = 83^*3.5^{4s/2.7} - 82 \\ f(s) = 0.145^*2.6^{2s+0.07} - 0.1 \\ u = (1 - f(s))^{v_i} \\ \bar{f} = f(s)^* v_i \end{cases}, \quad (9)$$

$$\begin{cases} E(s, v_i) = E_1(s, v_i) + E_2(s, v_i) \\ E_1(s, v_i) = \xi\left(\lfloor \bar{f} \rfloor, v_i\right)^*\left(\lceil \bar{f} \rceil - \bar{f}\right) \\ E_2(s, v_i) = \xi\left(\lceil \bar{f} \rceil, v_i\right)^*\left(1 - \lceil \bar{f} \rceil + \bar{f}\right) \\ \xi(b, v_i) = \frac{b}{v_i} + \frac{b(v_i - b)!}{v_i!}\bar{\xi} \\ \bar{\xi} = \sum_{t=2}^{v_i - b + 1}\left[\frac{t(v_i - t + 1)!}{(v_i - b - t + 1)!(v_i - t + 1)}\right] \end{cases}, \quad (10)$$

where $Beta_{\xi,\ \theta}(s)$ is a Beta distribution curve fitting the attacker's skill at different levels s, m is the number of exploitable vulnerabilities; $s \in [0,1]$ is the skill level factor; E is the number of estimated attack attempts; u and ξ are auxiliary variables; and $\lceil \bar{f} \rceil$ and $\lfloor \bar{f} \rfloor$ represent the ceiling and floor of $\bar{f}$, respectively.

2.2.2 MTTC assessment considering network vulnerability

The MTTC is used to estimate the average frequency of cyberattacks on the components of power systems. It measures

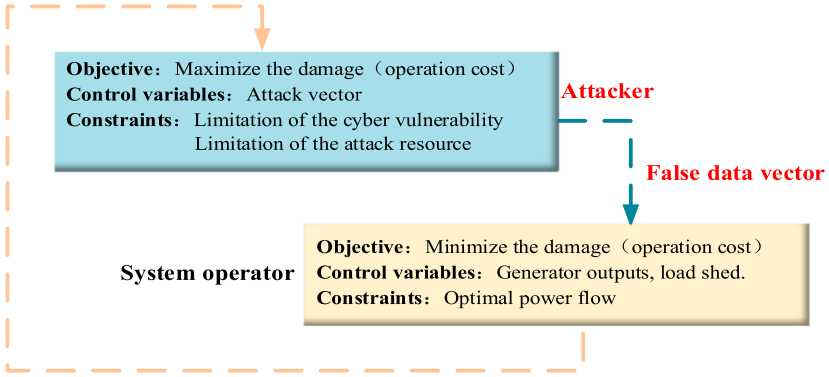

FIGURE 3
Immediate LR attack model considering cyber vulnerability.

the efforts (represented by time) an attacker spends for a successful attack in a statistical form. The MTTC of the LR attack aiming at the communication line can be divided into two parts: the MTTC of SG_j and G, which are modeled as follows:

$$MTTC_d\left(SG_j\right) = \frac{\sum_{i\in\mathcal{I}\left(SG_j\right)} T_{d,i}\left(CM_i\right)\cdot p_d\left(CM_i \wedge SG_j\right)}{p_d\left(SG_j\right)}, \quad (11)$$

where $T_{d,i}(CM_i)$ is the mean time to compromise of CM_i and $p_d(SG_j \wedge CM_i)$ is the probability of the intruder reaching SG_j by invading CM_i, which can be calculated by (2). $p_d(SG_j)$ is the overall probability of SG_j, calculated by (3).

According to the "AND" relationship between SG_j, the MTTC of G is denoted as follows:

$$MTTC_d\left(G\right) = \sum_{j=1}^{\mathcal{J}} MTTC_d\left(SG_j\right). \quad (12)$$

The MTTC model quantitatively evaluates the cost of intruding into communication links of substations through cyber vulnerabilities. In practice, the intruder inevitably has limited attack time to intrude into communication links to inject false data. Hence, from the attacker's perspective, it is necessary to model the LR attack model considering the impact of cyber vulnerability.

3 Bi-level model of LR attack considering cyber vulnerability

From the intruder's perspective, LR attacks are classified into immediate and delayed attacking goals. The immediate LR attack aims to maximize the system's operating cost. A two-layer model representing the behavior of the attacker and operator in Figure 3 is proposed to identify the attack scenario with maximum operating cost, considering multiple restrictions of cyber vulnerability, attack resources, and power flow constraints (Liu et al., 2016). The upper layer represents the attacker, who constructs an attack vector that maximizes the operation cost of the power system. The result of the attack vector is delivery to the lower layer. The lower layer represents the operator, who dispatches the generator output and load shedding to mitigate the impact of the attack decision.

This paper makes the following assumptions about the characteristics of attackers and operators, which are reasonable (Liang et al., 2015):

1) Power system employees may leak power network configuration due to financial interests and revenge behavior.
2) Load measurements are attackable. In power systems, loads are constantly changing. The load measurement should not deviate far from their actual values to prevent attacks from being detected.
3) The measurement of the generator output is not a feasible attacking variable because the integrity of the generator output can be easily verified by communication between the system control center and the power plant.
4) The bus injection measurement of zero-injection buses cannot be attacked. Zero-injection buses have neither generation nor load connection, so LR attacks cannot be carried out through such buses.

3.1 The upper-level problem

The upper-level problem is constructed from the attacker's perspective, aiming to maximize the generation and load shedding costs by the injected bus power.

$$\max_{\Delta \boldsymbol{D}} \sum_{g=1}^{N_g} c_g P_g^* + \sum_{d=1}^{N_d} cs_d S_d^*, \quad (13)$$

$$\text{s.t.}\delta_{t,d} = 1 \Leftrightarrow T - t_d \geq 0 \forall d, \quad (14)$$

$$\sum_{d=1}^{N_d} \Delta D_d = 0, \quad (15)$$

$$-\tau D_d \delta_{t,d} \leq \Delta D_d \leq \tau D_d \delta_{t,d} \forall d, \quad (16)$$

$$\Delta D_d = 0 \Leftrightarrow \delta_{D,d} = 0 \forall d, \quad (17)$$

$$\sum_{d=1}^{N_d} \delta_{D,d} \leq R. \quad (18)$$

Constraint (14) indicates whether intruders can successfully invade the communication link, where T is the limited attacking time of the intruder and t_d is the value of $MTTC_d$ calculated based on cyber vulnerabilities in the communication link between the substation of load bus d and the control center. Constraints

(15)–(16) ensure that falsified load measurements can be injected successfully. It is necessary to ensure that the sum of bus loads remains unchanged before and after the attack and that the load change is within a specific range. The integer variable $\delta_{t,d}$ binds constraint condition (16). Constraint (17) models the logical relationships of the attack vector. In addition, limited by attack resources, the communication links that an attacker can invade simultaneously should not exceed the limit, represented by (18).

3.2 Lower-level problem

$$\{\boldsymbol{P}^*, \boldsymbol{S}^*\} = \arg\left\{ \mathrm{Min}_{\boldsymbol{P},\boldsymbol{S}} \sum_{g=1}^{N_g} c_g P_g + \sum_{d=1}^{N_d} cs_d S_d \right\}, \tag{19}$$

$$s.t. \sum_{g=1}^{N_g} P_g = \sum_{d=1}^{N_d} (D_d - S_d), \tag{20}$$

$$\boldsymbol{PL} = \boldsymbol{SF} \cdot \boldsymbol{KP} \cdot \boldsymbol{P} - \boldsymbol{SF} \cdot \boldsymbol{KD} \cdot (\boldsymbol{D} + \Delta \boldsymbol{D} - \boldsymbol{S}), \tag{21}$$

$$-PL_l{}^{\min} \le PL_l \le PL_l{}^{\max} \ \forall l, \tag{22}$$

$$P_g{}^{\min} \le P_g \le P_g{}^{\max} \ \forall g, \tag{23}$$

$$0 \le S_d \le D_d + \Delta D_d \ \forall d. \tag{24}$$

Lower-level model constraints (19)–(24) can represent the SCED model, which responds according to the decision variables ΔD determined by the upper-level model. Constraint (20) is the power balance constraint of the system. Constraint (21) is the line power flow constraint. Constraints (22)–(24) are the bounds of rated line capacity, generator output, and load shedding, respectively.

In the upper-level problem, Eqs (14) and (17) can be transformed into a mixed integer linearized form. For Eq. (14), we linearize it using the big M method (Yuan et al., 2011; Che et al., 2019), which is (25). Eq. (17) can be linearized in the same way.

$$\begin{cases} (T - t_d)/M \le \delta_{t,d} \le 1 + (T - t_d)/M \\ 0 \le |(T - t_d)| + (T - t_d) \le M \cdot \delta_{t,d} \\ 0 \le |(T - t_d)| - (T - t_d) \le M \cdot (1 - \delta_{t,d}) \\ \delta_{t,d} \in \{0, 1\} \end{cases} \forall d. \tag{25}$$

Replacing the lower-level optimization problem with the Karush–Kuhn–Tucker (KKT) optimal condition can transform the bi-level model into an equivalent single-level mixed integer programming model. The resulting single-level MILP problem can be solved by commercial solvers, such as CPLEX and Gurobi.

4 Quantitative analysis

In order to reflect the impact of the LR attack on the operation cost of the power system, the system parameters of the IEEE 14-bus system are modified. $PL_{1-2}{}^{\max}$ is set to 160 MW, and $PL^{\max}$ of other lines is set to 60 MW. Other configuration data settings are obtained from MATPOWER 6.0 (Zimmerman and Murillo-Sánchez, 2016). The cost of the unmet demand load is set as cs_d = 100 $/MWh. Generator parameters are shown in Table 2. The fabricated magnitude ratio of load measurement is limited at τ = 50%.

The IEEE 14-bus system is used to investigate the impact of LR attacks. The data of substations corresponding with buses are transmitted to the control center through communication links between the substations and the control center. Therefore, the system has 14 communication links, which can be utilized to inject false data through different cyber vulnerabilities.

TABLE 2 Generator parameters.

Number	1	2	3	4	5
Gen. bus	1	2	3	6	8
$P^{\min}$ (MW)	0	0	0	0	0
$P^{\max}$ (MW)	300	50	30	50	20
c (/MWh)	20	30	40	50	35

Figure 4 shows the power system and LR attack model. On the left side of the figure is the topology of the IEEE 14-bus system, and on the right is the attacker's LR attack process on the corresponding substation. The proposed LR attack includes five main steps. The first step is to obtain the measurements of buses. Then, the cost evaluation of intruding into communication links through cyber vulnerabilities is implemented. The evaluation flow of communication links of buses 4, 5, 7, and 8 is taken an example. Later, considering the costs of intruding communication links, the proposed LR attack model solves the attack vector, limited by attack time and resources. Finally, by injecting the solved attack vector, the misled non-optimal operation instruction of generator output and load shedding is implemented by power systems through physical control.

4.1 Cyber vulnerability evaluation of communication links

Five known vulnerabilities, namely, file transfer protocol (ftp), denial of service (dos), the anomaly of buffer overflow (bof), cross-site scripting (xss), and execution code overflow (eco), may exist in countermeasures of communication links (CVE Database, 2023). Due to the uncertainties of zero-day vulnerabilities, for demonstration, it is assumed that no more than five zero-day vulnerabilities may exist in countermeasures of communication links.

4.1.1 Estimates of $T_{d,\ i}(v_i)$ with different types and numbers of vulnerabilities

According to Eq. (5), the skill level, s, of the attacker will influence the compromise time, and s is represented by a Beta distribution with (?, ?) = (1.5, 2.0). The total number of vulnerabilities, ?, was fixed to 9,447, which can be updated based on the available vulnerability database of power system networks (Zieger et al., 2018). Table 3 shows the $T_{d,\ i}(v_i)$ with 1–5 known and zero-day vulnerabilities.

It can be seen from Table 3 that the time of exploiting zero-day vulnerabilities is significantly longer than the time for known vulnerabilities. With the increase in vulnerabilities, $T_{d,\ i}(v_i)$ gradually decreases. This is in line with the reality that as the number of vulnerabilities increases, it gives the intruder more opportunities to choose the attack path, which can reduce the time needed to carry out a cyberattack successfully.

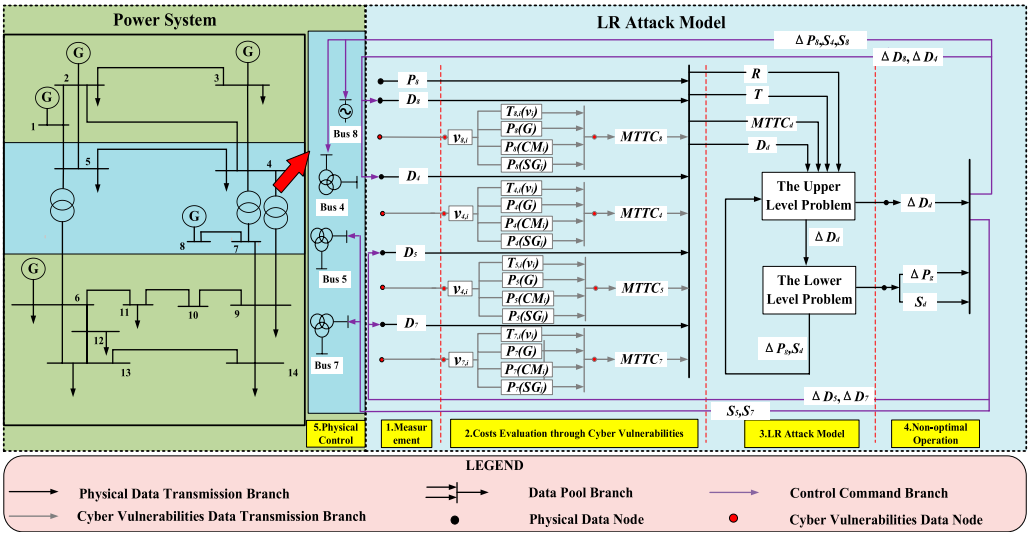

FIGURE 4
Proposed LR attack model for power systems.

TABLE 3 $T_{d,\ i}(v_i)$ with known and zero-day vulnerabilities.

v_i	1	2	3	4	5
Known vulnerability (days)	120.93	100.93	86.87	76.48	68.5
Zero-day vulnerability (days)	271.42	224.93	191.93	165.27	144.94

TABLE 4 CVSS scores of vulnerabilities.

Vulnerability	Zero-day	ftp	dos	bof	xss	eco
CVSS score	0.8	6.4	5.0	6.8	4.5	7.5

TABLE 5 MTTC to invade each communication link.

Bus	1	2	3	4	5	6	7
MTTC (days)	279.9	243.7	198.5	320.5	380.5	356.8	289.4
Bus	8	9	10	11	12	13	14
MTTC (days)	205.6	231.3	328.2	489.5	409.8	231.6	188.9

4.1.2 Estimation of the MTTC on each communication link

For estimating the MTTC, the CVSS scores should be assigned in advance, which can be evaluated based on the access vector, access complexity, and authentications with different grades (Zhang et al., 2015). The CVSS scores for cyber vulnerabilities in countermeasures of communication links are listed in Table 4.

Intruders can find the vulnerability distribution in countermeasures through source code or automation analysis tools. For demonstration, in this paper, the number of these vulnerabilities in countermeasures of communication links is set to a random number of 1–5. According to the MTTC assessment method in Section 2.2.2, the estimated MTTC of each communication link can be obtained, as shown in Table 5.

As seen in Table 5, although the intruder has the same overall goal among these communication links, the MTTC of each communication link is different because the distribution of cyber vulnerabilities in countermeasures of communication links is dissimilar. The intrusion time of bus 14 is the shortest, 188.9 days, which means the intruder can easily tamper with the load measurement in its communication link. The intrusion time of bus 11 is the longest, 489.5 days, indicating that the LR attack executed through fabricating the load measurement of bus 11 needs the maximum attacking time.

4.2 Impact analysis of the LR attack model considering cyber vulnerabilities

The LR attack impact can be obtained by solving the proposed bi-level model of LR attack in Section 3. The most hazardous scenario in the LR attack considering cyber vulnerabilities is subject to the available attack time and resources. The intruder's available attack time decides the number of intruded communication links. Meanwhile, the available attack resources decide the number of simultaneously falsified measurements of load buses.

4.2.1 LR attack with the different available attack times

Table 6 shows the most damaging LR attack scenarios with the limitation of the different available attack times, T, and the static attack resource, R = 4. Although the intruder has the attack resource to falsify four load-bus measurements simultaneously, the attack time T = 200 limits the intruder from attacking indispensable communication links. According to Table 5, with T = 200, the intruder only has time to attack two

TABLE 6 LR attacks with different attack time limitations.

Attacking time T	0 (SCED)	200	300	400	500
Attacked bus	--	3 and 14	2, 3, 9, and 14	2, 3, 4, and 9	2, 3, 4, and 9
No. of attacked buses	0	2	4	4	4
Load shedding (MW)	0	0	9.35	19.12	19.12
Operation cost ($/h)	6205.6	6252.7	6828.3	7609.6	7609.6

TABLE 7 Fabricated quantities of LR attacks with T = 300 days.

Number of bus	Measurement	Fabricated quantity (MW)
2	P_2^{inj}	10.85 (50%)
3	P_3^{inj}	−33.05 (35.1%)
9	P_9^{inj}	14.75 (50%)
14	P_{14}^{inj}	7.45 (50%)

TABLE 8 Fabricated quantities of LR attacks with T = 500 days.

Number of bus	Measurement	Fabricated quantity (MW)
2	P_2^{inj}	10.85 (50%)
3	P_3^{inj}	−47.1 (50%)
4	P_4^{inj}	21.5 (45%)
9	P_9^{inj}	14.75 (50%)

communication links, i.e., communication links of substations corresponding with buses 3 and 14. By falsifying load measurements of buses 3 and 14, an increase of 4.1 $/h in the operation cost and no load shedding occurs. The more attack time the intruder has, the more communication links can be attacked. When the attack time $T \geq 300$ days, the intruder can attack enough communication links to falsify four load-bus measurements. However, due to the cyber vulnerability distribution, the attack scenario causing the maximum operation cost and load shedding of 7609.6 $/h and 19.12 $/h, respectively, happens when the attack time $T \geq 400$ days, for the reason that the communication link that corresponds with bus 4 needs 320.5 days to invade.

Table 7 shows the fabricated quantities of measurements in intruded communication links of substations corresponding with load buses. It can be seen that the sum of fabricated load injections is zero. Table 7 shows that when T = 300 days, the fabricated quantities of load measurements of substations at buses 2, 9, and 14 reach the ratio limitation of the fabricated magnitude. The falsified load injection of bus 3 is the maximum, which tries to transfer the load at buses 2, 9, and 14 to bus 3. Table 8 shows that when T = 500 days, the fabricated quantities of buses 2, 3, and 9 reach the maximum ratio limitation. The falsified load injection of bus 3 is the maximum, which tries to transfer the load on buses 2, 4, and 9 to bus 3.

4.2.2 LR attack with different attack resource limitations

Table 9 shows the most damaging LR attack scenarios with the limitation of different available attack resources, R, and the static attack time, T = 300. As seen from Table 5, when the attack time T = 300, the intruder has time to attack five substations' communication links corresponding with load buses 2, 3, 9, 13, and 14. The available attack resources limit the number of simultaneously falsified load measurements. The more available attack resources the intruder has, the more the measurements of buses with load can be falsified simultaneously. When the attack resource, R = 1, the LR attacks cannot be implemented because the LR attack model's constraints cannot be satisfied. With the increase of attack resources from 2 to 5, the operation cost increased from 6351.4 $/h to 7244.9 $/h, and the load shedding increased from 0 MW to 14.56 MW. Although the intruder has more attack resources with R = 6, the intruder does not have sufficient time to attack enough communication links due to the attack time limitation. Therefore, the operation cost and load shedding of R = 6 are the same as the results of R = 5.

4.3 Comparison of LR attack models

Table 10 compares the scheduling results and operating costs of the SCED without attack and different LR attack models. As shown in Table 10, it can be found that under the SCED without attack, the total operation cost is 6205.6 $/h, and no load shedding occurs. The attack scenario in the traditional LR attack causes an operation cost of 7609.6 $/h and a load shedding of 19.12 MW. However, when cyber vulnerabilities in communication links are considered, the attack scenario in the traditional LR attack may not be achieved due to the limitation of attacking time to occupy essential communication links to launch an attack. Therefore, with a limited attack time of 300 days, a more practical attack scenario can be found by the LR attack model considering cyber vulnerabilities, where the operation cost is 6828.3 $/h and a load shedding of 9.35 MW occurs. With a limited attack time of 500 days, the impacts of the LR attack considering cyber vulnerabilities and the traditional LR attack are the same. The reason for the same attack impact is that, based on Table 5, the attack time of 500 days means that the attacker has enough time to intrude into communication links of all buses with load to inject falsified data, which is unified with the assumption in the traditional LR attack that all buses with load can be intruded. Hence, the attack scenario found by the traditional LR attack model is just a case in the proposed bi-level LR attack model with sufficient attack time.

TABLE 9 LR attacks with different attack resource limitations.

Attacking resources R	1	2	3	4	5	6
Attacked bus	--	2 and 9	2, 3, and 9	2, 3, 9, and 14	2, 3, 9, 13, and 14	2, 3, 9, 13, and 14
No. of attacked buses	0	2	3	4	5	5
Load shedding (MW)	0	0	2.43	9.35	14.56	14.56
Operation cost ($/h)	6205.6	6351.4	6449.5	6828.3	7244.9	7244.9

TABLE 10 Comparison of the scheduling results and operating costs of the SCED without attack and different LR attack models with $R = 4$.

		LR attacks with T = 300 days	LR attacks with T = 500 days	Traditional LR attacks	Original SCED
Generation dispatch on gen. bus (MW)	1	199.65	189.88	189.88	180.17
	2	0	0	0	45.11
	3	30	30	30	13.72
	6	0	0	0	0
	8	20	20	20	20
Total generation (MW)		249.65	239.88	239.88	259
Operation cost ($/h)		6828.3	7609.6	7609.6	6205.6

5 Conclusion

This paper studied the modeling and impacts of LR attacks by considering cyber vulnerabilities in power systems. Unlike the existing works about LR attacks in power systems, the costs of falsifying load measurements through intruding into communication links of substations are quantitatively evaluated by the MTTC and considered in the proposed bi-level LR attack model. The proposed model can find the practical attack scenario because the intruder inevitably faces attack time limitations. Finally, a quantitative analysis was conducted to evaluate cyber vulnerabilities and LR attack impact on power systems. The cyber vulnerabilities will impact the available attack vector. Moreover, the attack scenario of the existing LR attack model is verified as an attack vector found by the proposed bi-level LR attack model with sufficient attack time to intrude into all communication links of substations.

Data availability statement

Publicly available datasets were analyzed in this study. These data can be found at: MATPOWER, a MATLAB power system simulation package [on-line], available at: http://www.pserc.cornell.edu/matpower/.

Author contributions

XS, HG, and YC contributed to the conception and design of the study. HG organized the mathematical model. WW and BY performed the statistical analysis. XS and HG wrote sections of the manuscript. XS and YC contributed to the manuscript revision and proofreading. All authors contributed to the article and approved the submitted version.

Funding

The authors are grateful for the financial support from the National Natural Science Foundation of China (Grant No. 52107070), the Provincial Natural Science Foundation of Hunan (Grant No. 2022JJ40490), the National Key R&D Program of China (Grant No. 2022YFE0129300), and the Research Foundation of the Education Department of Hunan Province (Grant No. 21B0325).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Bahrami, M., Fotuhi-Firuzabad, M., and Farzin, H. (2020). Reliability evaluation of power grids considering integrity attacks against substation protective IEDs. *IEEE Trans. Industrial Inf.* 16 (2), 1035–1044. doi:10.1109/tii.2019.2926557

Che, L., Liu, X., Li, Z., and Wen, Y. (2019). False data injection attacks induced sequential outages in power systems. *IEEE Trans. Power Syst.* 34, 1513–1523. doi:10.1109/tpwrs.2018.2871345

CVE Database (2023). CVE details. Available at: https://www.cvedetails.com/index.php (Accessed March 23, 2023).

Deng, R., Xiao, G., Lu, R., Liang, H., and Vasilakos, A. V. (2016). False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Trans. Industrial Inf.* 13 (2), 411–423. doi:10.1109/tii.2016.2614396

Gao, S., Lei, J., Wei, X., Liu, Y., and Wang, T. (2022). A novel bilevel false data injection attack model based on pre-and post-dispatch. *IEEE Trans. Smart Grid* 13 (3), 2487–2490. doi:10.1109/tsg.2022.3156445

Lau, P., Wang, L., Liu, Z., Wei, W., and Ten, C. W. (2021). A coalitional cyber-insurance design considering power system reliability and cyber vulnerability. *IEEE Trans. Power Syst.* 36 (6), 5512–5524. doi:10.1109/tpwrs.2021.3078730

Li, T., Chen, L., Jensen, C. S., Pedersen, T. B., Gao, Y., and Hu, J. (2022). "Evolutionary clustering of moving objects," in Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, May 2022 (IEEE), 2399–2411.

Li, Y., Zhang, H., Liang, X., and Huang, B. (2019). Event-triggered-based distributed cooperative energy management for multienergy systems. *IEEE Trans. Industrial Inf.* 15 (4), 2008–2022. doi:10.1109/tii.2018.2862436

Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2016). The 2015 Ukraine blackout: implications for false data injection attacks. *IEEE Trans. Power Syst.* 32 (4), 3317–3318. doi:10.1109/tpwrs.2016.2631891

Liang, J., Sankar, L., and Kosut, O. (2015). Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Trans. Power Syst.* 31 (5), 3864–3872. doi:10.1109/tpwrs.2015.2504950

Liu, S., Yu, J., Deng, X., and Wan, S. (2022). FedCPF: an efficient-communication federated learning approach for vehicular edge computing in 6G communication networks. *IEEE Trans. Intelligent Transp. Syst.* 23 (2), 1616–1629. doi:10.1109/tits.2021.3099368

Liu, X., Bao, Z., Lu, D., and Li, Z. (2015). Modeling of local false data injection attacks with reduced network information. *IEEE Trans. Smart Grid* 6 (4), 1686–1696. doi:10.1109/tsg.2015.2394358

Liu, X., and Li, Z. (2016). False data attacks against AC state estimation with incomplete network information. *IEEE Trans. Smart Grid* 8 (5), 2239–2248. doi:10.1109/tsg.2016.2521178

Liu, X., and Li, Z. (2014). Local load redistribution attacks in power systems with incomplete network information. *IEEE Trans. Smart Grid* 5 (4), 1665–1676. doi:10.1109/tsg.2013.2291661

Liu, X., Li, Z., Shuai, Z., and Wen, Y. (2016). Cyber attacks against the economic operation of power systems: A fast solution. *IEEE Trans. Smart Grid* 8 (2), 1023–1025. doi:10.1109/tsg.2016.2623983

Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* 14 (1), 1–33. doi:10.1145/1952982.1952995

Pliatsios, D., Sarigiannidis, P., Lagkas, T., and Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Commun. Surv. Tutorials* 22 (3), 1942–1976. doi:10.1109/comst.2020.2987688

Sommestad, T., Ekstedt, M., and Nordstrom, L. (2009). Modeling security of power communication systems using defense graphs and influence diagrams. *IEEE Trans. Power Deliv.* 24 (4), 1801–1808. doi:10.1109/tpwrd.2009.2028796

Tan, S., Song, W. Z., Stewart, M., Yang, J., and Tong, L. (2016). Online data integrity attacks against real-time electrical market in smart grid. *IEEE Trans. Smart Grid* 9 (1), 313–322. doi:10.1109/tsg.2016.2550801

Ten, C. W., Liu, C. C., and Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans. Power Syst.* 23 (4), 1836–1846. doi:10.1109/tpwrs.2008.2002298

Xiang, Y., Ding, Z., Zhang, Y., and Wang, L. (2016). Power system reliability evaluation considering load redistribution attacks. *IEEE Trans. Smart Grid* 8 (2), 889–901. doi:10.1109/TSG.2016.2569589

Yang, L., Sun, Q., Zhang, N., and Li, Y. (2022). Indirect multi-energy transactions of energy internet with deep reinforcement learning approach. *IEEE Trans. Power Syst.* 37 (5), 4067–4077. doi:10.1109/tpwrs.2022.3142969

Yuan, Y., Li, Z., and Ren, K. (2011). Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid* 2 (2), 382–390. doi:10.1109/tsg.2011.2123925

Zhang, F., and Yang, Q. (2022). False data injection attack detection in dynamic power grid: A recurrent neural network-based method. *Front. Energy Res.* 10, 1005660. doi:10.3389/fenrg.2022.1005660

Zhang, Y., Wang, L., Xiang, Y., and Ten, C. W. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Trans. Smart Grid* 6 (4), 1707–1721. doi:10.1109/tsg.2015.2396994

Zhang, Y., Xiang, Y., and Wang, L. (2017). Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. *IEEE Trans. Smart Grid* 8 (5), 2343–2357. doi:10.1109/tsg.2016.2523515

Zieger, A., Freiling, F., and Kossakowski, K. P. (2018). "The β-time-to-compromise metric for practical cyber security risk estimation," in Proceedings of the 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF), Hamburg, Germany, May 2018 (IEEE), 115–133.

Zimmerman, R., and Murillo-Sánchez, C. (2016). MATPOWER 6.0 user's manual. Available at: http://www.pserc.cornell.edu/matpower/manual.pdf (Accessed October 8, 2020).

Nomenclature

Indices and sets	
n	Bus index
d	Load bus index
l	Transmission line index
g	Generator index
CM	Countermeasures in LR attack
SG	Sub-goal in LR attack
G	Goal in LR attack
$I(SG_j)$	Set of countermeasures CM_i needed to defeat to achieve SG_j
J	Set of the LR attack sub-goals SG_j
CVSS	Common Vulnerability Scoring System
MTTC	Mean time to compromise
Parameters	
M	Sufficiently large positive constant
ε	Sufficiently small positive constant
τ	Bound of $\Delta D_d/D_d$ for each load d
c_g	Generation cost (/MWh) of generator g
cs_d	Load shedding cost (/MWh) of load bus d
D_d	Actual value of load bus d (in MW)
KD	Bus–load incidence matrix
KP	Bus–generator incidence matrix
N_n	Number of buses
N_d	Number of load buses
N_g	Number of generators
N_l	Number of transmission lines
P_g^{max}, P_g^{min}	Maximum and minimum generation outputs (in MW) of generator g
PL_l^{max}	Capacity (in MW) of the transmission line
R	Attacking resources
T	Limited attacking time of the intruder
SF	Shifting factor matrix
σ	Number of total vulnerabilities
Variables	
$P_d(CM_i)$	Probability that CM_i is reached for the communication link of substation at bus d
$P_d(SG_j)$	Probability that SG_j is reached for the communication link of substation at bus d
$P_d(G)$	Probability that G is reached for the communication link of substation at bus d
$T_{d,i}(v_i)$	Compromise time in CM_i of the communication link of substation at bus d
v_i	Number of known vulnerabilities of the component
s	Skill factor of the intruder
ΔD_d	Attack on the measurement (in MW) of load d
ΔP_g	Output power change of generator g
PL_l	Power flow (in MW) of transmission line l
P_g	Generation output (in MW) of generator g
S_d	Load shedding (in MW) of load d
t_d	Compromise time of load d
$\delta_{D,d}$	Binary variable 1, if load d is attacked
$\delta_{t,d}$	Binary variable 1, if load d could be attacked
t_1, t_2, t_3	The mean time of three sub-processes
P_1, P_2, P_3	The probabilities of three sub-processes