UDC 004.056

Mitigating the impact of cyber incidents such as load altering attacks

Leonid Galchynsky [1], Daria Kosaryk [2], and Vladyslav Lychyk [1]

[1] *National Technical University «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine*

[2] *Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine*

Abstract

Modern power systems are constantly exposed to cyberattacks that threaten to disable them and cause serious damage and even destruction. The cyber threat factor is nowadays on a par with such traditional threats as natural disasters, fires, and other destructive phenomena. Therefore, cyber threats raise the question of considering protection against them as a factor of power system sustainability necessary for survival, which should now be considered in the context of cyber resilience. This paper considers the issue of finding a solution to mitigate the harmful effects on the power system of one of the types of cyberattacks, namely, Load Altering Attacks (LAA). The danger of such an attack is that, taking advantage of the weak protection of a large number of IoT clients, an attacker can conduct a coordinated attack on a large number of compromised clients and suddenly change the load in the power grid. As a result, not only users will suffer, but also the basic equipment of the power grid itself, in particular, power generators. This paper proposes a solution that, by optimizing the regulator mode of the power generator, can significantly mitigate the harmful effects of LAA attacks.

Keywords: Cyber resilience, power grid, power generator, regulator, LAA, LQR, Nelder–Mead algorithm.

Introduction

A modern power system is a complex heterogeneous network that combines the actual technological aspects of the power system and information systems [1], which provide real–time data collection from various digital sensors in power systems and data on power equipment assets [2, 3], and IT is used to monitor, analyze and calculate this data for intelligent and automatic control of power systems [4]. The power grid includes the entire process of power generation, transmission, distribution, consumption, dispatching, and communication of power systems [5]. However, along with the undoubted improvement of management due to the rapid development of IT technologies, the structure and operation of networks are becoming more complex, and the risks of safe operation of power systems are becoming more serious. That is why the issue of reliable energy supply now depends not only on the level of management and the impact of usual global external factors, such as weather conditions, accidents, natural disasters, etc. The cyber threat factor has grown to the level of global threats in recent years and should be considered in the context of cyber resilience, where countering cyber attacks should be considered as one of the important components of the overall system survival (resilience) [6]. The researchers' analysis shows that current approaches to cyber defense of electric power companies need to be improved [7]. Modern power grids are very complex, and cyberattacks can occur in any link of the power grid. There are many types of cyberattacks in the power grid, including integrity violations [8], availability interference [9], exploits, worms [10], DoS [11], false data entry [12], password theft by keyloggers, and other cyberattacks [13]. The implementation of these attacks has certain specifics in the power system environment, and each of them requires a detailed consideration. However, it can be noted that all of them have common features with attacks on other objects. However, there is one type of cyberattack that is specific to power grids – a Load Altering Attack (LAA).

Figure 1 shows the diagram of an attack of the LAA type. A load shifting attack is a specific cyberattack targeting the consumption sector of the power grid [14]. However, this is not the only goal of such an attack. The attackers are aiming to disrupt power supply in the grid and even disable technological equipment up to complete destruction. Based on this, it is advisable to raise the question not only and not so much about detecting and neutralizing a cyberattack of the LAA type, but to put the survival of the technological infrastructure of the power system, in particular the one that provides power generation, at the forefront. That is, the issue of cyber defense is being switched to the issue of cyber resilience. If there is a group of vulnerable remote–controlled loads in the power grid, LAA can damage the power system by controlling and changing vulnerable loads to overload the circuit or significantly deviate power system frequencies from the nominal value [15]. A number of studies have revealed the vulnerability of the Internet of Things (IoT) to attackers [16, 17]. These studies have demonstrated that an attacker can hack a wide range of IoT devices directly or through mobile applications designed for them. However, almost all previous studies aimed to identify the impact of these vulnerabilities on personal privacy and security. However, after the Mirai botnet distributed denial of service (DDoS) attack, which compromised 600,000 devices targeting victim servers, it was specifically shown that the threat of an LAA attack could become a reality for power grids. At the same time, the number of consumers using IoT technologies is steadily growing by 7 million every day, and the number of Mirai botnet clones is growing out of control. As a result, a number of researchers [18] have identified one specific way in which an attacker can use compromised IoT devices to disrupt critical infrastructure such as power grids. This method consists in the ability to simultaneously turn on or off a large number of devices powered by electricity in a certain region, because IoT device vendors do not invest in strengthening the cybersecurity of their products.

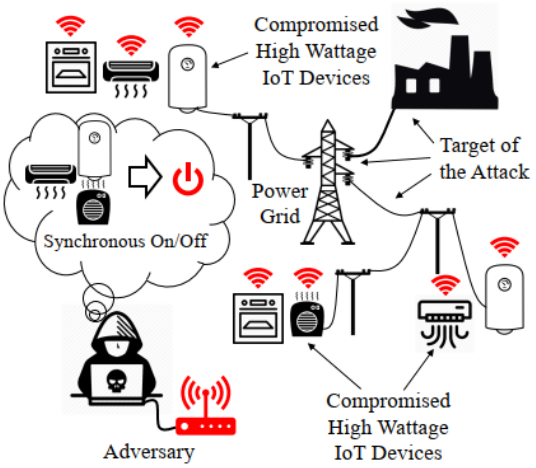

Figure 1: Scheme of a variable load attack (LAAs) [18]

According to the classification [18], attacks can be divided into three types:

- Frequency instability attacks: A sudden increase (or decrease) in electricity demand – possibly due to the synchronized switching on or off of many high–powered IoT devices – leads to an imbalance between supply and demand. This imbalance instantly generates a sudden drop in the voltage frequency in the system and this can lead to a frequency threshold being exceeded, causing generators to shut down and potentially a large–scale blackout.
- Attacks that cause line failures and lead to cascading failures: if the imbalance in supply and demand after the attack is not significant, the system frequency is stabilized by the main generator controller. Since the transmission of electricity in the grid follows Kirchhoff's laws, the grid operator is practically unable to influence the change in power flows after the primary controllers react. Thus, even a small increase in demand can lead to line overload and failures. This can especially happen during peak loads when reserve capacity is limited. These initial line failures can consequently lead to further line failures, known as cascading failures [19].
- Attacks that increase operating costs due to an unexpected sharp

change in demand set by the standard day–ahead load forecast. This forces the grid operator to buy additional electricity from ancillary services at the expense of backup generators, which usually have higher prices than generators that are planned for the day ahead.

- In any case, these attacks lead to a decrease in the quality of electricity supply. The quality of electricity in different countries is determined by the relevant laws and regulations. In Ukraine, the requirements for electricity quality are defined by DSTU EN 50160:2014 "Characteristics of the supply voltage in general–purpose electrical networks" (DSTU EN 50160:2014). The frequency of the supply voltage for low voltage networks for systems synchronously connected to the IPS of Ukraine should be within the following limits: – 50 Hz ± 1% for 99.5% of the time per year and 50 Hz + 4% (– 6%) for 100% of the time. The indicator of long–term flicker (flickering) caused by voltage fluctuations for low voltage networks should be less than or equal to 1 for 95% of the monitoring time.
- At the same time, the International European Standard CENELEC EN 50160:2010 and was adopted in Ukraine on May 20, 2014 and entered into force on October 1 of the same year. This standard sets the voltage at 400 V / 230 V ±10% (three–phase/single–phase network) at a current frequency of 50 Hz.

However, the requirements of power quality standards, while setting certain limits for their violations, do not explicitly provide estimates of the damage that may be caused to both consumers and the power system itself, depending on the size of the deviation of the power supply parameters from the nominal ones. A partial answer to the quantification of deviation damage is given in a US government analytical report based on the materials of a large–scale blackout in 2003 [20]. The 2003 blackout was not triggered by a cyberattack, but the materials collected provided real data on the blackout and its consequences, regardless of the cause. At the same time, the scale and damage from a blackout caused by an LAA attack may be comparable. Figure 2 shows a picture of events that can occur in the power system network due to significant disturbances based on real data. The black color shows a significant change in frequency. The points of turbine reverse stroke with subsequent shutdown are shown in red. The analysis of data on the dynamics and consequences of blackouts allows us to rank losses depending on the deviation of the nominal frequency on an interval scale. Table 1 presents the damage ranges when changing frequencies.

Table 1

Frequency ranges recorded during blackout and power grid damage

Frequency deviation	Damage
>+3 Hz	Damage to grid equipment and users.
>+1,5 Hz	Damage to user equipment. Switching to the shutdown mode.
+0.5 – +1.5 Hz	Violation of some elements in the user network.
+0.2 – –0.2	Zero–risk zone.
+0.5 – –0.5 Hz	Nominal mode.
–0.5 – –1,5 Hz	The threat of generator equipment.
< –2,5 Hz	Switching to the shutdown mode.
<–3 Hz	Damage to power grid equipment.

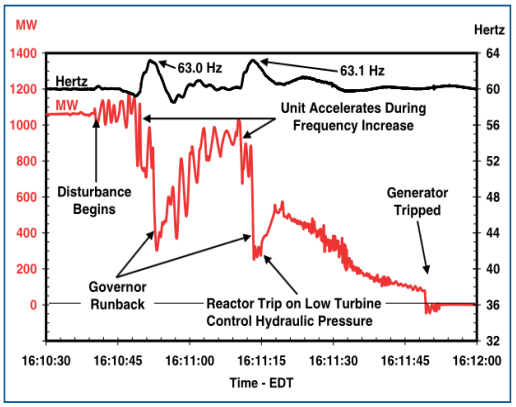

Figure 2: Changes in generation frequency and equipment modes during large–scale blackout [20]

The speed of generators in power systems corresponds to the frequency. If demand exceeds supply, the rotational speed of turbine generators slows down and the kinetic energy of the rotor is transformed into increased electrical power to meet the additional demand. Accordingly, this leads to a drop in the system frequency. This behavior of turbine generators is in accordance with the laws of mechanics and is calculated by the generator's inertia. The primary controller sends a change to the turbine generator actuator, which leads to the restoration of the frequency. Similarly, a supply that exceeds demand causes the generators' rotors to accelerate and the system frequency to increase. Accordingly, the controller sends a control signal to the turbine generator to reduce the frequency

The system frequency reduction/increase cannot be continued for a long time, as serious damage to the generator can occur at frequencies below/above the rated values. If the frequency rises above or below a certain threshold value, the protective relays switch off or completely disconnect the generators. Thus, within a few seconds after the first signs of a frequency change, the primary controller activates and increases/decreases the mechanical input, which stabilizes the generator rotor speed and, accordingly, the system frequency [26]. Although equipment, including power generators, has a certain margin of safety, in the event of significant deviations from the nominal frequency over time, they are at risk of damage and also affect equipment wear. An emergency shutdown avoids fatal consequences for the generator, but it creates a problem for the power grid as a whole, as it can lead to cascading blackouts. Hence the requirement that the generator controller must ensure that the deviation is as low as possible in as short a time as possible.

1. Analysis of recent research and publications

The speed of generators in power systems corresponds to the frequency. If demand exceeds supply, the rotational speed of turbine generators slows down and the kinetic energy of the rotor is transformed into increased electrical power to meet the additional demand. Accordingly, this leads to a drop in the system frequency. This behavior of turbine generators is in accordance with the laws of mechanics and is calculated by the generator's inertia. The primary controller sends a change to the turbine generator actuator, which leads to the restoration of the frequency. Similarly, a supply that exceeds demand causes the generators' rotors to accelerate and the system frequency to increase. Accordingly, the controller sends a control signal to the turbine generator to reduce the frequency

The system frequency reduction/increase cannot be continued for a long time, as serious damage to the generator can occur at frequencies below/above the rated values. If the frequency rises above or below a certain threshold value, the protective relays switch off or completely disconnect the generators. Thus, within a few seconds after the first signs of a frequency change, the primary controller activates and increases/decreases the mechanical input, which stabilizes the generator rotor speed and, accordingly, the system frequency [26]. Although equipment, including power generators, has a certain margin of safety, in the event of significant deviations from the nominal frequency over time, they are at risk of damage and also affect equipment wear. An emergency shutdown avoids fatal consequences for the generator, but it creates a problem for the power grid as a whole, as it can lead to cascading blackouts. Hence the requirement that the generator controller must ensure that the deviation is as low as possible in as short a time as possible.

2. Results and discussion

2.1 Mathematical model of a synchronous generator

For several decades, synchronous generators have been the main sources of electricity in power systems. Consequently, all disturbances in the grid are reflected in the generator's operation. The basic single–line diagram of a single machine, known in the literature as Single Machine Infinite Bus (SMIB), connected to an infinite bus, is shown as in Figure 3. G is the equivalent of a single machine, Et is the voltage of the infinite bus, and re and Xe are the total resistance between the two buses with voltages Et and Eb, respectively.

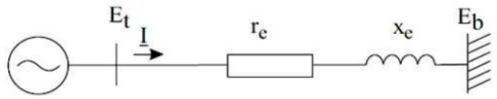

Figure 3: Single Machine to Infinite Bus System single–line diagram [28]

In the SMIB system, if we ignore the stator resistance and the DC component of the stator current, as well as the winding damping effect, the mathematical model of a synchronous generator can be obtained by describing the equation of interaction between the mechanical force of the turbine rotor and the electromotive force of the electric generator stator. To describe the dynamics of a synchronous generator in the SMIB system, the Heffron–Phillips model is generally recognized, based on the idea of dynamic equilibrium between mechanical and electromotive forces. This model can be represented with varying degrees of detail. In this paper, it is enough to focus on the system of three equations, as shown in the classic monograph [29]. Fig. 4 shows a schematic representation of the SMIB in the presence of a regulator.

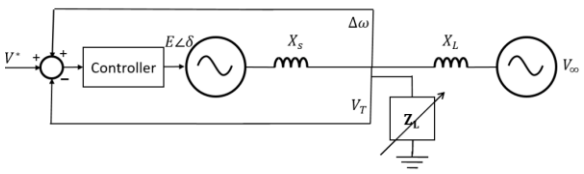

Figure 4: SMIB system with a regulator

From the point of view of control theory, the control scheme looks like the one shown in Figure 5.

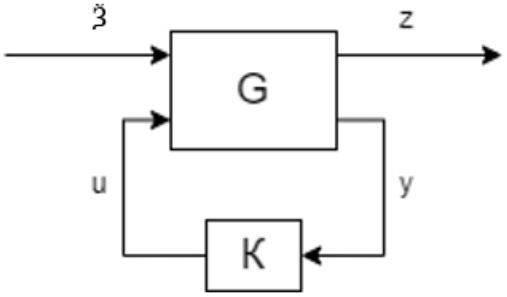

Figure 5: Controlled power generator system with regulator

The system G maintains the desired behavior with the help of the controller K, where u is the control signal, ξ is the disturbance, z is the control output, and y is the measured input.

The third–order Heffron–Phillips model for a synchronous generator is as follows:

$$\begin{bmatrix} \Delta\dot{\omega}_r \\ \Delta\dot{\delta} \\ \Delta\dot{\psi}_{fd} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & 0 & 0 \\ 0 & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} \Delta\omega_r \\ \Delta\delta \\ \Delta\psi_{fd} \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b_{33} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \Delta u \end{bmatrix} + \begin{bmatrix} z_{11} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta \mathrm{M_M} \\ 0 \\ 0 \end{bmatrix} \quad (1)$$

where are the elements of the matrix:

$$a_{11} = -\frac{K_D}{2H},\ a_{12} = -\frac{K_1}{2H},\ a_{13} = -\frac{K_2}{2H},\ a_{21} = \omega_0 = 2\pi f_0,\ a_{32} = -\frac{K_4}{T_{d0}},\ a_{33} = -\frac{1}{K_4 T_{d0}},\ b_{33} = \frac{1}{2H},\ z_{11} = \frac{\omega_0 R_{fd}}{L_{adu}}.$$

For the dynamic system described by (), the state variables are:

$\Delta\omega_0$ – rotor speed deviation, δ – rotor angle, ψ_{fd} – instantaneous value of flow adhesion;

Δu – changing the voltage at the generator terminals is a control; ΔM_M – a change in the generator's electromagnetic torque is a perturbation of the generator's equilibrium.

For complete identification and modeling capability, it is necessary to determine several parameters that are taken as constants for a linear time–invariant dynamic system. In particular, these are:

K_D – damping coefficient, H – coefficient of inertia, ω_0 – nominal rotor angular speed,

R_{fd} – rotor circuit resistance, L_{adu} – stator inductance. K_1 – K_4 known as Heffron–Phillips constants, де – K_1 – Effect of torque angle on electric torque, K_2 – influence of internal voltage on electric torque, K_3 – constant excitation winding, K_4 – the effect of torque angle on the field voltage. For ease of calculation, all values are given in relative units. K_1 до K_4 are the parameters of the generator, and the output can be found in [29]. The values of the constants are given in Table 2.

Table 2

Values of constants for the third-order Heffron-Phillips model [29]

№	Parameter	Value
1	H	4.63
2	Td_0	7.76
3	ω_0	50
4	K_D	0
5	K_1	0.5441
6	K_2	1.2067
7	K_3	0.6584
8	K_4	0.6981
9	R_{fd}	0.0006
10	L_{adu}	1.66

We will now consider the model of a controlled static generator as a dynamic system that is invariant in time. It can be represented in the state space used to synthesize the control system. The matrix equation of the linear model of a synchronous generator in state space is as follows:

$$\dot{x} = Ax + Bu + Z\check{z} \quad (2)$$

where x – vector of internal states of the system, u – vector of control signals, A – state matrix, B – control matrix, Z – disturbance impact matrix. It can be added that in this model, the control vector has only one non-zero component, which corresponds to the voltage to the turbine control actuator, and the disturbance vector is a transformed torque that depends on disturbances outside the bus.

2.2 LAA mitigation model

2.2.1 Building an optimal Kalman controller

Control theory provides a well-developed framework for the analytical design of controllers for linear systems. In particular, we will use the method of optimal controller design (LQR). This method allows you to get the potentially best result when the model parameters are correctly chosen. The linear quadratic regulator (LQR) problem is an optimal control problem with the following formulation. Let the mathematical model of the control object be given:

$$\dot{x} = \dot{} Ax = Ax + Bu \ ; x \in E^n, u \in E^m, t \in [0, \infty], x(0) = d$$

where A, B — matrices with constant components, and the pair (A, B) is stabilized, d — is a given constant vector. We will assume that we are looking for a control law as a linear dependence on the state coordinates:

$$u = K_x,$$

where K — is a constant matrix. The natural question then is: what value of K will give us the best quality of the controller? To do this, let's introduce the integral quadratic functional:

$$J(K) = \int_0^\infty [x^T(t, \mathrm{K})\mathrm{Qx}(t, \mathrm{K}) + u^T(t, \mathrm{K})\mathrm{Ru}(t, \mathrm{K})]dt \quad (3)$$

The matrix Q is sign-positive, and R > 0 is a positive definite symmetric matrix.

Accordingly, the LQR optimization problem takes the form:

$$\min J(K), \quad (4)$$

$K \in S$, where S – a set of matrices of size m x n with variable real components for which the zero equilibrium position of a closed system is asymptotically stable according to Lyapunov. In fact, this is a problem of finding the optimal value in Hilbert space and, as a result, we get a two-point boundary value problem where the state variables are defined at the beginning of the interval and the additional ones (Lagrange multipliers) at the end of the interval.

The solution of this problem leads to a system of Euler's differential equations, from which a linear relationship between the control and the vector of Lagrange multipliers can be obtained, in particular, the optimal control can be expressed through a linear relationship: $\boldsymbol{u}_0(t) = \boldsymbol{R}^{-1}\boldsymbol{B}^T(t)\lambda_0(t)$.

However, this is not enough. Because we do not know the values of the Lagrange multipliers. But if there is such a matrix P(t), that for any solution {x(t), λ(t)} of the Euler system, the identity is fulfilled:
(t)= –P(t)x(t), then this makes it possible to obtain a feedback control law. If the specified matrix P(t) is found, then we can finally find the functional relationship between the control vector and the system state vector:

$$u = -R^{-1}B(t)^T P(t)x(t) \quad (5)$$

Substituting the expressions for **u** into the Euler equation, we eventually get a differential equation:

$$\dot{P} = -P(t)A(t) - A^T(t)P(t) + P(t)B(t)R^{-1}B^T(t)P(t) - Q \quad (6)$$

Equation (6) is called the matrix Riccati differential equation (MRDE), and it has been established [30] that the matrix Riccati differential equation has the following property: if matrices A and B have constant components, then as t $\rightarrow\infty$ its solution approaches a constant matrix. Then the equation (6) becomes the matrix algebraic Riccati equation (MARR):

$$P(t)A(t) + A^T(t)P(t) - P(t)B(t)R^{-1}B^T(t)P(t) + Q = 0 \quad (7)$$

It is also proved that the found positively symmetric solution P = P_0 of this equation is the only one, which implies that it is possible to construct an optimal controller with a coefficient matrix: $K_0 = -R^{-1}B^T P$.

There is no analytical solution to the algebraic Riccati matrix equation in general, and its numerical solution in general is a non-trivial problem and has been the subject of intensive research for reliable algorithms in the recent past, in particular [31].

At the moment, the results of these studies have already been implemented in special application packages, in particular Matlab, so we will not investigate the specifics of these algorithms, but will use them to solve our problem. It does provide guaranteed asymptotic stabilization. For example, if we substitute the values of the parameters from Table 2, we get the following system of equations:

$$\begin{bmatrix} \Delta\dot{\omega}_r \\ \Delta\dot{\delta} \\ \Delta\dot{\psi}_{fd} \end{bmatrix} = \begin{bmatrix} 0 & -0.059 & -0.130 \\ 50. & 0 & 0 \\ 0 & -0.09 & -0.196 \end{bmatrix} \begin{bmatrix} \Delta\omega_r \\ \Delta\delta \\ \Delta\psi_{fd} \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 998.1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \Delta u \end{bmatrix} + \begin{bmatrix} 2.51 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Delta M_м \\ 0 \\ 0 \end{bmatrix} \quad (8)$$

To obtain a specific value of the optimal controller, we must also specify the values of the elements of the matrices Q and R. Since both matrices are symmetric and positively definite, we can define them as follows:

$$Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (9)$$

The solution of the Riccati equation allows us to obtain the P matrix and, consequently, the control as a function of the state variables. The LQR calculated in this way really shows a good quality of stabilization. Figure 5 shows comparative graphs of frequency changes during disturbance in the absence of the controller and in its presence.

2.2.2 Parametric optimization to mitigate the harmful effect of LAA

The Kalman controller is indeed optimal in the context of the quadratic criterion and guarantees asymptotic stability. However, this is not enough. The question remains as to how well it reduces damage from the effects of LAA attacks, as well as other disturbances with significant amplitudes of parameter deviations from the nominal operating mode. The point is that guaranteeing stabilization alone is not enough, even if it is optimal stabilization with respect to the quadratic criterion. As was shown above, in electrical networks, operational requirements require additional criteria dictated by both the technical conditions of individual devices and the integrity of the power grid.

These requirements give rise to a methodology known by the acronym BIBO (Boundary Input - Boundary Output), which

refers to the fact that the output parameters of the system must be within certain limits under given constraints on the input parameters. The LQR theory of optimal control is not designed to solve such a problem and left some uncertainty about the choice of optimal controller parameters. At the same time, if the system dynamics itself was parameterized based on the nature of the object, the values of the Q and R matrices were left to the intuition of the designers. The LQR theory does not provide any recommendations for the choice of matrices, except for those that impose restrictions on the type of matrices Q and R. Therefore, finding the optimal LQR will be considered as the first step to finding a controller that best solves the problem of mitigating the harmful effects of disturbances caused by LAA attacks or disturbances of other types of attacks.

2.2.3 Determination of the parametric optimization criterion

The next step is to formulate a criterion by which to assess the level of damage from the consequences of an attack. In principle, this should be a functional that would assess deviations from the ideal mode from disturbances. To a certain extent, the root mean square criterion corresponded to this idea, but not completely. In our opinion, a more adequate function should be one that measures the total value of the absolute values of deviations from the nominal values of the controlled variables, taking into account the weighting factors that take into account the amount of damage depending on the range of deviation. It should also be noted that the monitored parameter will be the frequency of the electric voltage in the grid, as the main parameter of electricity quality.

$$JP = \sum_{i=0}^{N} abs(\omega_i - \omega_n) * S_d \qquad (10)$$

Where JP – parametric criterion; ω_i – is the frequency value at the i-th moment; ω_n– value of the nominal frequency deviation threshold; S_d – the value of the weighting factor depending on the size of the deviation. In determining the values of the weighting coefficients shown in the Table 3, the results of studies were taken into account [20].

Table 3

Values of weighting coefficients

№	Frequency deviation range	The value of the weighting factor
1	0.	0
2	>0.2 <0.5	0.5
3	>0.5 <1.5	1.5
4	>1.5 <2.5	4.5
5	>2.5 <3	9
6	>3	20

The values of the weighting coefficients were selected based on an expert analysis of the materials of the blackout damage, based on the potential levels of damage, and may be further refined.

3. The problem of finding the optimal SMIB controller

The problem of mitigating the effects of LAA-type cyberattacks on the SMIB configuration network can now be formulated as the problem of finding the optimization of losses according to criterion (11).

$$\min JP(Q, R) \qquad (11)$$

$$Q \in F_q,\ R \in F_r,$$

where F_q – is a set of symmetric sign-positive matrices, F_r – is a set of positively definite matrices.

The formal definition of parametric damage minimization is quite simple, but solving problem (10) is not a straightforward task, since minimizing the criterion JP(Q, R) is impossible by gradient methods, let alone an analytical solution. The reason is that the direction of movement to the optimal point can only be calculated based on the values of the criterion, not its gradient. Here, the choice of an efficient gradient-free method is key to solving problem (10). In this work, we chose the Nelder-Mead algorithm [32], a method that does not require the calculation of derivatives, which makes it suitable for problems with non-smooth functions and functions whose values are calculated by a procedure.

That is, for our problem, we first determine the initial values of Q and R. Next, we calculate the matrix P by solving the MARP and calculate the control vector using the expression (7). This allows us to calculate the transient response to the disturbance and makes it possible to estimate the value of the JP criterion. The next step is the formation of

the so-called simplex, which is a set of n + 1 points with the values of the criterion at certain values of the independent variables. That is, the procedure must be repeated n + 1 times (n is the number of independent variables in the problem). The essential requirement of this initial set is that the selected points of the working simplex and the corresponding set of function values at the vertices for the initial working simplex should not lie in the same hyperplane. Next, the search for the optimum begins by changing the position of the current worst candidate by moving relative to the centroid at each iteration of the algorithm. The movement will be relative to the centroid of the remaining simplex, i.e., the "center of gravity" of the other candidates for replacement.

The movement in the direction of the optimum is realized either by stretching the simplex or, conversely, by compressing it. The general approach of this algorithm, in contrast to gradient descent, is that instead of trying to find a solution directly, it tries to find a search area that contains a potential solution and gradually narrow it down. Despite the fact that in general, the convergence of the Nelder-Meade algorithm to the optimum has not been rigorously proven, the method works for many problems. The corresponding module is contained in the Matlab library - the minimize function (method='Nelder-Mead'), which was used to solve the problem ().

Taking as a starting point the values of the matrices Q and R{q_{11}=1, q_{22}=1,q_{33}=1, r_{33}=1} as for the previously obtained LQR controller, an initial simplex was formed around the specified point. Starting with these initial values, the Nelder-Meade algorithm significantly improved the initial value of the JP criterion in 64 iterations, which corresponded to the previously found value of the JP criterion, as shown in Table 4.

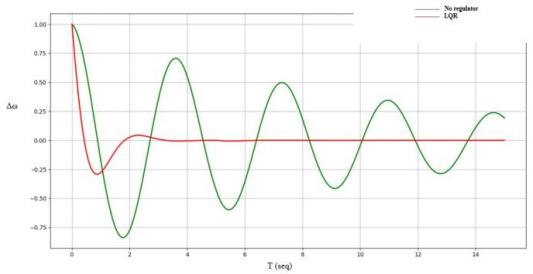

Figure 6: Frequency stabilization dynamics in the presence and absence of the LQR controller

Fig. 7 clearly shows the better quality of disturbance stabilization of the optimized controller compared to the previously obtained stabilization by the LQR procedure.

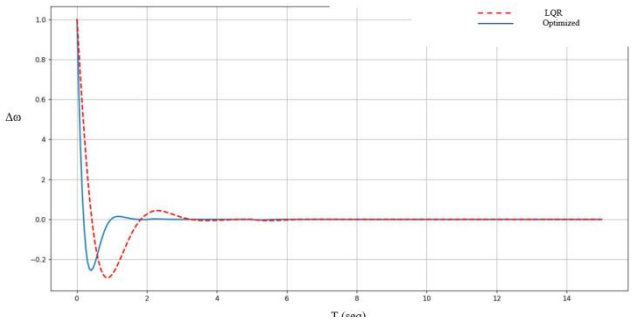

Figure 7: Frequency stabilization dynamics for the LQR controller and the optimized controller

The Table 4 shows the comparative values of the criterion of losses from a sudden change in load for different disturbance control options.

Table 4

Comparative values of the stabilization criterion for different disturbance control options

Adjustment option	Criterion value (conditional units)
No regulator	506.23
LQR regulator	47.15
Optimized controller	19.72

The graphs in Fig. 6, Fig. 7, and the data in Table 4 convincingly show that the quality of stabilization in the presence of the controller improves the quality of stabilization of the generator against disturbances by an order of magnitude. At the same time, the optimized controller performs two and a half times better than the LQR controller with arbitrarily taken values of the coefficients of the matrices Q and R. This means mitigating the negative effects of disturbances.

Conclusions

The vast majority of cyberattacks on critical infrastructure cannot be detected and identified at the outset. The list of such attacks includes a load-altering attack (LAA), which is specific to power grids. The current level of digitalization of all spheres of life, in particular the steady upward trend in the growth of IoT devices with their relatively weak cybersecurity, makes it possible for attackers

to organize an attack on the power system. The consequences of such an attack can be devastating, comparable to large-scale disasters caused by natural disasters. A strategy to counter this type of attack should include such an important element as mitigating the harmful effects of an LAA attack. This is especially true for the initial stage of the attack, when power generators are in a state of abrupt load change. The research results presented in this paper propose a solution that mitigates the "first strike" of a LAA attack by adjusting the regulators of electric generators accordingly by minimizing the proposed criterion. Moreover, this solution also applies to mitigating the effects of a sharp change in load caused by other reasons, which indicates an increase in the level of resilience of the power system. It should be noted that this study concerned the simplest of power grids - a single-line scheme of a single SMIB machine. Modern power systems are much more complex. However, they all consist of SMIBs as an integral element. Based on system-wide principles, it can be argued that the higher the level of resilience of system elements, the higher the level of resilience of the system as a whole. Therefore, better stabilization at the SMIB level will improve the resilience of the power system as a whole. However, how and in what way is the subject of future research, as well as the question of how to counter LAA attacks at all stages.

References

[1] Asaad, M., Ahmad, F., Alam, M.S., Sarfraz, M.: Smart grid and Indian experience: A review. Resour. Policy 74, 101499 (2019).

[2] Gunduz, M.Z., Das, R.: Cyber–security on smart grid: Threats and potential solutions. Comput. Networks 169, 107094 (2020).

[3] Su, Q., Chen, C., Li, J.: Trendrank method for evaluating the importance of power grid nodes considering information network. IET Gener. Transm. Distrib. 17(3), 539–550 (2023).

[4] Dileep, G.: A survey on smart grid technologies and applications. Renewable Energy 146, 2589–2625 (2019).

[5] Mrabet, Z.E., Kaabouch, N., Ghazi, H.E., Ghazi, H.E.: Cyber–security in smart grid: Survey and challenges. Comput. Electr. Eng. 67, 469–482 (2018).

[6] Гальчинський Л., Личик В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, 2 (8), 27–33. https://doi.org/10.32689/maup.it.2023.2.3

[7] Wang, H., Ruan, J., Zhou, B., Li, C., Wu, Q., Raza, M.Q., Cao, G.Z.: Dynamic data injection attack detection of cyber physical power systems with uncertainties. IEEE Trans. Ind. Inform. 15(10), 5505–5518 (2019).

[8] Gunduz, M.Z., Das, R.: Analysis of cyber–attacks on smart grid applications. In: Proceedings of 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), pp. 1–5. IEEE, Piscataway, NJ (2018).

[9] Lopez, C., Sargolzaei, A., Santana, H., Huerta, C.: Smart grid cyber security: An overview of threats and countermeasures. J. Energy Power Eng. 9(007), 632–647 (2015)

[10] Procopiou, A., Komninos, N.: Current and future threats framework in smart grid domain. In: Annual IEEE International Conference on Cyber Technology in Automation, Control, Intelligent Systems, pp. 1852–1857. IEEE, Piscataway, NJ.

[11] Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C.L.P.: Cyber security and privacy issues in smart grids. IEEE Commun. Surv. Tutorials 14(4), 981–997 (2012).

[12] J. L. Mathieu, P. N. Price, S. Kiliccote, and M. A. Piette, "Quantifying changes in building electricity use, with application to demand response," IEEE Trans. on Smart Grid, vol. 2, no. 3, pp. 507–518, 2011.

[13] Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on cyber security for smart grid communications. IEEE Commun. Surv. Tutorials 14(4), 998– 1010 (2012).

[14] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. 2017. Grid Shock: Coordinated Load–Changing Attacks on Power Grids: The Non–Smart Power Grid is Vulnerable to Cyber Attacks as Well. In 2017 Annual Computer Security Applications Conference. ACM, New York, NY, USA, 12 pages. https: //doi.org/10.1145/3134600.3134639.

[15] Mohsenian–Rad, A.H., Leon–Garcia, A.: Distributed internet–based load altering attacks against sm art power grids. IEEE Trans. Smart Grid 2(4), 667–674 (2011).

[16] Soltan, S., Mittal, P., & Poor, H.V. (2018). BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. USENIX Security Symposium.

[17] Galchynsky, L., Graivoronskyi, M., & Dmytrenko, O. (2021). Evaluation of MachineLearning Methods to Detect DoS / DDoS Attacks on IoT.CEUR Workshop Proceedings,3241, 225–236, URL: https://ceur–ws.org/Vol–3241/paper21.pdf.

[18] ANTONAKAKIS, M., APRIL, T., BAILEY, M., BERNHARD, M., BURSZTEIN, E., COCHRAN, J., DURUMERIC, Z., HALDERMAN, J. A., INVERNIZZI, L., KALLITSIS, M., ET AL. Understanding the Mirai botnet. In Proc. USENIX Security Sympsion'17 (Aug. 2017).

[19] SOLTAN, S., MAZAURIC, D., AND ZUSSMAN, G. Analysis of failures in power grids. IEEE Trans. Control Netw. Syst. 4, 3 (2017), 288–300.

[20] U.S.–CANADA POWER SYSTEM OUTAGE TASK FORCE. Report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal–Web.pdf.

[21] C. Mellucci et al., "Load alteration fault detection and reconstruction in power networks modelled in semi–explicit differential algebraic equation form," in American Control Conf. IEEE, 2015.

[22] Q. Su et al., "Observer–based detection and reconstruction of dynamic load altering attack in smart grid," Journal of the Franklin Institute, vol. 358, no. 7, pp. 4013–4027, 2021.

[23] G. Rinaldi et al., "Load altering attacks detection, reconstruction and mitigation for cyber–security in smart grids with battery energy storage systems," in European Control Conf. IEEE, 2022, pp. 1541–1547.

[24] Q. Ma et al., "Dynamic load–altering attack detection based on adaptive fading Kalman filter in power systems," Global Energy Interconnection, vol. 4, no. 2, pp. 184–192, 2021.

[25] S. Amini, F. Pasqualetti, and H. Mohsenian–Rad, "Detecting dynamic load altering attacks: A data–driven time–frequency analysis," in IEEE SmartGridComm, 2015.

[26] [92] E.–N. S. Youssef, F. Labeau, and M. Kassouf, "Detection of load–altering cyberattacks targeting peak shaving using residential electric water heaters," Energies, vol. 15, no. 20, p. 7807, 2022.

[27] A. Ebtia et al., "Spatial–temporal data–driven model for load altering attack detection in smart power distribution networks," IEEE Trans. Ind. Informat., 2024.

[28] Padiyar K. R. Power System Dynamics, BS Publications, 2008.

[29] Prabha Kundur. Power System Stability and Control. Power System Engineering Series. – McGraw–Hill, Inc. 1994. 1176 pp. ISBN 0–07–035958–X.

[30] Daniel Liberzon. Calculus of Variations and Optimal Control Theory: A Concise Introduction Illustrated Edition.

[31] A. Lanzon, Y. Feng, B. Anderson, and M. Rotkowitz. "Computing the Positive Stabilizing Solution to Algebraic Riccati Equations with an Indefinite Quadratic Term via a Recursive Method". IEEE Transactions on Automatic Control, 53(10):2280 – 2291, 2008.

[32] Bürmen, A., Puhan, J., and Tuma, T. (2006), "Grid Restrained Nelder–Mead Algorithm", Comput. Optim. Appl. 34, pp. 359–375.