frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 21 November 2024
DOI 10.3389/fenrg.2024.1502078

OPEN ACCESS

EDITED BY
Liwei Ju,
Northeast Electric Power University, China

REVIEWED BY
Zengji Liu,
Nanjing University of Posts and Telecommunications, China
Yingjun Wu,
Hohai University, China
Mohamed A. Mohamed,
Minia University, Egypt

*CORRESPONDENCE
Liu Ren,
liuren248@foxmail.com

RECEIVED 26 September 2024
ACCEPTED 11 November 2024
PUBLISHED 21 November 2024

CITATION
Ren L, Binyuan Y, Hengdao G, Junrong L, Yihua Z, Yun F, Liang T and Zeyuan Z (2024) Research on relay setting attack defense in power systems based on a three-layer optimization model.
Front. Energy Res. 12:1502078.
doi: 10.3389/fenrg.2024.1502078

Research on relay setting attack defense in power systems based on a three-layer optimization model

Liu Ren[1,2,3,4]*, Yan Binyuan[5], Guo Hengdao[1,2,3,4], Liu Junrong[5], Zhu Yihua[1,2,3,4], Fu Yun[5], Tu Liang[1,2,3,4] and Zhou Zeyuan[5]

[1]State Key Laboratory of HVDC, Electric Power Research Institute, China Southern Power Grid, Guangzhou, China, [2]National Energy Power Grid Technology R&D Centre, Guangzhou, China, [3]Guangdong Provincial Key Laboratory of Intelligent Operation and Control for New Energy Power System, Guangzhou, China, [4]CSG Key Laboratory for Power System Simulation, Electric Power Research Institute, China Southern Power Grid, Guangzhou, China, [5]Information Centre of Guizhou Power Grid Co., Guizhou, China

With the intelligent development of power systems, the number of relays continues to increase. Differences in manufacturers, systems, and protocols lead to growing security risks. Tampering with relay settings could potentially cause power outages or even system instability. Consequently, relay settings have gradually become a key target for cyberattacks, particularly in smart grids where traditional defense measures struggle to effectively address complex and diverse attack scenarios. To address this issue, this paper proposes a three-layer optimization defense model based on game theory, designed to adapt to various attack scenarios. The core methodology of this model includes a three-layer structure: The first layer optimizes the protection level of each relay by allocating limited defense budgets. The second layer analyzes the potential system damage based on the attacker's strategy choices. The third layer comprehensively calculates system losses to evaluate the effectiveness of defense plans. Through layer-by-layer optimization of budget allocation, the model minimizes the unsupplied energy loss caused by relay setting attacks. Compared to existing methods, this model not only improves defense effectiveness under resource constraints but also addresses multiple complex attack scenarios. Experimental results demonstrate that this model significantly enhances the system's defense capabilities and effectively reduces the impact of attacks on system security operations.

KEYWORDS

power system, relay setting attack, game theory model, three-layer optimization, defense strategy, cybersecurity

1 Introduction

With the global development of intelligent power systems, cybersecurity has become a critical issue in power system operations (Yohanandhan et al., 2020). The widespread application of smart grids and the integration of Internet of Things devices have made distribution systems more automated and efficient. However, these advancements have also introduced severe cybersecurity challenges. In recent years, power systems

have been frequently subjected to various cyber attacks, with key equipment such as relays becoming primary targets for attackers (Abraham et al., 2024). For instance, the cyber attack on Ukrainian power companies in 2015 resulted in large-scale power outages, directly affecting hundreds of thousands of users (Kabeyi and Olanrewaju 2022). Such attacks have exposed the vulnerability of power system relays and revealed the inadequacies of traditional defense measures in addressing complex attack scenarios (Elgazzar et al., 2022).

As power systems grow more complex, cyber attack methods have become increasingly diverse. Relay setting attacks have gradually evolved into a highly destructive form of attack (Ghiasi et al., 2023). Research on defense strategies against relay setting attacks is crucial for ensuring the secure operation of power systems. Game theory models provide an effective theoretical framework for this problem, capable of simulating the gaming process between attackers and defenders (Shan et al., 2020). Through optimized defense budget allocation, the overall system security can be enhanced under limited resource conditions, reducing system losses caused by attacks (Lau et al., 2020). This defense strategy can significantly improve the risk resistance of relays under attack and provide a theoretical basis for addressing future complex attack scenarios (Abdelkader et al., 2024).

Relay setting attacks primarily include Active Relay Setting Attacks (ARSA) and Passive Relay Setting Attacks (PRSA) (Ganjkhani et al., 2022). In active attacks, parameters such as relay startup current are tampered with by attackers, causing relays to misjudge system states and trigger tripping, leading to power supply interruptions (Zhou et al., 2021). Passive attacks involve modifying relay operation times or other parameters, resulting in delayed responses to faults and expanding the scope of system failures (Altaf et al., 2022). These two attack mechanisms pose serious threats to system stability, especially when attackers control multiple relays, potentially causing large-scale power outages and system collapse (Wang et al., 2024).

In current research, scholars focus on defense model design, detection and identification methods, and modeling of attack-defense interactions. These directions are pursued concurrently to enhance the security of power system relays and reduce their vulnerability to cyber attacks.

In the field of attack model development, a method was proposed in Ganjkhani et al. (2022) to simulate system losses caused by relay setting attacks. Both active and passive relay setting attacks were considered, and the impact on the power system was highlighted by optimizing the selection of attack strategies to maximize energy disruption. An indirect attack model was proposed in Wang et al. (2023), and a defense strategy to prevent relay mistripping was designed. This strategy implements blocking cause identification technology as a built-in function of relays to resist indirect collaborative attacks. In (Zhang and Dong 2017), researchers proposed a trip confirmation scheme based on majority rules through reliability studies of remote relays, aiming to reduce the possibility of erroneous tripping.

Regarding detection and identification methods, a data mining-based detection tool was proposed in Mohamed and Magdy (2022). This tool utilizes training datasets generated by Monte Carlo simulation to detect anomalous changes in relay settings. It uses rough set classification to generate a set of If-Then rules for checking whether updated settings have been tampered with during online operations. A deep learning-based system was developed in Khaw et al. (2020) to identify malicious attacks by detecting abnormal changes in current and voltage signals. This system first uses current and voltage measurements to train deep learning models, which are then used to detect malicious data injected by attackers. In Ameli et al. (2019), an effective intrusion detection method was proposed through voltage measurement comparisons, distinguishing between false signals triggered by attacks and real internal faults. This method uses unknown input observers and state-space models to estimate local voltage and compare it with measured values.

In the area of attack-defense interaction modeling, a game model based on three-layer optimization was proposed in Ganjkhani et al. (2022). The focus is on how defenders can minimize unsupplied energy loss under limited attacker resources. This model integrates defense budget allocation, attack strategy selection, and system loss calculation into a comprehensive optimization framework (Hasan et al., 2020). further explored game models for dynamic attacks, considering the long-term impact of attackers' phased attack strategies on system security. This research adopted a new attacker-defender model, taking into account the temporal order of attacks (Macwan et al., 2016). focused on data injection attacks, proposing a defense mechanism that detects and mitigates attacks through basic laws in power systems. This mechanism utilizes Kirchhoff's laws and communication capabilities under the IEC61850 standard to detect and locate data injection attacks.

Current research on relay setting attacks has several limitations: 1) Defense models lack universality and struggle to adapt to various system environments. Existing models are often designed for specific attack types or system structures, showing insufficient adaptability to complex and varied attack scenarios. 2) The real-time performance and accuracy of detection and identification methods in complex scenarios need improvement. Current detection algorithms may face challenges in computational efficiency and accuracy when processing large-scale, high-dimensional data. 3) Existing attack-defense interaction models have high computational complexity, making it difficult to respond to dynamic attacks in large-scale systems. In practical applications, these models may struggle to quickly respond to changes in attacker strategies, affecting defense effectiveness.

To address these limitations, a three-layer optimization defense model based on game theory is proposed in this paper. A defense strategy adaptable to various attack scenarios has been designed. The core methodology of this model includes a three-layer structure: The first layer optimizes the protection level of each relay by allocating limited defense budgets. The second layer analyzes the potential system damage based on the attacker's strategy choices. The third layer comprehensively calculates system losses to evaluate the effectiveness of defense plans. Through layer-by-layer optimization of budget allocation, the unsupplied energy loss caused by relay setting attacks is minimized. Compared to existing methods, this model offers the following advantages: 1) It provides a more flexible and efficient defense framework by integrating a three-layer optimization model and dynamic budget allocation mechanism,

capable of adapting to complex relay setting attack scenarios. 2) It improves defense effectiveness under resource constraints and can simultaneously address both active and passive relay setting attacks. The model's effectiveness has been verified through case studies on test systems. Experimental results demonstrate that this model significantly enhances the system's defense capabilities and effectively reduces the impact of attacks on system security operations. This approach provides a more comprehensive and effective solution for defending against relay setting attacks in power systems.

The structure of this paper is as follows: Chapter 2 discusses the mechanisms and impacts of relay setting attacks in power distribution systems. This chapter analyzes the vulnerability of relays under different types of attacks, particularly the impact of active and passive relay setting attacks on system security. A detailed vulnerability analysis provides the foundation for subsequent defense model design. Chapter 3 presents the game theory-based defense model design. This chapter constructs a three-layer optimization model, systematically describing the interaction between defense budget allocation and attacker strategies. The model maximizes system security while minimizing unsupplied energy loss caused by attacks through optimized budget allocation. Chapter 4 verifies the model's practical effectiveness through experimental design and case analysis. Based on the IEEE 123-node test system, the defense effects of different budget allocation strategies under active and passive relay attacks are evaluated. The role of defense strategies in enhancing system security is demonstrated, and specific schemes for optimizing budget allocation are provided. Chapter 5 summarizes the main conclusions of the research, elaborates on the effectiveness of game theory in defending against relay setting attacks, and points out potential directions for future research, such as introducing dynamic defense mechanisms and strategies for addressing other types of attacks.

2 Mechanisms and impacts of relay setting attacks in power distribution systems

2.1 Relay protection mechanisms in power distribution systems

Overcurrent protection relays are crucial devices for ensuring stable operation in power distribution systems. These relays detect current changes in the system and can promptly trigger circuit breakers or reclosers, thereby preventing short-circuit faults or other abnormal conditions from causing greater impact on the system. The foundation of overcurrent protection lies in the relay's ability to quickly issue a trip signal when the current value exceeds a set threshold, thus protecting downstream equipment. The core of this process is the relay's precise judgment of current, ensuring that it can operate at the appropriate time to avoid system collapse due to slow response or misoperation.

In practical operation, the protection mechanism of relays involves principles of overcurrent protection and requires close coordination with circuit breakers and reclosers. Circuit breakers execute the opening operation after receiving a trip signal from the relay, disconnecting the faulty line and protecting other parts of the system. Reclosers are responsible for reclosing the circuit after the fault has been cleared, allowing power supply to be restored as quickly as possible. This collaborative working mechanism greatly improves the system's fault tolerance and reduces the scope of power outages caused by faults. The coordinated action between relays, circuit breakers, and reclosers is crucial for ensuring the stability of the power system.

The response speed of overcurrent relays is directly related to their time dial settings. The time dial determines the operating time of the relay, which is the delay time from detecting a fault current to issuing a trip command. The operating time of a relay under fault conditions is represented by the following formula:

$$T_{r,g} = \Theta_r \left(\frac{\alpha_r}{\left(\frac{I_{r,g}}{I_r^{Th}} \right)^{\beta_r} - 1} + \gamma_r \right)$$

where $I_{r,g}$ is the fault current seen by relay r, I_r^{Th} is the adjusted pickup current, Θ_r is the time dial setting, and α_r, β_r, and γ_r are constants representing the characteristics of the curve selected for relay r. These parameters determine the relay's response time to various fault currents, allowing the relay to adjust its operation time automatically based on the magnitude of the current.

To ensure reliable relay operation in multiple fault scenarios, a layered coordination approach is typically adopted. This approach dictates that relays closest to the fault point operate first, while relays farther from the fault point act as backup protection based on set time delays. The core of this protection mechanism lies in ensuring that only the faulty part of the system is isolated, thereby avoiding widespread power outages due to incorrect tripping. The time dial values and pickup current settings in the aforementioned formula directly influence the protection level of the relay, ensuring each relay operates at the correct time point.

The protective action of relays must also be matched with the ratios of current and voltage transformers. The ratio settings of transformers significantly affect the operational accuracy of relays. Improper transformer ratio settings may lead to inaccurate fault current judgments by relays, resulting in delayed relay actions or incorrect tripping. Therefore, when designing relay protection mechanisms, it is necessary to consider time dial and pickup current settings and the electrical parameters of the entire system. This comprehensive approach ensures that relay actions align with the system's actual operating conditions.

2.2 Relay setting attacks

2.2.1 Active relay setting attacks

In ARSA, control over relay settings can be gained by attackers. The pickup current setting I_r^{Th} can be maliciously modified, causing the relay to incorrectly judge the system as being in an overload or short-circuit state, thereby sending erroneous trip signals. The pickup current setting determines the current level at which the relay automatically triggers a trip when detected. By lowering this setting to a level far below normal operating currents, attackers can trigger relay trips during normal system operation, leading to circuit breaker openings and power supply interruptions in the system.

This type of attack mechanism relies on adjusting relay parameters and can be described by the following formula:

$$I_r^{Th,bb} = \chi^a I_r^{Th}, \quad \chi^a < \frac{I_{r,g}}{I_r^{Th}} - \delta$$

where $I_r^{Th,bb}$ represents the pickup current of relay r after ARSA, χ^a is the scaling factor of ARSA, and δ represents the tolerance for measurement errors in the system. The attacker adjusts χ^a and δ to ensure that the relay's setting is reduced to an extremely unreasonable level, causing the relay to incorrectly detect a fault and trip even in the absence of an actual fault.

These attacks often directly impact downstream loads in the system. When relays trigger tripping, the downstream circuit breakers are forced to open, causing a sudden disconnection of large loads. The power outage in downstream loads affects end users and may further trigger cascading reactions such as system voltage imbalance or frequency fluctuations, increasing system operational instability. The immediate nature of ARSA implies that once successful, the system will instantly enter an abnormal state, placing higher demands on the real-time monitoring and response capabilities of maintenance personnel.

In distribution systems, the destructive nature of ARSA is manifested in the erroneous tripping behavior of the relays themselves and potentially more severe consequences through coordinated actions between relays, circuit breakers, and reclosers. Typically, the tripping of one relay can trigger a chain reaction in related equipment, rapidly expanding the fault area. For large-scale distribution systems, a single relay's erroneous operation may lead to power outages across entire regions. Particularly during high-load periods, power outages caused by such attacks affect downstream equipment and adversely impact upstream power supply equipment, further exacerbating system instability.

2.2.2 Passive relay setting attacks

In PRSA, relay settings are modified by attackers to prevent expected operation during system faults. The characteristic of these attacks is that their effects are not immediately apparent. Instead, they cause relay failures when future system faults occur, leading to delayed or incorrect tripping, thereby expanding the impact range of faults. These attacks often involve adjustments to the relay's time dial and pickup current settings, causing the relay to fail to respond promptly under fault conditions and disrupting relay coordination.

The key mechanism of PRSA is to violate the time coordination constraints between relays by adjusting their operation times. Suppose relay r is responsible for protecting a certain line segment, with relay r' as its backup. The time coordination relationship between them can be expressed by the following constraint:

$$T_{r',g} - T_{r,g} \geq \Delta T, \forall r' \in \mathcal{S}_r$$

where $T_{r',g}$ is the operation time delay of the backup relay r' when a fault g occurs downstream of relay r, $T_{r,g}$ is the operation time of relay r, and ΔT is the required time coordination margin between them. Under normal conditions, the primary relay r will trip first, and the backup relay r' will only operate if the primary relay fails.

In a Passive Relay Setting Attack (PRSA), the attacker manipulates the settings of relay r, increasing its operation time delay $T_{r,g}$, causing the backup relay r' to trip before the primary relay. The attacker disrupts the time coordination by altering the parameter ΔT^b, as shown in the following equation:

$$T_{r,g}^{bb} = T_{r,g} + \Delta T^b, \quad \Delta T^b > \Delta T + \delta$$

where $T_{r,g}^{bb}$ is the operation time delay of relay r after the attack, and ΔT^b is the additional delay introduced by the attack. δ represents the tolerance for measurement errors in the system. By increasing the operation delay, PRSA prevents the primary relay from responding in time to faults, causing the downstream backup relay to trip prematurely and thus widening the scope of the outage.

The impact of PRSA on power distribution systems lies in its increase of system vulnerability during fault conditions. The consequences of the attack are manifested only when the system experiences short circuits or other faults after relay settings have been modified. Compared to active attacks, PRSA is more covert. Attackers can quietly alter relay parameters without triggering immediate anomalies. The effects of the attack are revealed only through relay failures during fault occurrences, often exacerbating the scope and severity of accidents.

This attack method endangers not only single relays but can also aggravate fault consequences by affecting multiple relays across the entire distribution system. Particularly when time settings of multiple relays are simultaneously tampered with, widespread power outages may occur.

2.3 Vulnerability analysis of relay setting attacks

The relay protection mechanism in power distribution systems relies on communication networks, firmware, and local access interfaces of devices. Vulnerabilities in these aspects provide attackers with multiple potential pathways to launch attacks on relay settings. By infiltrating the system through different means, attackers may cause relay malfunctions or misoperations, thereby jeopardizing the security and stability of the power grid. Understanding these vulnerabilities can provide a basis for formulating defense measures.

2.3.1 Security vulnerabilities in communication networks

Relays in power distribution systems are typically connected to control centers via Wide Area Networks (WAN) and use standard communication protocols (such as IEC104 and IEC61850) for data transmission. The extensive coverage of these communication networks exposes them to multiple potential attack entry points. The overall failure probability of the system is:

$$P_{fail} = P_{attack} \cdot P_{relay} \cdot \left(1 - R_{response}\right)$$

where P_{fail} represents the system failure probability, P_{relay} indicates the probability that the attacker controls the relay, $R_{response}$ denotes the emergency response capability of the control center, and P_{attack} is the total attack success probability. The total attack success probability is calculated as:

$$P_{attack} = 1 - \left(S_{net} \cdot S_{protocol} \cdot S_{physical}\right)$$

where S_{net} refers to the security of the network layer, $S_{protocol}$ refers to the security of the protocol layer, and $S_{physical}$ refers to the security of the physical layer.

System networks can be infiltrated by attackers through firewall vulnerabilities or other weaknesses. Upon successful infiltration, network protection measures can be bypassed, allowing direct access to relay control interfaces and alteration of settings (Reda et al. 2022). This may result in relay failures during actual faults. For instance, relay pickup current or time dial settings can be modified by attackers, preventing normal tripping during actual faults (Zhou et al., 2021).

Communication network vulnerabilities are not limited to the physical layer but are closely related to the security of software, protocols, and data transmission (Ghiasi et al., 2023). Remote attack methods may be employed by attackers, such as Distributed Denial of Service (DDoS) or man-in-the-middle attacks (Wang et al., 2024). These attacks can sever the connection between control centers and relays, affecting the normal protective functions of the system.

2.3.2 Exploiting firmware vulnerabilities in relays

The firmware of relays, which serves as their core operating logic, can be targeted by attackers through the injection of malicious code. Firmware attacks may occur during the production, installation phases, or even during firmware updates. The final probability of a successful firmware tampering can be expressed as:

$$P_{success} = P_{tamper} \cdot \frac{R_{attacker} \cdot L_{knowledge}}{E_{security}}$$

where $R_{attacker}$ represents the resources available to the attacker, $E_{security}$ denotes the effectiveness of security measures, $L_{knowledge}$ reflects the depth of the attacker's understanding of the firmware logic, and P_{tamper} is the probability of firmware tampering.

The probability of firmware tampering is calculated as:

$$P_{tamper} = 1 - \left(S_{update} \cdot \left(1 - P_{implant}\right)\right)$$

where S_{update} represents the security of the firmware update channel, and $P_{implant}$ indicates the probability of successfully implanting malicious code by the attacker.

As firmware updates for many relays are conducted through online channels, malware can be intercepted and implanted by attackers during updates (Amin et al., 2021). Malicious firmware typically includes triggers and payloads. Triggers activate malicious operations based on specific events or signals, while payloads are the actual attack behaviors (Li et al., 2024). Once firmware is tampered with, relays can be remotely controlled or triggered at specific times by attackers, causing malfunctions or erroneous actions at critical moments (Trevizan et al., 2022). For instance, relay response times might be delayed by attackers, preventing timely tripping during system faults and disrupting protection coordination (Wang et al., 2021). To defend against such attacks, digital signatures and encryption can be used to verify the integrity of firmware updates. Regular auditing and upgrading of firmware can also reduce the possibility of malicious code implantation.

2.3.3 Local access attacks on relays

Although many relay devices are located within physically well-protected substations, relays distributed along distribution lines often lack strict physical protection (Vahidi et al., 2023). Through physical contact, attackers can directly connect to device interfaces and modify relay settings (Rajkumar et al., 2020). In some cases, attackers might even use techniques such as electromagnetic interference to disrupt internal circuits or data storage of relays, leading to abnormal device operation (Trevizan et al., 2022). The formula for calculating the probability of successful local attacks is:

$$P_{local} = \frac{N_{prots} \cdot P_{EMI}}{E_{physical}}$$

where $E_{physical}$ represents the effectiveness of physical protection measures, N_{prots} refers to the number of exposed physical ports, and P_{EMI} denotes the success rate of electromagnetic interference (EMI) attacks.

Direct connection to device interfaces and modification of relay settings can be achieved by attackers through physical contact (Wlazlo et al., 2021). In some cases, techniques such as electromagnetic interference might be used by attackers to disrupt internal circuits or data storage of relays, leading to abnormal device operation. Although local access attacks require physical contact, they pose higher risks in unattended outdoor equipment. Relay normal operation can be affected by attackers through forceful damage or high-tech tools like electromagnetic pulses. Additionally, exposed physical ports provide attackers with ways to bypass other protective measures (Kampourakis et al., 2023). To defend against local attacks, measures can be taken to strengthen relay external packaging, install anti-tampering detection devices, or reduce the possibility of local attacks through more advanced physical protection means (Yu et al., 2023).

3 Game theory-based defense model for relay setting attacks

3.1 Design and optimization of the game theory model

The stability and reliability of the power system are directly affected by the security of relay settings. In the face of potential cyber-attack threats, both defenders and attackers need to make optimal decisions in the game process. Two game models are analyzed in this paper: incomplete information game model and complete information game model, to discuss defense and attack strategies under different information conditions. In incomplete information games, strategies of both parties have asymmetry and uncertainty, while in complete information games, both parties have a clearer understanding of each other's strategies and resources. Through a three-layer optimization model in the game theory framework, this paper will discuss the budget allocation of defenders and strategy selection of attackers from these two scenarios respectively, ultimately maximizing system security.

3.1.1 Defense and attack strategy modeling

The strategic interaction between defenders and attackers can be described using game theory models. The defender's goal is to reduce the Expected Energy Not Supplied (EENS) under attack

through rational budget allocation. The attacker aims to maximize system losses by selecting specific attack strategies. The strategies of defenders and attackers interact: the defender's budget allocation directly affects the attacker's success rate, while the attacker's strategy selection influences the system's operational state and security.

3.1.1.1 Two game scenarios:

a) Incomplete Information Game: In real situations, attackers and defenders may not fully understand all strategies and resources of their opponents. Attackers might be unaware of the defender's focus on protecting certain relays, while defenders may struggle to predict specific attack targets and resource constraints of attackers. This asymmetric information reflects real-world complexity, so the game model needs to consider how this information incompleteness affects decisions and outcomes. In this scenario, defenders and attackers must make optimal decisions based on expectations of their opponent's type and behavior.
b) Complete Information Game: In some scenarios, it is assumed that defenders and attackers have complete knowledge of each other's resources, strategies, and objectives. Here, strategy selection in the game can be simplified to a zero-sum game, with both parties directly confronting each other under complete information conditions. This type of scenario is more suitable for situations where information about the opponent is fully known, optimizing budget allocation and strategy selection to maximize one's own benefits or minimize losses.

To adapt to these two different information conditions, subsequent chapters of this paper will explore the Bayesian game model under incomplete information games, and the simplified bi-level optimization under complete information games. This approach will provide optimal decision support for defenders and attackers under different information conditions.

3.1.2 Mathematical description of the three-layer optimization model

The interaction between defenders and attackers is described by the three-layer optimization model. It integrates defense budget allocation, attack strategy selection, and system loss calculation into a comprehensive optimization framework. The three-layer structure consists of:

(1) Defense Budget allocation Layer (First Layer): The defender's probability of relay failure is reduced through the allocation of limited defense budgets. The decision variable for the defender is the budget allocation d_r, for each relay, with the objective of minimizing the system's EENS. The defender's budget allocation is represented by the vector $\mathbf{d} = [d1, \ldots, d_r, \ldots, d_R]$, where d_r represents the defense budget allocated to relay r. The defender's total budget D_{max} is subject to the following constraint:

$$\sum_{r=1}^{R} d_r \le D_{max}$$

The total budget constraint is represented by the set $\mathcal{D}$:

$$\mathcal{D} = \left\{ \mathbf{d} \in \mathbb{R}_{+}^{R} | \sum_{r=1}^{R} d_r \le D_{max} \right\}$$

This set indicates that the defender's total budget D_{max} needs to be allocated across all relays, and the sum of budget allocations cannot exceed the defender's available budget.

The EENS calculation formula is:

$$EENS = \sum_{r \in \mathcal{S}} \rho_r(d_r, d^s) \cdot \theta_r$$

where d_r represents the defense budget allocated to relay r, d^s represents the system-level defense budget, and θ_r is the load loss caused by the failure of relay r. $\mathcal{S}$ is the index set of all relays r in the power system, where failures or losses may occur. The higher the EENS, the greater the power supply loss under attack. Therefore, the defense strategy should prioritize reinforcing high-load nodes.

Defense strategies are typically divided into device-level and system-level. Device-level defense aims to enhance the local security of each relay, mainly including strengthening physical barriers, upgrading firmware security, introducing multi-factor authentication, adding firewalls for each relay, etc. These measures improve overall system security by reducing the failure probability $\rho_r(d_r)$ of specific relays, typically described using an exponential decay model:

$$\rho_r(d_r) = e^{-\mu_r d_r}$$

where μ_r is the sensitivity coefficient of relay r, representing the degree to which the defense budget allocated to that relay affects its failure probability.

System-level defense focuses on the security of the entire system, mainly including encryption of network-wide communication, system monitoring upgrades, integration of attack detection systems, etc. The system-level defense budget d^s System-level defense focuses on the security of the entire system, mainly including encryption of network-wide communication, system monitoring upgrades, integration of attack detection systems, etc. The system-level defense budget

$$\rho_r(d_r, d^s) = \beta e^{-\mu_r d_r} + (1-\beta) e^{-\xi d^s}$$

where β is the weighting factor between the device-level and system-level budgets, ξ represents the effectiveness parameter of system-level defense, d_r is the local defense budget allocated to each relay to reduce its failure probability, and d^s is the system-level defense budget used to enhance the protection capability of the entire system. Reasonable allocation of defense budgets requires a balance between device-level and system-level to minimize overall failure probability.

(2) Attacker's Strategy Selection Layer (Second Layer): $k \in \mathcal{K} = \{1, \cdots, K\}$ is defined as the attack scenario, where $\mathcal{K}$ is the set of all attack scenarios, and K is the total number of scenarios. The number of possible attack combinations is calculated by:

$$\binom{x}{y} = \frac{x!}{y!(x-y)!}$$

where x represents the total number of relays, and y is the number of relays attacked simultaneously.

The attacker selects one or more relays as attack targets within the limited resource constraint. The attacker's goal is to disrupt the system by maximizing load loss. The attacker selects the attack target set $\mathcal{S}_c$ and optimizes their attack strategy to maximize system loss. The specific optimization problem is described as:

$$\max_{\mathcal{S}_c} \sum_{r\in\mathcal{S}_c} \rho_r(d_r, d^s)\cdot\theta_r$$

subject to:

$$\sum_{r\in\mathcal{S}_c} c_r \le C$$

where θ_r represents the load loss caused by the failure of relay r. The attacker's selection is limited by the total available resources C, and c_r denotes the resources required to attack relay r. The attacker maximizes system loss by selecting the relay set $\mathcal{S}_c$.

Due to limited resources, both the defender and attacker need to make optimal decisions within their budgets. The attacker selects the target relay combination $\mathcal{S}_c$ to maximize the system's load loss θ_r, while the defender allocates budget d_r to reduce the relay failure probability $\rho_r(d_r, d^s)$ to minimize losses.

(3) System Loss Calculation Layer (Third Layer): The system loss $\phi_c(\mathbf{d})$ is jointly determined by the defense budget $\mathbf{d}$ and attack strategy $\mathcal{S}_c$. The loss function is expressed as:

$$\phi_c(\mathbf{d}) = \rho_r(d_r, d^s)\cdot\theta_r$$

The core problem of the entire three-layer structure can be represented by a typical Min-Max optimization problem. The defender's goal is to minimize system loss under the worst-case attack scenario:

$$\min_{\mathrm{d}\in\mathcal{D}} \max_{\mathrm{k}\in\mathcal{K}} \left[\phi_c(\mathbf{d})\cdot \mathrm{T}^R(d^t)\right]$$

where the system recovery time $\mathrm{T}^R(d^t)$ represents the time required for the system to return to normal operation after an attack. It depends on the budget d^t allocated by the defender for identifying and restoring the system. By optimizing d^t, the defender can accelerate the recovery process and reduce the total system loss. After an attack, the defender must also consider how to optimize the recovery time $\mathrm{T}^R(d^t)$, which is related to the identification system's budget d^t:

$$\mathrm{T}^R(d^t) = T_i - T(d^t)$$

$$T(d^t) = \frac{2\Delta TR}{1+e^{-\gamma(d^t-D^t)}}$$

where T_i represents the recovery time of the distribution system without an identification system, $T(d^t)$ is the time reduced by deploying an identification system, ΔTR is the reduced recovery time after installing the identification system, D^t is the minimum budget required to install the identification system, and γ is a parameter controlling the smoothness of the function. When the budget d^t exceeds a certain threshold D^t, the identification system can significantly shorten the recovery time. However, when the budget is insufficient, the reduction in recovery time is limited. By optimizing d^t, the defender can accelerate system recovery speed, thereby reducing the total system loss.

3.2 Budget allocation strategy for security measures

In power system defense strategies, rational defense budget allocation is crucial for ensuring system security and resilience. As relay security directly determines the system's risk resistance under cyber attacks, budget allocation must consider both device-level and system-level defenses. Through mathematical modeling, this paper explores how to allocate budgets for these two types of defense measures under limited budget conditions to optimize overall defense effectiveness. While the proposed model assumes rational decision-making by both attackers and defenders, we recognize that real-world scenarios often involve irrational or unpredictable strategies by attackers. Attackers may not always follow optimized or predictable paths due to limited information, resource constraints, or other contextual factors. To address this complexity, future extensions of this model could incorporate stochastic elements, introducing randomness into the attacker's strategy selection. This would allow for a more robust defense model that reflects the uncertainty and variability of real-world cyber-physical system attacks.

3.2.1 Simplification and modeling of the budget allocation problem

In the budget allocation problem, defenders need to find a balance between device-level and system-level defenses to minimize the EENS of the entire system.

The defender's core objective is to minimize the system's expected loss by rationally allocating budgets d_r and d^s within the budget constraint D_{max}. The optimization problem can be formulated as the following min-max problem:

$$\min_{d\in\mathcal{D}} \max_{k\in\mathcal{K}} \left[\sum_{r\in\mathcal{S}_c} \rho_r(d_r, d^s)\cdot\theta_r\right]$$

Where the attacker maximizes the system's load loss θ_r by selecting attack scenarios $\mathcal{S}_c$, while the defender minimizes these losses through budget allocation strategies d_r and d^s.

To simplify this bi-level optimization problem, it can be assumed that the attacker chooses the worst-case attack scenario S_c^*, i.e., the attack strategy that maximizes system loss. Under this assumption, the defender's goal is transformed into minimizing system loss under the worst-case attack scenario:

$$\min_{d\in\mathcal{D}} \sum_{r\in\mathcal{S}_c^*} \rho_r(d_r, d^s)\cdot\theta_r$$

The defender's optimization process can be solved using standard optimization algorithms (such as linear programming or nonlinear programming). Based on the importance of each relay and its load loss after failure, the defender rationally allocates defense budgets d_r and d^s to ensure system loss is minimized when an attack occurs.

3.2.2 Game strategies under incomplete information

In scenarios with incomplete information, defenders and attackers may not accurately understand each other's full strategies. Therefore, traditional complete information game models fail

to accurately reflect real situations. In such cases, randomness and expectation analysis in decision-making become particularly important. Defenders can dynamically adjust their defense strategies based on risk assessments of potential attack targets, while attackers can choose optimal attack paths by inferring the defender's strategy from historical data. To more precisely characterize this uncertainty, a Bayesian game model is introduced in this paper, enabling defenders to make optimal decisions under uncertainty.

The Bayesian game model is used to describe how participants make optimal strategic decisions based on each other's behaviors and type information under incomplete information conditions. In Bayesian games, each participant's type is private information, and other participants can only make strategic decisions based on known type distributions.

Let the attacker's type be θ_A and the defender's type be θ_D, both drawn from their respective type spaces with known distributions. Each participant chooses the optimal strategy based on their observed type and expectations of other participants' types. This framework better aligns with real-world power systems, as defenders may not know the attacker's exact targets, and attackers may be unclear about the specific protection strength for certain relays.

The defender's goal is to minimize system loss under incomplete information. Assuming the attacker's attack intensity on each relay depends on their type θ_A, the defender allocates defense budgets d_r and d^s according to their type θ_D. The defender's loss function can be expressed as:

$$L_D(d,\theta_D) = \sum_{r\in\mathcal{S}} \rho_r(d_r,d^s)\cdot\theta_r$$

Under incomplete information, the defender can only estimate expected losses based on the distribution of the attacker's type $P(\theta_A)$. Thus, the defender's expected loss function is:

$$\mathbb{E}_{\theta_A}[L_D(d,\theta_A)] = \int_{\theta_A} L_D(d,\theta_A)P(\theta_A)d\theta_A$$

This expected loss function considers the loss weights brought by different attacker types θ_A and is an important basis for the defender's decision-making.

The attacker's goal is to choose the optimal attack strategy $\mathcal{S}_c$ to maximize system loss. Assuming the attacker attacks based on the defender's type θ_D and defense strategy d_r, their loss function $L_A(d,\theta_A)$ is expressed as:

$$L_A(d,\theta_A) = \sum_{r\in\mathcal{S}} \rho_r(d_r,d^s)\cdot\theta_r$$

Under incomplete information, the attacker does not know the defender's exact defense strategy and can only estimate expected losses based on the distribution of the defender's type $P(\theta_D)$. Therefore, the attacker's expected utility is:

$$\mathbb{E}_{\theta_D}[L_A(d,\theta_D)] = \int_{\theta_D} L_A(d,\theta_D)P(\theta_D)d\theta_D$$

Based on this expected loss, the attacker chooses the optimal attack combination $\mathcal{S}_c$ without knowing the defender's strategy.

In the Bayesian game model, participants make optimal decisions based on their own types and beliefs about other participants' types. Defenders and attackers make decisions based on expected losses and utilities, aiming to find the Bayesian Nash Equilibrium. The Bayesian Nash Equilibrium is the optimal strategy combination made by participants after considering all information (including the distribution of the opponent's type and their own type).

The conditions for Bayesian equilibrium can be expressed as:

$$d^* = arg\min_{d\in\mathcal{D}} \mathbb{E}_{\theta_A}[L_D(d,\theta_A)]$$

$$\mathcal{S}_c^* = arg\max_{\mathcal{S}_c\in\mathcal{K}} [L_A(d,\theta_D)]$$

Under Bayesian equilibrium conditions, the defender's strategy d^* minimizes expected losses across all possible attack types, while the attacker's strategy $\mathcal{S}_c^*$ maximizes expected losses across all possible defense types.

3.2.3 Optimization strategies under complete information game theory

In practical scenarios, complete and incomplete information games are applicable to different situations. For cases where both attackers and defenders have a clear understanding of each other's resources and strategies, the incomplete information game can be simplified to a complete information game. In complete information games, as both parties have consistent knowledge of system parameters, resources, and strategies, uncertainty need not be considered, and the game can be directly transformed into a zero-sum game problem. Next, the simplification of the bi-level optimization problem using the Lagrange multiplier method within the complete information game framework will be explored.

To transform the attacker's budget constraint into a constraint in the defender's optimization process, the Lagrange multiplier λ_c is introduced, forming the following Lagrangian function:

$$L(d,\lambda_c) = \sum_{r\in\mathcal{S}_c} \rho_r(d_r,d^s)\cdot\theta_r + \lambda_c\left(C - \sum_{r\in\mathcal{S}_c} c_r\right)$$

This Lagrangian function transforms the bi-level optimization problem into a single-level optimization problem under the attacker's resource constraint $\sum_{r\in\mathcal{S}_c} c_r \le C$. The defender chooses the optimal budget allocation strategy considering all possible attack scenarios $\mathcal{S}_c$, minimizing system losses in the worst-case scenario. Through this approach, the defender can solve complex game problems through simpler computational methods, enhancing system security and robustness.

In addition to relay setting attacks, the optimization framework could be extended to address other types of cyber threats, including False Data Injection Attacks (FDIA) and Denial of Service (DoS) attacks. FDIA, which manipulates data to mislead system operations, could be integrated into the second layer of the model by adding mechanisms for data validation and anomaly detection. Meanwhile, DoS attacks, which impair communication networks, could be addressed by incorporating network redundancy and prioritizing critical communication channels in the system-level defense budget allocation.

4 Case study

4.1 Experimental design

The IEEE 123-node test system is a classic distribution network test system used to study and verify various power system optimization methods and defense strategies. The system comprises 123 nodes, forming a complete distribution network topology, including main substations, lines, loads, and protective relays. Through experiments on this test system, the impact of attack and defense strategies on grid security, stability, and reliability can be evaluated. In practical applications, the assumption that both attackers and defenders act rationally may not always be valid. Attackers might deploy suboptimal or randomized strategies, driven by motivations beyond simply maximizing system disruption. To mitigate this, integrating probabilistic elements into the defense strategy could further strengthen the system's resilience. By allowing the defense model to account for random or suboptimal attacker behaviors, the overall effectiveness of the system's defense mechanism can be improved under unpredictable attack conditions.

The primary objectives of the experimental design are to evaluate the effectiveness of various defense budget allocation strategies and their ability to reduce EENS during ARSA and PRSA. Specifically, the experiments aim to quantify the reduction in system losses as a result of different budget allocations, and analyze the system's resilience under both single-relay and multi-relay attack scenarios.

The experimental design is based on several key assumptions. First, it is assumed that critical relays, such as those near substations, are more vulnerable to attacks and thus require higher priority for defense budget allocation. Second, the experiments assume a limited total defense budget, which must be optimally allocated between device-level and system-level defenses. Finally, it is assumed that attackers are rational and aim to maximize system loss by selecting optimal attack combinations, while defenders aim to minimize these losses through strategic budget allocation.

Figure 1 shows the single-line diagram of the IEEE 123-node test system. The system serves 85 concentrated loads with a total active load of 3,490 kW (kW). Circuit breakers and reclosers are configured at critical nodes to protect the main substation and its branch lines. Each relay provides protection for specific line segments and serves as a backup protection device for other relays. When certain relays fail, others can take over their protective tasks, ensuring system continuity and reliability.

To enhance the experiment's realism, seven protective relays were added to line segments (13–18), (13–52), (18–135), (67–97), (67–72), and (76–86). These relays' settings consider differences in line load, distance, and conditions to ensure timely fault isolation at critical nodes when attacked. The failure of each relay may lead to load interruption, making rational defense budget allocation the core of the experimental design. The experiment assumes that relay R1 is located at the main substation and has undergone initial reinforcement measures, with its failure probability approaching zero, denoted as $\rho_1 \approx 0$. Other relays have no initial reinforcement measures and have higher failure probabilities.

To optimize budget allocation, the experiment also assumes the installation of an attack identification system. This system can accelerate system recovery after an attack. The budget required for the system is set at 30 ($D^t = 30$), reducing the system recovery time from an initial 5 h ($\rho^i = 5$) to 3 h ($\Delta TR = 2$). The installation of the attack identification system can significantly reduce power supply restoration time. Attacks are divided into ARSA and PRSA. ARSA directly modifies relay settings to trip under normal working conditions, while PRSA delays relay response time during fault conditions, expanding the system's fault impact range.

Defense budget allocation must consider the importance of relays in the system. Relays at the system's core, such as those near the main substation, will receive priority for more defense budget. The successful attack probability ρ_r^d for these relays can be reduced to near 0 through reinforcement measures. For relays in secondary system areas, basic protection is provided, and their successful attack probability may remain at a higher level. This experimental design ensures a comprehensive evaluation of attack and defense strategies. System performance under attack is assessed through experimental results under different defense configurations.

4.2 Results analysis

This section explores the impact of two types of attacks on system performance through the analysis of single-relay and multi-relay attack scenarios. The experiments were based on the IEEE 123-node test system, combining different budget allocation strategies to evaluate the changes in EENS under various attack scenarios, thereby optimizing the defense budget allocation strategy.

4.2.1 Single-relay attack

In the experiments, the performance changes of individual relays under attack were first analyzed. By comparing the performance of various relays under ARSA and PRSA, the differences in the impact of different attacks on system load loss were determined.

Figure 2 shows the Load Loss (LL) for each relay under ARSA and PRSA with no defense measures. The figure reveals that PRSA causes significantly higher load losses for relays R2, R5, R6, and R7 compared to ARSA. For instance, PRSA attacks on R2 result in load losses approaching 2.2MW, while ARSA losses are about 1.2 MW. This indicates that R2 is more significantly affected under PRSA attacks, especially when this relay is upstream, where PRSA can easily cause more widespread cascading outages. For relay R3, the situation is reversed, with ARSA causing greater load losses than PRSA, mainly because R3 is downstream and its load is more directly affected by ARSA.

The experimental results reveal differences in the vulnerability of single relays under different attack types, with PRSA being more destructive to the system. Therefore, system protection strategies should allocate different defense resources based on the importance of different relays, with priority measures taken for critical relays such as R2 and R5 to reduce their vulnerability under PRSA.

4.2.2 Multi-relay attack

In addition to single-relay attacks, multi-relay simultaneous attacks were simulated to analyze their impact on system EENS. Three groups of relays were selected for simultaneous attacks, comparing the destructive power of ARSA and PRSA in these scenarios.

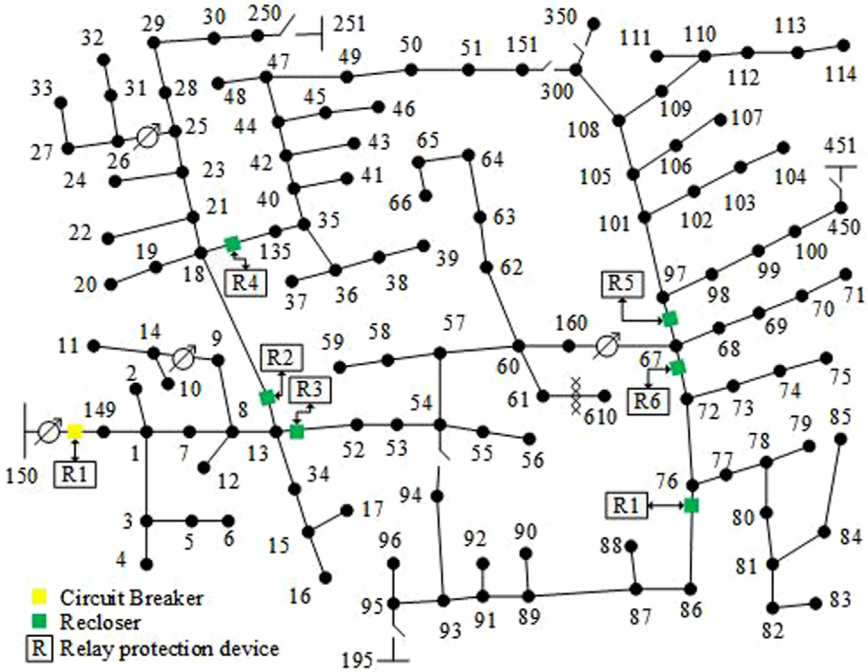

FIGURE 1
IEEE 123-node test feeder.

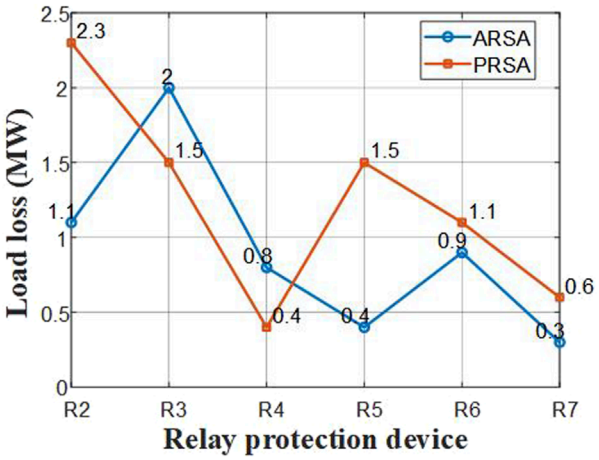

FIGURE 2
Comparison between ARSA and PRSA under different relay protection devices.

Figure 3 illustrates the maximum EENS changes when one, two, or three relays are simultaneously attacked. The results indicate that in multi-relay attack scenarios, PRSA's destructive power significantly exceeds that of ARSA. For instance, when R3, R6, and R7 are simultaneously subjected to PRSA attacks, the EENS reaches 17 MWh, while the same relay combination under ARSA attacks only results in an EENS of 16 MWh. Particularly in the combined attack on R2, R3, and R5, the load loss caused by PRSA nearly reaches the system's maximum limit, reflecting the high risk of multi-relay PRSA attacks to the system.

The experimental results demonstrate that under multi-relay attacks, PRSA is often more destructive than ARSA, especially when multiple critical relays are simultaneously attacked. The chain reaction caused by PRSA may lead to global power supply interruptions. Therefore, when formulating defense strategies, the system should adequately respond to the special effects of PRSA, ensuring high system stability even when multiple relays are simultaneously attacked.

4.2.3 Optimization effect of budget allocation strategies

To further enhance the system's attack resistance, the performance of optimal and non-optimal budget allocation strategies under different attack scenarios was evaluated through experiments. The results indicate that rational budget allocation strategies can significantly reduce EENS and improve the system's defense effectiveness.

(1) Comparison of Optimal and Non-optimal Allocation Strategies

Figure 4 compares the impact of ARSA and PRSA on system EENS under different budget allocation strategies. The figure shows EENS changes under three different budget allocation strategies. The red solid line represents the optimal allocation strategy considering both ARSA and PRSA. As the budget increases, EENS gradually decreases. When the budget reaches 30, the EENS reduction is most significant, indicating that the system's defense effect reaches its optimal state at this point. As the budget further increases, EENS

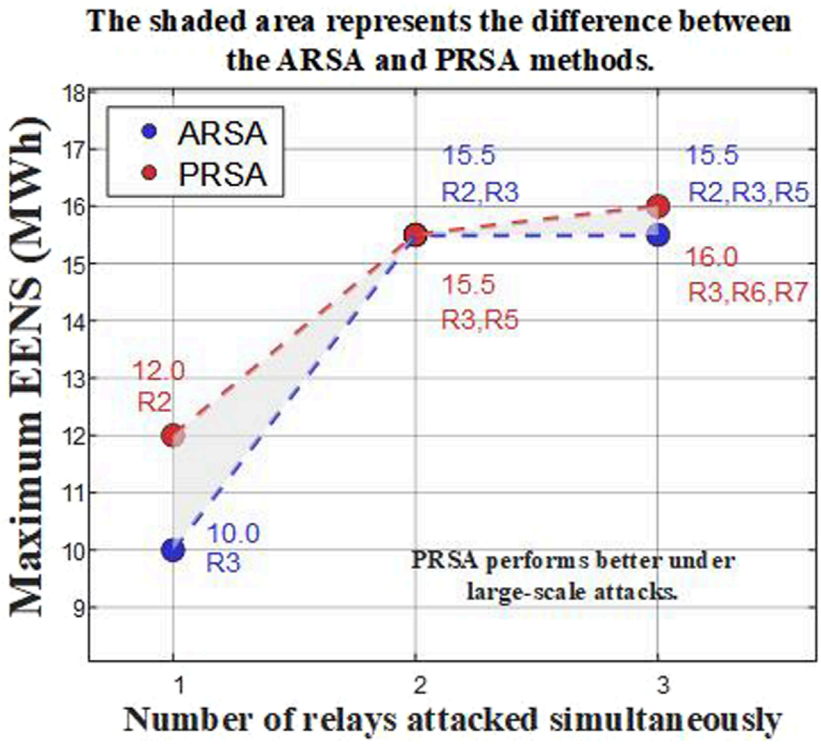

FIGURE 3
Comparison of maximum EENS under different attack scales for ARSA and PRSA methods.

changes become more gradual, indicating that the system's overall recovery capability is significantly improved under higher budgets. The blue dashed line represents the defense strategy considering only ARSA. Under higher budgets, this strategy shows good control over system EENS, but at lower budgets, EENS exhibits higher values, especially when the budget approaches 30, where the defense effect is clearly inferior to the optimal allocation strategy. When only ARSA is considered, the system shows greater vulnerability to PRSA attacks and cannot effectively reduce EENS. The green dashed line represents the defense strategy considering only PRSA. This strategy performs excellently at lower budgets, with a large decrease in EENS, but as the budget increases, its defense effect gradually approaches that of the optimal allocation strategy. In terms of overall defense effectiveness, it is still slightly inferior to the optimal strategy considering both ARSA and PRSA. When the budget reaches higher values, the PRSA strategy cannot achieve the optimal defense effect.

(2) Optimization Direction of Defense Strategies

Figure 5 illustrates the resource allocation proportions for various systems and relays under different budget levels. The vertical axis represents the budget allocation percentage for each defense measure, ranging from 0% to 100%. The horizontal axis represents budget size, varying from 50 to 500 units. Different colored areas correspond to relays and systems, showing their dynamic allocation proportions in the total budget as the budget changes.

At low budgets, the attack identification system (d^t) occupies the majority of the allocation proportion. As the budget increases, the proportion of d^t gradually decreases. This trend reflects that under limited resources, defense strategies focus more on ensuring basic attack identification capabilities. However, as the budget increases, the resources required for d^t gradually decrease, shifting the focus of resource allocation.

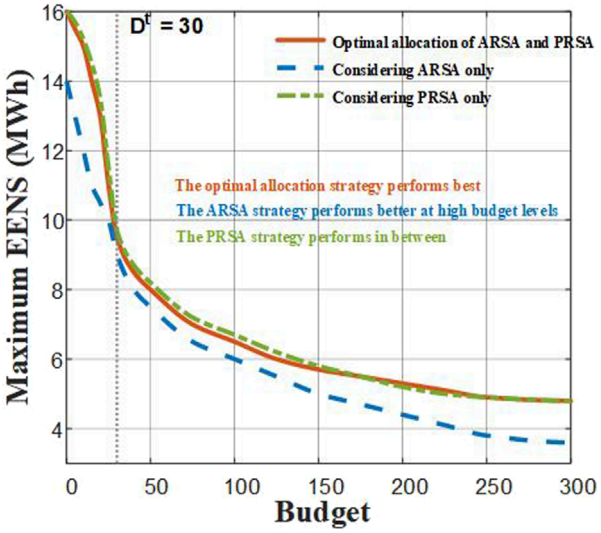

FIGURE 4
Comparison of EENS variations with budget changes under different strategies.

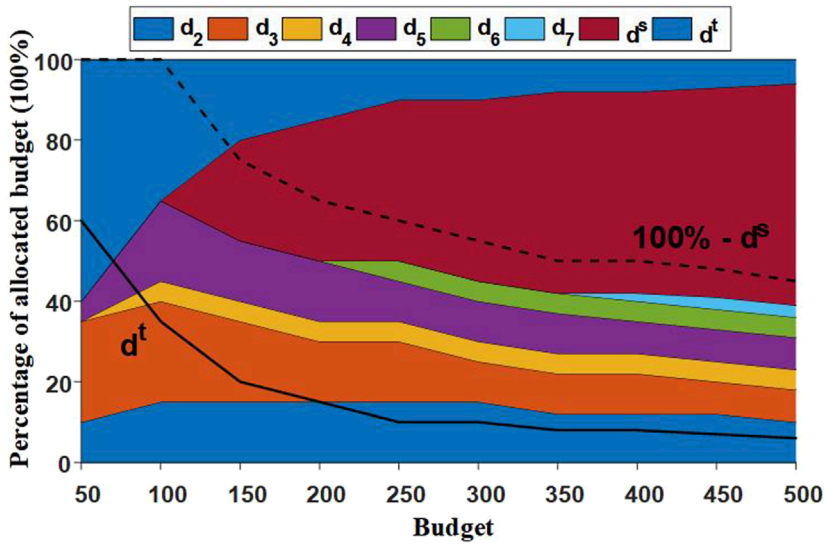

FIGURE 5
Resource allocation trends at different budget levels.

Concurrently, the allocation proportion for system-wide defense measures (d^s) significantly increases with budget growth. At low budgets, d^s receives almost no resource allocation, but as the budget increases, its proportion gradually expands, eventually becoming the main object of resource allocation in high-budget situations. This indicates a gradual shift in defense strategy from single-point protection to comprehensive system protection to improve overall defense levels.

Critical relays such as d_2, d_3, and d_5 maintain relatively stable allocation proportions across the entire budget range. Regardless of budget increases, these relays consistently receive certain resources, reflecting their continued importance in system security. In contrast, d_4, d_6, and d_7 have smaller resource allocation proportions but receive some resources as the budget increases, reflecting further expansion of system defense at higher budgets.

To further assess the robustness of the proposed defense model, a sensitivity analysis was conducted to explore the effects of varying budget levels and allocation strategies on system resilience. Three different budget scenarios were considered: low-budget, medium-budget, and high-budget. The sensitivity analysis revealed that while higher budgets naturally lead to improved resilience and lower EENS, the allocation strategy plays a critical role in maximizing the effectiveness of the defense. Under low-budget conditions, focusing resources on critical relays such as those near the main substation resulted in significant reductions in EENS, while in higher-budget scenarios, more resources could be distributed across secondary relays, further improving system resilience.

The three-layer optimization defense model offers practical applicability in various power system environments, especially those facing resource constraints. By dynamically allocating the defense budget across device-level and system-level protections, the model ensures that critical relays receive priority in budget allocation, while also addressing system-wide security measures. This adaptability allows the model to be deployed in real-world scenarios, where resource availability may fluctuate. Additionally, the model can be easily integrated with existing power system security frameworks due to its modular nature.

5 Conclusions and prospects

This research proposes a three-layer optimization model based on game theory framework for defending against relay setting attacks in power systems. By considering two types of attacks, ARSA and PRSA, the allocation of defense budgets is optimized to minimize expected energy losses under different attack scenarios. The study utilizes zero-sum game theory concepts to establish a strategy interaction model between defenders and attackers, further verifying the effectiveness of this defense strategy in the IEEE 123-node test system through experiments.

Through theoretical derivation and simulation experiments, the following conclusions are drawn:

(1) Rational allocation of defense budgets can effectively reduce expected energy losses when the system is subjected to relay setting attacks.
(2) Active and passive attacks have significantly different impacts on relays, especially in scenarios where multiple relays are simultaneously attacked, with PRSA being more destructive.
(3) Experiments show that in low-budget situations, device-specific defense measures contribute more to system security, while in high-budget situations, system-wide defense measures become more important.

This research primarily focuses on defending against relay setting attacks, specifically ARSA and PRSA. However, other types of cyberattacks, such as FDIA and DoS attacks, are also prevalent in power systems. The current model does not directly address these attack vectors. Future extensions of this work could adapt the three-layer optimization model to cover a broader range of cyber threats by integrating defense mechanisms against FDIA and DoS attacks,

which target different system vulnerabilities such as data integrity and network availability.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

LR: Writing–review and editing, Writing–original draft, Supervision, Methodology, Conceptualization. YB: Writing–review and editing, Funding acquisition, Data curation. GH: Writing–review and editing, Project administration, Methodology. LJ: Writing–review and editing, Visualization, Formal Analysis. ZY: Writing–review and editing, Formal Analysis, Data curation. FY: Writing–review and editing, Resources, Investigation. TL: Writing–review and editing, Visualization, Resources. ZZ: Writing–review and editing, Validation, Resources.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. Research supported by the science and technology project of Guizhou Power Grid Company (GZKJXM20222346).

Conflict of interest

Authors YB, LJ, FY, and ZZ were employed by Information Centre of Guizhou Power Grid Co. Authors LR, GH, ZY, and TL Were employed by China Southern Power Grid. Authors LR, GH, ZY, and TL Were employed by China Southern Power Grid.

The remaining 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.

The authors declare that this study received funding from Guizhou Power Grid Company. The funder had the following involvement in the study: Data curation, Formal analysis, Visualization, Resources, Investigation, Validation, and Writing–review and editing.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., et al. (2024). Securing modern power systems: implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results Eng.* 23, 102647. doi:10.1016/j.rineng.2024.102647

Abraham, D., Toftegaard, Ø., Dr, B. B. J., Gebremedhin, A., and Yayilgan, S. Y. (2024). Consequence simulation of cyber attacks on key smart grid business cases. *Front. Energy Res.* 12, 1395954. doi:10.3389/fenrg.2024.1395954

Altaf, M. W., Arif, M. T., Islam, S. N., and Haque, Md E. (2022). Microgrid protection challenges and mitigation approaches–A comprehensive review. *IEEE Access* 10, 38895–38922. doi:10.1109/access.2022.3165011

Ameli, A., Ali, H., El-Saadany, E. F., and Youssef, A. M. (2019). An intrusion detection method for line current differential relays. *IEEE Trans. Inf. Forensics Secur.* 15, 329–344. doi:10.1109/TIFS.2019.2916331

Amin, M., El-Sousy, F. F. M., Aziz, G. A. A., Gaber, K., and Mohammed, O. A. (2021). CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: a review. *Ieee Access* 9, 38571–38601. doi:10.1109/access.2021.3063229

Elgazzar, K., Khalil, H., Alghamdi, T., Ahmed, B., Abdelkader, G., Elewah, A., et al. (2022). Revisiting the internet of things: new trends, opportunities and grand challenges. *Front. Media SA* 1. doi:10.3389/friot.2022.1073780

Ganjkhani, M., Mehdi Hosseini, M., and Parvania, M. (2022). Optimal defensive strategy for power distribution systems against relay setting attacks. *IEEE Trans. Power Deliv.* 38 (3), 1499–1509. doi:10.1109/tpwrd.2022.3230946

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., and Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. *Electr. Power Syst. Res.* 215, 108975. doi:10.1016/j.epsr.2022.108975

Hasan, S., Dubey, A., Karsai, G., and Koutsoukos, X. (2020). A game-theoretic approach for power systems defense against dynamic cyber-attacks. *Int. J. Electr. Power and Energy Syst.* 115, 105432. doi:10.1016/j.ijepes.2019.105432

Kabeyi, M. J. B., and Olanrewaju, O. A. (2022). Sustainable energy transition for renewable and low carbon grid electricity generation and supply. *Front. Energy Res.* 9, 743114. doi:10.3389/fenrg.2021.743114

Kampourakis, V., Gkioulos, V., and Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Comput. and Secur.* 133, 103383. doi:10.1016/j.cose.2023.103383

Khaw, Y. M., Abiri Jahromi, A., Arani, M. F. M., Sanner, S., Kundur, D., and Kassouf, M. (2020). A deep learning-based cyberattack detection system for transmission protective relays. *IEEE Trans. Smart Grid* 12 (3), 2554–2565. doi:10.1109/tsg.2020.3040361

Lau, P., Wei, W., Wang, L., Liu, Z., and Ten, C.-W. (2020). A cybersecurity insurance model for power system reliability considering optimal defense resource allocation. *IEEE Trans. Smart Grid* 11 (5), 4403–4414. doi:10.1109/tsg.2020.2992782

Li, T., Zhang, X., Zhao, H., Xu, J., Chang, Y., and Yang, S. (2024). A dual-head output network attack detection and classification approach for multi-energy systems. *Front. Energy Res.* 12, 1367199. doi:10.3389/fenrg.2024.1367199

Macwan, R., Drew, C., Panumpabi, P., Valdes, A., Vaidya, N., Sauer, P., et al. (2016). Collaborative defense against data injection attack in IEC61850 based smart substations. *IEEE Power Energy Soc. General Meet. (PESGM)*, 1–5. doi:10.1109/pesgm.2016.7741376

Mohamed, N., and Magdy, M. A. S. (2022). Data mining-based cyber-physical attack detection tool for attack-resilient adaptive protective relays. *Energies* 15 (12), 4328. doi:10.3390/en15124328

Rajkumar, V. S., Tealane, M., Ştefanov, A., and Palensky, P. (2020). Cyber attacks on protective relays in digital substations and impact analysis. *2020 8th Workshop Model. Simul. Cyber-Physical Energy Syst.*, 1–6. doi:10.1109/mscpes49613.2020.9133698

Reda, H. T., Anwar, A., and Mahmood, A. (2022). Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* 163, 112423. doi:10.1016/j.rser.2022.112423

Shan, H., Gene, X., and Zhuang, J. (2020). A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. *Reliab. Eng. and Syst. Saf.* 195, 106683. doi:10.1016/j.ress.2019.106683

Trevizan, R. D., Obert, J., De Angelis, V., Nguyen, Tu A., Rao, V. S., and Chalamala, B. R. (2022). Cyberphysical security of grid battery energy storage systems. *IEEE Access* 10, 59675–59722. doi:10.1109/access.2022.3178987

Vahidi, S., Ghafouri, M., Au, M., Kassouf, M., Mohammadi, A., and Debbabi, M. (2023). Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: a survey on challenges and opportunities. *IEEE Commun. Surv. and Tutorials* 25 (2), 1294–1335. doi:10.1109/comst.2023.3251899

Wang, L., Zhang, K., Bi, W., Wang, Y., Li, Y., and Mao, W. (2023). Indirect coordinated attack against relay via load-side power electronics and its defense strategy. *IEEE Trans. Industrial Inf.* 20, 5112–5124. doi:10.1109/tii.2023.3330307

Wang, Qi, Cai, X., Tang, Yi, and Ni, M. (2021). Methods of cyber-attack identification for power systems based on bilateral cyber-physical information. *Int. J. Electr. Power and Energy Syst.* 125, 106515. doi:10.1016/j.ijepes.2020.106515

Wang, X., Ji, Y., Sun, Z., Liu, C., and Jing, Z. (2024). Improving cyber-physical-power system stability through hardware-in-loop co-simulation platform for real-time cyber attack analysis. *Front. Energy Res.* 12, 1402566. doi:10.3389/fenrg.2024.1402566

Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., et al. (2021). Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Physical Syst. Theory and Appl.* 6 (3), 164–177. doi:10.1049/cps2.12014

Yohanandhan, R. V., Madurai Elavarasan, R., Manoharan, P., and Mihet-Popa, L. (2020). Cyber-physical power system (CPPS): a review on modeling, simulation, and analysis with cyber security applications. *IEEE Access* 8, 151019–151064. doi:10.1109/access.2020.3016826

Yu, Y., Wen, Y., Ding, W., and Zhou, J. (2023). Reinforcement learning solution for cyber-physical systems security against replay attacks. *IEEE Trans. Inf. Forensics Secur.* 18, 2583–2595. doi:10.1109/tifs.2023.3268532

Zhang, J., and Dong, Y. (2017). Cyber attacks on remote relays in smart grid. *2017 IEEE Conf. Commun. Netw. Secur. (CNS)*. doi:10.1109/CNS.2017.8228637

Zhou, T. L., Xiahou, K. S., Zhang, L. L., and Wu, Q. H. (2021). Multi-agent-based hierarchical detection and mitigation of cyber attacks in power systems. *Int. J. Electr. Power and Energy Syst.* 125, 106516. doi:10.1016/j.ijepes.2020.106516