Nafees, Muhammad Nouman, Saxena, Neetesh and Burnap, Peter 2023. POSTER: Adaptive moving target defense: Enhancing dynamic perturbation through voltage sensitivity analysis in power systems. Presented at: 21st International Conference on Applied Cryptography and Network Security (ACNS 2023), Kyoto, Japan, 19-22 June 2023. 21st International Conference on Applied Cryptography and Network Security (ACNS 2023) Proceedings.

POSTER: Adaptive Moving Target Defense: Enhancing Dynamic Perturbation through Voltage Sensitivity Analysis in Power Systems

Muhammad Nouman Nafees, Neetesh Saxena, and Pete Burnap

School of Computer Science and Informatics, Cardiff University, UK
`{nafeesm,saxenan4,burnapp}@cardiff.ac.uk`

Abstract. Moving target defense (MTD) strategies significantly protect power systems against stealthy false data injection attacks. However, traditional MTD approaches in power systems predominantly focus on single-parameter perturbation, leaving gaps in addressing the complexity and unpredictability of attack surfaces. In this work, we present a novel MTD strategy that departs from the traditional approach and utilizes multiple parameter perturbations to enhance the resilience of power systems against cyber threats while ensuring system stability. Our contributions include investigating the impact of individual and combined parameter perturbations on power system stability and performance, utilizing voltage sensitivity analysis to identify critical parameters, and considering the trade-offs between system security and operational constraints. The proposed algorithm dynamically perturbs the selected parameters, incorporating insights from the power flow Jacobian matrix analysis, and continuously adapts the MTD strategy based on the obtained results.

Keywords: Moving target defense · Dynamic perturbation · Voltage sensitivity analysis.

1 Introduction

The perturbation technique in Moving Target Defense (MTD) is crucial in safeguarding power systems from stealthy False Data Injection (FDI) attacks. By dynamically modifying system parameters and configurations, MTD increases the attack surface's intricacy and unpredictability, posing considerable challenges for adversaries attempting to comprehend and exploit the system.

Previous research in this area has primarily focused on perturbing single parameters [1], [3]; however, this study investigates the impact of combined parameter perturbations on system performance and stability. The advantage of considering multiple parameters lies in a more comprehensive and robust MTD strategy. Nonetheless, it necessitates rigorous analysis of power system stability when perturbing multiple parameters, and a clear limit of perturbation should be thoroughly investigated. This approach ensures that the MTD strategy does not compromise the power system's stability and performance while enhancing its resilience against cyber threats. In this context, voltage sensitivity analysis in power systems plays a crucial role in identifying the critical parameters that significantly influence system stability and performance, ultimately enabling more effective defense strategies.

1.1 Contributions

In this work, we contribute to the field of MTD research by exploring the feasibility and effectiveness of adaptive perturbation strategies in power systems. We investigate the impact of individual and combined parameter perturbations on the power system's stability and performance, employing voltage sensitivity analysis to identify critical parameters.

To implement the adaptive MTD strategy, we propose an algorithm that dynamically perturbs the selected parameters, incorporating insights from the power flow Jacobian matrix analysis [2]. The algorithm determines and applies parameter perturbations within their defined ranges while considering system constraints and operational requirements. By iteratively exploring different combinations of parameter perturbations and continuously adapting the MTD strategy based on the obtained results, our algorithm significantly contributes to the novelty and advancement of MTD research in power systems.

2 Methodology

In this section, we outline the steps to investigate the impact of dynamic perturbation strategies for MTD on power system performance. The methodology includes simulating parameter perturbations and conducting voltage sensitivity analysis.

2.1 Sensitivity Analysis Approach

We thoroughly investigate the effectiveness of adaptive MTD perturbation strategies by incorporating additional power systems components such as Distributed Flexible AC Transmission System (D-FACTS) devices, load profiles, generator settings and voltage set-points, and transmission line parameters using PowerWorld Simulator. This expanded analysis allows us to investigate the interactions and impact of these components on the power system's resilience to FDI attacks, ultimately enhancing power system security.

We conduct a sensitivity analysis to pinpoint the most critical parameters and determine their optimal combinations. Then, we perturb individual parameters within their operating limits, observing the impact on system performance and stability. We calculate the sensitivity indices for each parameter, representing the relative change in bus voltages per unit change in the parameter. The sensitivity indices enable us to quantify the impact of each parameter on the system's voltage profile, allowing for a more targeted and efficient approach when designing adaptive MTD strategies. We rank the parameters based on their sensitivity indices, identifying those with the most significant impact on the system, and use the ranked parameters to explore different combinations to maximize the MTD benefits while maintaining system stability and performance.

2.2 Algorithm for Dynamic Parameter Perturbations

The power flow Jacobian matrix is crucial to numerous optimization, security, operation, and planning applications in power systems. To this end, it contains the partial derivatives of the active and reactive power flow mismatch equations concerning voltage magnitudes and phase angles, and it is typically very sparse. To implement the adaptive MTD strategy, we develop an algorithm that dynamically perturbs the selected parameters, incorporating the insights from the power flow Jacobian matrix analysis.

Algorithm 1 Dynamic Parameter Perturbations

```
1: Initialize the IEEE 9-Bus System with PowerWorld Simulator and SimAuto interface.
2: Define perturbation ranges and limits for each parameter, considering system constraints and operational requirements:
     – Voltage magnitudes: $V_{\min} \leq V \leq V_{\max}$
     – Transmission line limits: $|S| \leq S_{\max}$
     – Generator real/reactive power limits: $P_{\min} \leq P \leq P_{\max}$, $Q_{\min} \leq Q \leq Q_{\max}$
3: Use a random number generator to select perturbation values for chosen parameters within their defined ranges.
4: Apply the perturbations to the IEEE 9-Bus System through the SimAuto interface.
5: Monitor the system's performance and stability, recording the relevant data.
6: Evaluate the effectiveness of the MTD strategy based on observed changes in system performance and stability.
7: Iterate the process, exploring different combinations of parameter perturbations, and continuously adapting the MTD strategy based on the obtained results.
```

3 Simulation and Results

In this section, we discuss the simulation setup and results of our investigation on the impact of dynamic perturbations strategies for MTD on power system performance. We perform individual and combined parameter perturbations and analyze their effects on system stability and analyze its efficacy. Stability refers to the ability of the power system to maintain a stable voltage profile and frequency response, while efficacy refers to the efficiency and reliability of the system in maintaining its process with perturbations.

3.1 Simulation Setup

To investigate the impact of adaptive MTD strategies on power system performance, we conduct simulations using the PowerWorld Simulator. The IEEE

Table 1. Results of Individual and Combined Parameter Perturbations

Perturbation Type	**Parameter**	**Impact on Stability**	**Efficacy**
Individual	Generator active power	Moderate	Moderate
Individual	Generator voltage setpoints	High	Moderate
Individual	Load profiles	Moderate	Low
Individual	D-FACTS devices (affecting line reactance)	High	Moderate
Combined	Generator active power and D-FACTS devices	High	Moderate
Combined	Load profiles, tap settings, and D-FACTS devices	Moderate	High

9-Bus System, with three generators and base kV levels of 13.8 kV, 16.5 kV, 18 kV, and 230 kV, is used as the test case. This system is relatively easy to control due to its limited number of voltage control devices and complex lines of powers of hundreds of MVA each. We consider a range of power system components for perturbation, including generator settings, voltage set-points, load profiles, and D-FACTS devices (affecting the reactances of the transmission lines).

3.2 Individual and Combined Parameter Perturbations

We perform both individual and combined parameter perturbations within their respective operating limits. The perturbations are applied to the 9-Bus System using the SimAuto interface. Based on our proposed algorithm, we can dynamically search for the best parameters to perturb for implementing MTD in power systems. This adaptive approach allows us to select optimal combinations of parameters that maximize the security benefits while minimizing the impact on system stability and performance. The results of these perturbations are presented in Table 1.

3.3 Impact of Perturbations on Power System Stability and Performance

We conduct a sensitivity analysis to identify the most critical parameters significantly affecting the system's stability and performance. The sensitivity indices for each parameter are calculated, representing the relative change in bus voltages per unit change in the parameter. Based on the sensitivity analysis, we identify the most critical parameters, such as load profiles, tap settings and D-FACTS devices (affecting transmission line reactance), and their combinations that can be used to implement an effective MTD strategy while maintaining the system's stability and performance. The findings help develop a more robust and adaptive cybersecurity approach for power systems, considering the trade-offs between security and operational constraints.

4 Discussion and Conclusion

We summarize the key findings of our study on the adaptive MTD strategy for power systems, focusing on the insights from sensitivity analysis and dynamic parameter perturbations. Lastly, we present the conclusion.

4.1 Discussion

Our study presents a MTD strategy that leverages the insights gained from voltage sensitivity analysis and dynamic parameter perturbations. The proposed approach introduces unpredictability and complexity to power systems, making it more challenging for adversaries to plan and execute cyber-attacks. In this direction, the critical parameters and their combinations identified through simulations and sensitivity analysis play a vital role in implementing this defense strategy.

The trade-offs between system security and operational constraints must be carefully managed. While increasing the number of perturbed parameters can improve defense effectiveness, it may introduce additional operational complexities and costs. For instance, deploying D-FACTS devices can enhance system security but requires investment and ongoing maintenance expenses.

4.2 Conclusion

In conclusion, based on voltage sensitivity analysis and dynamic parameter perturbations, the MTD strategy provides a robust and adaptive cybersecurity approach for power systems. By balancing system security and operational constraints, we enhance power system resilience against cyber-attacks and other threats. Future work will evaluate the proposed MTD strategy's effectiveness against stealthy FDI attacks and assess its ability to reveal such attacks by combining them with anomaly detection techniques and Kalman filter-based detection methods. These enhancements will further bolster the defense capabilities of power systems, ensuring their security and reliability amid evolving cyber threats.

References

1. Lakshminarayana, S., Belmega, E.V., Poor, H.V.: Moving-target defense for detecting coordinated cyber-physical attacks in power grids. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). pp. 1–7. IEEE (2019)
2. Talkington, S., Turizo, D., Grijalva, S., Fernandez, J., Molzahn, D.K.: Conditions for estimation of sensitivities of voltage magnitudes to complex power injections. IEEE Transactions on Power Systems (2023)
3. Zhang, M., Fan, X., Lu, R., Shen, C., Guan, X.: Extended moving target defense for ac state estimation in smart grids. IEEE Transactions on Smart Grid (2022)