Research on Attack Penetration Prevention Techniques of Power Terminal Network

Xiaojun Zhou¹, Liming Wang¹*, Yupeng Cai², Shuai Ren², Tong Li², Yidong Yuan³, Qi Li³

¹ Institute of Information Engineering, CAS, Beijing, 100000, China
² Electric Power Research Institute, State Grid Liaoning Electric Power Co., Ltd., Shenyang, Liaoning, 110003, China
³ Beijing Smart-Chip Microelectronics Technology Co., Ltd., Beijing, 100000, China

*Corresponding author’s e-mail: wangliming@iie.ac.cn

Abstract. After the power terminal network is attacked, it is necessary to adopt effective security strategies to block the attack in time to prevent further expansion of the attack damage. At this time, not only the availability of the system must be considered, but also the impact of the attack must be minimized. Traditional network isolation methods may cause excessive protection problems such as excessive isolation range and high isolation strength, and affect the continuity of power system business. Therefore, this paper conducts research on the attack penetration prevention techniques of power terminal network, under the condition of minimally affecting the real-time business continuity of the power grid, blocking low-risk terminals’ control commands and/or isolating high-risk terminals’ communication to realize accurate attack penetration prevention.

1. Introduction

With the continuous integration of all aspects of the power system with modern information technologies such as mobile Internet and artificial intelligence, and advanced communication technologies, the construction of the ubiquitous power internet of things is being steadily carried out. All aspects of the power system will be interconnected and human-computer interaction will be established to develop a smart service system with comprehensive status perception, efficient information processing, and convenient and flexible applications. As a basic component of the ubiquitous power internet of things, the power terminal network is essential for its security, safe and stable operation. However, as we all know, system vulnerabilities are inevitable, as well as network attacks. When the power terminal network is under attack, it is necessary to adopt an effective attack penetration prevention strategy under the condition of ensuring the minimum impact and preventing further spread of the attack.

Khanna et al. proposed a priority-based protection strategy against the malicious data attacks in power grid to selectively protect critical components[1]. Touhiduzzaman et al. colored the security mechanism in the substation, allocated diverse security mechanism through Nash equilibrium, and calculated the criticality of the entire network and protected it[2]. Flick et al. discussed in detail the direct attacks on smart meters and smart devices and the attacks on supporting networks and applications, and gave suggestions on how to defend against these attacks[3]. Ming et al. proposed power grid protection strategy in depth, including physical, terminal, border, network, application and...
data[4]. Tian et al. developed a subjective APT-honeypot game model to prove the existence of Bayesian-Nash equilibrium strategies in defense and attack strategies under bounded rationality[5]. Wang et al. proposed an interval state estimation-based defense mechanism to detect the established cyber-attacks[6]. All these studies have proposed different security strategies, which have played a positive role in the security of the power grid. However, they did not consider how to minimize the impact on the power grid when the security strategy was implemented.

This paper conducts an in-depth study on the attack penetration prevention strategy of the power terminal network. Firstly, a set of attack penetration prevention strategies for the electric power terminal is developed. The terminal equipment, network connection and execution rules in the power terminal network are respectively modeled abstractly to obtain the formal description of the attack penetration prevention strategy set. Then, attack penetration prevention strategies are optimized to obtain a simplified set. The rule set-based algorithm is used to remove the redundancy of the strategy set, and the conflict resolution of the strategy set is carried out with the implementation of negative strategy and the principle of removing the earliest strategy. Finally, specific attack penetration prevention strategies are implemented. Once the terminal network is being attacked, for low-risk power terminals, control commands blocking strategy would be implemented; for high-risk power terminals, network isolation strategy would work. The structure of this paper is as follows: The second part elaborates on the construction process of the attack penetration prevention strategy of the power terminal. The third part is the optimization of the attack penetration prevention strategy set to obtain the simplified strategy set. The fourth part is the implementation process of the attack penetration prevention strategy. The fifth part is a summary of this paper.

### 2. Construction of attack penetration prevention strategy

Firstly, the attacked terminal is determined based on the result of anomaly recognition and network impact analysis is conducted.

In general, the power terminal generally undertakes two tasks: uploading data and issuing control commands. If a power terminal is being attacked, both functions may be affected.

Secondly, breadth-first traversal from the attacked terminal to its upstream and downstream is performed. The direct precursor terminal found in the upstream breadth traversal process is used as the source end set, and the attacked terminal is used as the destination end to form an attack path blocking strategy; Then the attacked terminal is used as the source end, and the immediate subsequent terminals found in the downstream breadth-first traversal process are used as the destination set to form an attack penetration prevention strategy to control the influence of further expansion(shown in figure 1).

Thirdly, the strategies and related elements are formally described. The attack penetration prevention strategy rules(R) are defined as triples consisting of the source set(S), destination set(D), and action set(A), abbreviated as R=(S, D, A). The source set S is the starting point of the path to implement the strategy, the destination set D is the end of the path to implement the strategy, and the action set A represents the behavior implemented from the beginning to the end of the path. And the related elements are also formally modeled.

![Breadth-first traversal from the attacked terminal.](image)
1) Terminal device is modeled as

\[ H = (\text{HostID, Commands, Service, Value}) \] (1)

The meaning of each parameter is as follows: HostID represents the identification of the terminal device, here it is represented by an IP address; Commands represent the strategic commands that the terminal device needs to execute; Service represents the service provided by the terminal device; Value represents the value of the terminal device itself, which can be specified manually.

2) Network connection is modeled as

\[ C = (\text{HFrom, Protl, Hto}) \] (2)

The meaning of each parameter is as follows: Hfrom represents the terminal device that initiated a session; Protl represents the protocol used by the session; Hto represents the connected end terminal device.

3) Execution rule is modeled as

\[ \text{Executive_rule} = (\text{Object, Precond, Postcond}) \] (3)

The meaning of each parameter is as follows: Object represents the object of rule execution; Precond represents a set of preconditions for action execution; Postcond represents a collection of action execution results.

3. Optimization of attack penetration prevention strategy

When the attack penetration prevention strategy set is constructed, the system cannot guarantee that there will be no redundant or conflicting strategies. Therefore, the attack penetration prevention strategy set needs to be optimized.

First of all, it is necessary to design mechanisms for overlapping penetration prevention strategies to achieve orthogonalization, reduce the redundancy of strategies, and improve the efficiency of strategy issuance and execution. Secondly, it is important to conduct conflict removement mechanism to ensure the smooth implementation of the strategy set.

3.1 Redundancy reduction

When there is a tolerable intersection between two or more strategies, it is called strategy redundancy. In order to streamline the strategy set and improve the efficiency of strategy issuance and execution, redundancy must be removed.

According to the model of terminal device, network connection and execution rules, the artificial intelligence correlation analysis method is used to analyze all the strategies involving a certain terminal device. If there is redundancy in the strategy sets \( R_i \) and \( R_j \), after removing the redundancy, it is: \( (R_i - R_j) + R_j \), and the redundancy processing algorithm is as follows (shown in figure 2):

![Redundancy processing algorithm](image)

Then we prove that \( (R_i + R_j) \) is equivalent to \( (R_i - R_j) + R_j \) after redundancy reduction processing, namely \( R_i + R_j \leftrightarrow (R_i - R_j) + R_j \).

Prove Processing:

For \( \forall r' \in (R_i - R_j) + R_j \), obviously \( r' \in (R_i + R_j) \) is true. That is, \( (R_i + R_j) \supseteq (R_i - R_j) + R_j \).
For $\forall r' \in (R_i+R_j)$, if $\forall r' \in R_j$. Obviously, $r' \in (R_i-R_j)+R_j$ is true. That is, $(R_i+R_j) \leq (R_i-R_j)+R_j$.

If $r' \in R_i$:

① if $r' \notin (R_i \cap R_j)$, it can be known from the operational properties that $r' \in R_i-R_j$. That is, $r' \in (R_i-R_j)+R_j$.

② if $r' \in (R_i \cap R_j)$, then $r' \in R_j$ at the same time. that is, $r' \in (R_i-R_j)+R_j$.

So $(R_i+R_j) \leq (R_i-R_j)+R_j$.

In summary: $R_i+R_j \iff (R_i-R_j)+R_j$.

It can be proved that the strategies before and after redundant reduction processing are equivalent.

3.2 Conflict removal

When the goals of two or more strategies cannot be met at the same time, a strategy conflict will occur. In order to ensure the security of the system, the conflict strategy reduction method adopts the negative priority method, that is, the principle of giving priority to the implementation of the negative strategy when there is a conflict between affirmative and negative strategies. The conflict removal algorithm is as follows(shown in figure 3):

![Conflict removal algorithm](image)

Figure 3. Conflict removal algorithm.

After the redundancy reduction and conflict removal of the attack penetration prevention strategies, a relatively simplified strategy set can be obtained.

4. Implementation of attack penetration prevention strategy

According to the deployment characteristics of the extensive interconnection of power terminals, combining the law of power system operation, attack penetration prevention strategies can be classified as control commands blocking strategy and network isolation strategy.

4.1 Control commands blocking strategy

According to the results of the attack assessment, the security level of a specific power terminal can be quantified. For low-risk terminals with low impact on the program, the penetration prevention strategy is instantiated as industrial control protocol packet filtering rules(shown in figure 4). The packet filtering rules are applied to the security equipment (for example, firewall) of the power terminal network through the Simple Network Management Protocol (SNMP). The security equipment of the power terminal network maps the industrial control protocol packet filtering rules to the management objects in the MIB, so that the packet filtering rules are effective in the deep packet analysis (DPI) architecture. The control commands blocking strategy that takes effect upstream of the attacked terminal can effectively limit the issuance of control commands, thereby preventing the attacker from taking further actions and blocking the path of attack penetration; the control commands blocking strategy that takes effect downstream of the attacked terminal restricts the general control commands issued by the risk terminal to prevent the further spread of the hazard. Since there is no restriction on
the data transmission, the control commands blocking strategy can block the path of attack penetration while ensuring that low-risk terminals can continue to return field data for further analysis.

4.2 Network Isolation Strategy
For high-risk terminals with serious impacts, the penetration prevention strategy is instantiated as address or port filtering rules. The address or port filtering rules are applied to the network communication equipment (for example, switches or routers) of the power terminal network through the SNMP protocol. The network communication equipment of the power terminal network maps the address or port filtering rules to the management objects in the MIB, thereby closing the destination address or port. The network isolation strategy that takes effect upstream of the attacked terminal can quickly isolate high-risk terminals and block attacks; the network isolation strategy that takes effect downstream of the attacked terminal limits any data sent from high-risk terminals, thereby preventing the further spread of harm. This method also restricts the uplink and downlink data, so there will be no on-site data return (shown in figure 5).

5. Conclusion
This paper conducts an in-depth study on the attack penetration prevention strategy of the power terminal network. A set of attack penetration prevention strategies for the attacked power terminal is built, optimized and implemented, to achieve preventing further spread of attacks with the least impact on the power terminal network. Theoretical analysis shows that this method can realize the control commands blocking of low-risk terminals and the network isolation of high-risk terminals, which will play a positive role in the network security of power terminals.

Acknowledgments
We thank our colleagues in our research group for providing insightful feedback of the draft that helped improve the final paper. We would also like to thank Jiankai Wang and Wei An for their help in early discussions and providing insightful comments. This work was supported by Security
Protection Technology of Embedded Components and Control Units in Power System Terminal, under grant No.2019GW-12, for which we are grateful. This work was supported by Security Protection Technology of Embedded Components and Control Units in Power System Terminal (No.2019GW-12), and the project code is 5100-201941446A-0-0-00.

References

[1] Khanna, K., Panigrahi, B.K., Joshi, A. (2020) Priority-Based Protection Against the Malicious Data Injection Attacks on State Estimation. IEEE Systems Journal, 14(2):1945-1952.

[2] Touhiduzzaman, M., Hahn, A., Srivastava, A. (2018) A Diversity-based Substation Cyber Defense Strategy utilizing Coloring Games. IEEE Transactions on Smart Grid, 10(5):5405-5415.

[3] Flick, T., Morehouse, J. (2010) Securing the Smart Grid: Next Generation Power Grid Security. Syngress Publishing, Rockland.

[4] Ming, J., Yuan, F., Jiatian, D. (2015) Research on the Security Strategy of Power Grid Enterprises in the Era of Big Data. Information Security and Technology, 10(1):11-16.

[5] Tian, W., Ji, X., Liu, W., et al. (2020) Prospect Theoretic Study of Honeypot Defense Against Advanced Persistent Threats in Power Grid. IEEE Access, 8(1): 64075 - 64085.

[6] Wang, H., Ruan, J., Wang, G., et al. (2018) Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. IEEE Transactions on Industrial Informatics, 14(11):4766 – 4778.