Security Detection Technology of Ubiquitous Power Internet Terminal

Chao Zhou, Wei Huang, Yunxiao Sun, Haitao Jiang, Jing Guo
State Grid Jiangsu Electric Power Co., Ltd. Research Institute, Nanjing, China

Abstract. In order to explore the effect of terminal security system detection in the ubiquitous power internet of things, in this study, the data analysis method is used to study the technology of terminal security detection in the Internet. The research results show that under the influence of Internet, the terminal security of power system has great problems in protocol defects, hacker attacks, various viruses, software vulnerabilities, mis-operation and malicious behavior of users in backdoor network, information leakage, etc. In this study, the combination of VRV system and SVM algorithm to achieve various effective operations can significantly improve the accuracy of terminal security detection, the security has been greatly improved.

Keywords: power; Internet; terminal; security.

1. Introduction
With the development of society, the Internet has been fully improved. For all intelligent enterprises, the use of the Internet in enterprises is extremely important [1-2], because the use of the Internet will generate a lot of enterprise operation data [3-4]. The continuous accumulation of these data will form big data. Using effective algorithms to analyze the data can improve the efficiency of enterprise management very efficiently [5]. However, for the industry with more advanced intelligent technology, although the Internet brings convenience and efficiency at the business level, the network data attack will be multiplied at the same time, and the data security will face a very big test, especially for some key industries. If the security of intelligent manufacturing data cannot be guaranteed, the Internet will not only fail to provide effective help for enterprises, but also bring great trouble. Therefore, how to ensure the security of intelligent manufacturing data and avoid network attacks is very important [6].

In this study, on the basis of the Internet, VRV system and SVM algorithm are mainly used to study the security detection of power Internet terminals by data mining [7]. The core is to study the data security of the power system according to the real situation of the terminal, to ensure that the data will not be attacked, resulting in data loss or modification [8]. The most important thing is that when the data is attacked, it can be intercepted in advance, so as to comprehensively analyze and guarantee the data security of the terminal. Using the algorithm model in this study to analyze and describe the data characteristics of the terminal power grid can accurately defend and intercept the data attacks, so as to develop the later maintenance scheme of the terminal power grid data under the Internet [9]. Various kinds of different data attack methods and types of power failure factors are analyzed and studied to minimize the loss and cost caused by data attack.
In conclusion, in this study, the security detection technology of power terminal under the Internet is studied. The results show that under the influence of the Internet, power terminal security detection has a good performance in the detection level for a variety of security problems in the terminal under the combination of VRV system and SVM algorithm. This study is of great significance and value for the stability and long-term work of the terminal.

2. Methodology

2.1. Research on security threats of Internet power terminals

Protocol defect: The original design of TCP/IP mainly focuses on resource sharing, basically does not consider security issues, and lacks corresponding security supervision mechanism.

Hacker attack: hacker technology is gradually mastered by more and more people, which will not only cause the suspension of power network service and external contact, but also seriously affect the normal safety production of the internal network of the power system [10].

Virus: all kinds of viruses threaten the whole power network system all the time, which makes it have to consider the detection and prevention of all kinds of viruses in all aspects of the network. There is no doubt about the importance of complete virus defense [11].

Software vulnerabilities and backdoors: with the increasing frequency of CPU, vulnerabilities in software systems are inevitable. For example, powerful software like Windows developed by Microsoft also has various security vulnerabilities:

For the mis-operation and malicious behavior of the internal users of the network, the mainstream network security products such as firewalls are basically powerless. For example, someone inside steals the private key by using the password security vulnerability, and replays the stolen authorization information to obtain authorization. The security access risk of power mobile terminal is shown in figure 1.

Information leakage: malicious and negligent unreasonable information upload and release may cause sensitive information leakage, harmful information diffusion and endanger society [12].

| Information Leakage | GPRS APN | Office system, mail system |
|---------------------|----------|---------------------------|
| System leakage      |          |                           |
| Data leakage        |          |                           |
| Loss of hidden danger |        |                           |
| Illegal software    |          |                           |
| System FLAW         | WCDMA APT| ERP system                |
| IMIS forgery        |          |                           |
| Illegal use         |          |                           |
| Physical destruction|          |                           |
| IMIS forgery        |          |                           |
| Other industries    |          |                           |
| Service system      |          |                           |
| ERP system          |          |                           |

Figure 1. Security risk of electric power mobile terminal

2.2. Security inspection measures for power terminal

The virus events detected by the virus prevention system are counted. The terminals with more virus infection are focused on rectification to ensure that they can enter the network again after being in place on the same day. Terminals that fail to be rectified in time will not be used in the network. The firewall system is monitored in time. When finding the abnormal hit strategy, it is necessary to timely interact with the security personnel and the relevant personnel of the business system to ensure that the attack behavior is found as early as possible and the network attack is blocked [13].

Through the deep convinced behavior, the management equipment is exported from the local company to set the behavior security strategy of the external network end users. Through VRV to issue the patch automatic update script, all the internal and external customers can connect to the company's
WSUS server. The client security update is carried out, and the system of "information security daily clearing and daily settlement" is implemented. Problems such as weak password of terminal, non-installation of anti-virus software and non-registration found in security system patrol inspection on the same day must be rectified on the same day. The power mobile terminal area is shown in figure 2.

![Power mobile terminal area](image)

**Figure 2.** Power mobile terminal area

### 2.3. Principle and thinking of security detection for power terminal

The terminal security of power system is very important for the normal operation of power system. If there are many problems in the security of power system, it will bring great hidden danger to the power system. Aiming at the problem of terminal security in power system, in this study, a security detection algorithm based on the combination of VRV system and SVM algorithm is proposed. The protocol defects in the power system terminals are repaired and prompted. In this way, the security risk of virus and attack to the terminal can be reduced as much as possible. Aiming at the problem of hacker attack, in this study, the hacker attack is intercepted and identified, so as to remind the terminal security system to eliminate, and reduce the risk of attack as much as possible. To solve the problem of virus, the technology of this study will kill all external devices of the terminal, prevent virus from entering the system through other paths, and bring security problems. In view of the vulnerability of the terminal's own software, in this study, the terminal software is scanned and detected in an all-round way to prevent the path of virus from being brought in. In view of the risk security problems caused by the user's mis-operation, the possible vulnerabilities are patched. The security access detection logic of power terminal is shown in figure 3. In this study, the risk security problems are mainly reduced by setting multi-level authority and mutual verification. Finally, in view of the security problems caused by information disclosure, the technology of this study is mainly through multi-layer encryption of system data to prevent information disclosure. In addition, in order to solve the problem of information leakage, it is necessary to update and encrypt the terminal information base in time.
2.4. SVM algorithm

Based on statistical learning theory, the algorithm has good generalization ability and classification ability, so it has special advantages in solving high-level pattern recognition, small sample and nonlinear problems.

First, the training sample set should be given.

\[ p = \{(x_i, y_i)\}_{i=1}^{m} \in (\mathbb{R}^n \times Y) \]  \hspace{1cm} (1)

In the equation, \( Y = \{1,-1\}, x_i \in \mathbb{R}^n, y_i \in Y, i = 1,\ldots, m \) (1)

Second, the original algorithm equations (2) - (6) are sorted out. The feasible direction method is used to solve the problem, and the standard equation of quadratic programming is obtained.

\[
\begin{align*}
\max_w (a) &= \sum_{j=1}^{m} a_j - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} y_i y_j k(x_i, x_j) a_i a_j \quad (2) \\
\sum_{i=1}^{m} y_i a_j &= 0, 0 \leq a_i \leq c, i = 1,\ldots, m \quad (3)
\end{align*}
\]

\[
\begin{align*}
\min_w (a) &= \frac{1}{2} a^T G a + r^T a \\
Y^T a &= 0, i = 1, c_i^T a = -a_i \leq 0, i = \{2,\ldots, m + 1\} \quad (4)
\end{align*}
\]

\[
G = (g_{ij})_{m \times n} = (x_i x_j x_k)_{m \times n}^T, \quad r^T = (-1,-1,\ldots,-1), \quad Y^T = (y_1, y_2,\ldots, y_m) \quad (5)
\]

Thirdly, according to equation (7), \( w^* \) is obtained:

\[
w^* = \sum_{i=1}^{m} a_i^* y_i x_i \quad (7)
\]

\( w^* \) is substituted into equation (8) to calculate \( b^* \):

\[
a_i^* [y_j (w^T x_i + b^*) - 1] = 0 \quad (8)
\]

The classification hyperplane is determined by \( w^* \) and \( b^* \):
2.5. Security deployment system of power terminal

According to the process of terminal, the security detection of power system terminal can also be divided into pre installation and operation process. Inspection before installation is also extremely important. Detecting the device before use can eliminate the threat such as virus before operation. The time and proportion of virus detection in the running process are the largest. The deployment mode of security terminal is shown in figure 4. The deployment of power system terminals is very demanding and regular. The most important principle is to supervise, coordinate and help each other. Communication and information transmission between terminals only use special encrypted channels. With the development of society, the power consumption of power system is larger and larger, the types and quantity of power system terminals are more and more open, and the internal operation network is more and more complex. Therefore, the security and deployment of power terminals will play a very important role. In addition to external detection and prevention, the security of the terminal also needs the power of its own security system. It needs to install a powerful anti-virus and interception system, back up and encrypt the transmitted data, and clearly divide the operation authority of internal personnel to prevent information from being stolen and leaked by internal personnel. It can be seen that the terminal security detection of power system is an ecosystem project, which requires a lot of investment and coordination to achieve remarkable results.

![Security terminal deployment mode](image_url)

**Figure 4.** Security terminal deployment mode

3. Results and discussion

![Comparison of security detection accuracy of power terminals under the Internet](image_url)

**Figure 5.** Comparison of security detection accuracy of power terminals under the Internet
The comparison of security detection accuracy of power terminals under the Internet is shown in figure 5. It can be clearly seen from the figure that the accuracy of power terminal security monitoring rate based on VRV system and SVM algorithm under the Internet is higher than that of the previous power terminal security detection, no matter in the aspects of protocol defects, hacker attacks, various viruses, software vulnerabilities, mis-operation and malicious behavior of internal users of backdoor network, information leakage and other security factors. Therefore, VRV system and SVM algorithm are very helpful in terminal security detection of Internet power system.

![Accuracy Rate Comparison](image)

**Figure 6.** Research on the stability of power terminal security detection under the Internet

The stability of power terminal security detection under the Internet is shown in figure 6. It can be clearly seen from the figure that under the effect of Internet, the algorithm stability of power terminal security monitoring based on VRV system and SVM algorithm is very good, and the fluctuation is very small. It can be seen that the algorithm model used in this study is reliable for power terminal security detection under the Internet, and the detection data is real and reliable.

4. Conclusion

In this study, power terminal security detection technology under the Internet is studied. The research results show that the combination of VRV system and SVM algorithm has significant accuracy and stability in the detection of protocol defects, hacker attacks, various viruses, software vulnerabilities, mis-operation and malicious behavior of users in backdoor network, information leakage and other aspects. There are also some deficiencies in the research process of this study, and the terminal security risk factors are very many. In this study, some common factors are mainly analyzed and studied, and there are many types of terminals and different working methods. In this study, common terminals are mainly analyzed and studied. In the process of practical application, there will be more problems in terminal security than in the research process. In the research process, these objective factors are not fully considered, but this study is of great significance for the follow-up research in this field.

References

[1] Dai Xianzhong, Han Xinyang, Dong Yihua, Luo Haihua, Li Yu. Research on Multi-source and Multi-level Coordination Optimization Method of Energy Internet. Electric power engineering technology. 2019, 38 (2), pp, 1-9.

[2] Farhadi M, Mohammed O A. Protection of multi-terminal and distributed DC systems: Design challenges and techniques. Electric Power Systems Research, 2017, 143, pp. 715-727.

[3] Yang Jiru, Gao Zhiwei, Su Weihua. A Review of the Optimal Scheduling of the Energy Internet. Electric power engineering technology. 2019, 38 (1), pp, 49-55.

[4] Zhang Y, Chen M, Guizani N, et al. SOVCAN: Safety-oriented vehicular controller area network. IEEE Communications Magazine, 2017, 55(8), pp. 94-99.

[5] Haghnavaz S, Khodabandeh M, Zolghadri M R. Fast fault detection method for modular
multilevel converter semiconductor power switches. IET Power Electronics, 2016, 9(2), pp. 165-174.

[6] Palattella M R, Dohler M, Grieco A, et al. Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 2016, 34(3), pp. 510-527.

[7] Akpakwu G A, Silva B J, Hancke G P, et al. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE Access, 2017, 6, pp. 3619-3647.

[8] Sikorski J J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy, 2017, 195, pp. 234-246.

[9] Centenaro M, Vangelista L, Zanella A, et al. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. IEEE Wireless Communications, 2016, 23(5), pp. 60-67.

[10] Alaa M, Zaidan A A, Zaidan B B, et al. A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications, 2017, 97, pp. 48-65.

[11] Sicari S, Cappiello C, De Pellegrini F, et al. A security-and quality-aware system architecture for Internet of Things. Information Systems Frontiers, 2016, 18(4), pp. 665-677.

[12] Wang S, Fernandez C, Chen M, et al. A novel safety anticipation estimation method for the aerial lithium-ion battery pack based on the real-time detection and filtering. Journal of cleaner production, 2018, 185, pp. 187-197.

[13] Zamani R, Hamedani-Golshan M E, Haes Alhelou H, et al. Islanding detection of synchronous distributed generator based on the active and reactive power control loops. Energies, 2018, 11(10), pp. 2819.