Analysis of Terminal Security Access Technology under Ubiquitous Power Internet of Things

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

Abstract. In order to explore the effect of safe access of power system terminals under the action of the Internet of things, the safe access technology of power terminals under the Internet of things was studied by means of data analysis. The results showed that under the role of the Internet of things, power system terminals have excellent performance in self-verification of modules and data security detection before access. In the access, its combination of Security Socket Layer (SSL) protocol and improved Support Vector Machine (SVM) algorithm can effectively carry out data transmission evaluation protection and network security maintenance, as well as self-data destruction and remote control of the terminal after access. To sum up, the Internet of things showed a very significant effect on the security level of power terminal before, during and after the access, and greatly improved the work efficiency, false alarm rate and accuracy rate of the terminal in the later period. Therefore, this research is of great significance for the analysis of secure access of power system terminals under the Internet of things.

Keywords: electric power; Internet of things; terminal; access.

1. Introduction
With the promotion of smart grid construction, more and more terminals of different types need to be connected to power enterprise Intranet remotely to exchange data with Intranet application systems [1-2]. On the other hand, with the development of mobile application technology, power enterprises are expanding their production and management services to mobile terminals[3]. At present, many terminals in the market have very low safety coefficient and face very large security risks [4,5]. If people want to change it, they should combine software and hardware to make purpose-oriented improvements in all aspects, and make specially designed terminals without security risks for power enterprises. Moreover, complete systems and regulations are needed to ensure the safety of the work they are responsible for, so as to avoid attacks and data leaks [6,7]. Based on the research on the safety requirements of power system terminals, it is concluded that power terminals should meet the following requirements. The terminal needs of the power system can meet the required security guarantee to achieve the judgment and review of the core parts, work procedures, data integrity, safety assessment, etc., so as to ensure that the terminal is in an environment without hidden dangers [8,9]. The system terminal needs to have a mature security control system, so as to realize the verification of logins' identities. It should control the changes of users' permissions, ensure the smooth and safe information transmission between programs, and prevent data loss and changes caused by attacks on programs [10].
In addition, the traditional network connection technology based on fixed physical location can’t meet the needs of power enterprises. Most mobile terminals access enterprise Intranet through wireless network, making wired network access control technology no longer applicable [11]. Finally, with the expansion of power enterprises' mobile services, mobile applications will cover all fields of power enterprises' informatization, making business processing of mobile terminal more diversified. This requires that mobile access is not a single simple mode, but a diversified complex mode [12].

In summary, the research on the security access technology of power terminals under the Internet of Things is carried out in this study. The results show that the power terminals under the influence of the Internet of things perform well no matter before, during or after the access, which is of great significance for the later terminal work. The innovation of this study lies in the analysis and research of terminal access from the previous, middle and last levels. The research analysis is relatively comprehensive, and the research ideas and results have great reference value for the follow-up research.

2. Methodology

2.1. Power terminal access security requirements under the Internet of things

At present, many terminals in the market have very low safety coefficient and face very large security risks. If people want to change it, they should combine software and hardware to make purpose-oriented improvements in all aspects, and make specially designed terminals without security risks for power enterprises. What’s more, complete systems and regulations are needed to ensure the safety of the work they are responsible for, so as to avoid attacks and data leaks. According to the research on the safety requirements of power system terminals, it is concluded that power terminals should meet the following requirements. The specific demand flow chart is shown in figure 1. The terminal of the power system can meet the required security guarantee to achieve the judgment and audit of the core parts, the audit of working procedures, the audit of data integrity, the safety assessment of the terminal of the power system, so as to ensure that it is in an environment without security risks and threats. The system terminal needs to have a mature security protection system and implement an isolation plan for the program infected by virus, so as to realize the verification of the identity of the login personnel. It could control the changes of users' permissions, ensure the smooth and safe information transmission between programs, and prevent data loss, changes, and removals caused by attacks on programs. Power system terminals need to be equipped with the ability to judge whether data carry viruses, so as to realize the classification and storage of data. For data with different threat levels, corresponding security means should be adopted, and a mature risk assessment system should be established to evaluate and judge unknown risks. The system terminal also needs to have functions such as data repair and self-destruction, such as deleting data and repairing sensitive data to avoid leakage.

Figure 1. Power terminal security requirements flow chart
2.2. Power terminal security design ideas under the Internet of things

In this study, according to the security access system architecture of power terminals based on the Internet of things, the general idea was to meet the needs of terminals through three-level protection measures. The process of secure access of the terminal was divided into three processes to implement, that is, before access, during terminal access, and after terminal access. The three processes were treated differently and targeted safety analysis was conducted. Three-level differential treatment design was a system studied according to the threats faced by terminal access in the three processes of terminal, transmission, and work respectively, as shown in figure 2. The design process was as follows: first, terminal design. The terminal was upgraded and re-evaluated, the hardware with higher safety factor was replaced, the anti-virus and interception software was loaded, the risk assessment module and data transmission module were installed. The most important thing was to carry out a comprehensive assessment of possible risks and hidden dangers of the terminal before access, so as to ensure that the terminal itself was safe and without hidden dangers, and to strengthen the protection, attack and defense ability of the terminal in the event of danger. It completely ensured that the terminal had no hidden dangers and risks, that is, the danger was eliminated before the access. Second, channel design. SSL protocol was redesigned to cooperate with each other, and at the level of combining SSL protocol, a more advanced SSL protocol was proposed. This kind of protocol could achieve a more detailed review of identity, which had stronger risk resilience and ensured that the channel was secure. Third, the protection design of application system. The internal network security assessment system was designed to ensure the security of the system.

![Secure terminal architecture](image)

**Figure 2. Secure terminal architecture**

2.3. Improvement of SSL protocol

Data security is the lifeline of power enterprises. In the secure access system of power terminals, ensuring the safety of data transmission channels is also the most basic requirement of information security of power enterprises. At present, the realization of terminal remote access to enterprise Intranet and communication with enterprise Intranet application system is mostly realized through Virtual Private Network (VPN). With public network channel and secure encryption technology, a private logical channel is established between terminal and enterprise Intranet. Among them, SSL protocol is the most widely used VPN solution technology, which can achieve the communication security requirements of VPN. Others need to install the corresponding client, which has poor communication compatibility and is not convenient for maintenance management. SSL is based on Hyper Text Transfer Protocol (HTTPS) to access the enterprise Intranet application system through the browser, without the need to install customized client software, with better scalability and security. The SSL protocol structure is shown in figure 3.
Application Layer Protocol
ssl handshake protocol
SSL Change Password Protocol
SSL Alarm Protocol
SSL Record Protocol
User Data Packet Protocol (UDP)
Transmission Control Protocol (TCP)
Internet Protocol (IP)

Figure 3. The structure of the SSL protocol

Therefore, in order to ensure the security of data transmission between terminal and Intranet application system, and the confidentiality and integrity of data in the transmission process, SSL protocol was selected in this research and combined with Public Key Infrastructure (PKI) technology. SSL control protocol based on PKI were proposed, which could effectively prevent information from being stolen or tampered during transmission.

2.4. Improvement of SVM algorithm
SVM is a machine learning algorithm proposed by Vapnik et al. Based on the statistical learning theory, this algorithm has good generalization ability and classification ability. Therefore, it has special advantages in solving high-order pattern recognition, small sample and nonlinear problems. The service terminal flow of SVM algorithm is shown in figure 4.

The idea of SVM algorithm was to find a hyperplane and use it to separate two different sets. The following two-dimensional space was taken as an example to illustrate the algorithm. The SVM algorithm was to find a line to separate the black and white points in the figure, and the larger the distance between the line and the two sets of boundaries, the better. In fact, the improvement of SVM algorithm was to improve the solving speed of quadratic programming problem. The efficient feasible direction method was used to solve the quadratic programming problem.

The sample set for training was given:

\[ p = \{(x_1, y_1), \ldots, (x_m, y_m)\} \in (\mathbb{R}^n \times Y)^m \]

\[ Y = \{1, -1\} \]

\[ x_i \in \mathbb{R}^n, y_i \in Y, i = 1, \ldots, m \]

(1)

After sorting out the original algorithm formula (2) - (6), the feasible direction method was used to solve it, and the standard quadratic programming formula was obtained:

\[ \max w(a) = \sum_{j=1}^{m} a_j - \frac{1}{2} \sum_{i=1}^{m} \sum_{j=1}^{m} y_i y_j k(x_i, x_j) a_i a_j \]

(2)
\[
\sum_{i=1}^{m} y_ia_j = 0,0 \leq a_i \leq c, i = 1,2,..., m
\]  
(3)

\[
\min w(a) = \frac{1}{2} a^T G a + r^T a
\]  
(4)

\[
Y^T a = 0, i = 1, c_i^T a = -a_{i-1} \leq 0, i = \{2, ..., m + 1\}
\]  
(5)

\[
G = (g_{ij})_{m \times n} = (x_i x_i x_i)_{m \times n}, r^T = (-1,-1,...,-1), Y^T = (y_1, y_2, ..., y_m).
\]  
(6)

According to formula (7), \(w^*\) could be obtained:

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

\(W^*\) was substituted into formula (8) to calculate \(b^*\):

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

The classification hyperplane was determined by \(w^*\) and \(b^*\):

\[
f(x) = w^* x + b^* = \sum_{i=1}^{m} a_i^* y_i x_i x + b^*
\]  
(9)

3. Results and discussion

*Figure 5.* Comparison chart of detection accuracy of power terminal access under the Internet of things

The comparison of power terminal access detection accuracy under the Internet of things is shown in figure 5. In the figure, it can be clearly observed that the detection accuracy of power terminals after secure access based on SSL protocol and SVM algorithm under the Internet of things was much higher than that of the terminals when the Internet of things was not combined before, no matter in the aspects of terminal self-audit, risk assessment, virus defense, program isolation, data transmission or network security. It can be concluded that the Internet of things was of great help to the secure access of power system terminals and had a significant effect.
Figure 6. Comparison of the security access efficiency of power terminals under the Internet of Things

The comparison of power terminal security access efficiency under the Internet of things is shown in figure 6. It can be clearly observed from the figure that under the influence of the Internet of things, the working efficiency of power terminals after secure access based on SSL protocol and SVM algorithm, no matter in the aspects of risk assessment, virus defense, program isolation, data transmission or network security, was more improved than that of terminals when the Internet of things was not combined before. Therefore, it can be concluded that the Internet of things had a great effect on the secure access of power system terminals.

Figure 7. Comparison of false alarm rate of power terminal security access under the Internet of Things

The comparison of false alarm rate of power terminal security access under the Internet of Things is shown in Figure 7. It could be clearly observed from the figure that under the influence of the Internet of things, the false alarm rate of the power terminal after secure access based on SSL protocol and SVM algorithm was much lower than the false alarm rate of the terminal when the Internet of things was not combined before, both in terms of data transmission and network security. Therefore, it can be concluded that the Internet of things had a significant effect on the secure access of power system terminals.

4. Conclusion

In this study, the secure access technology of power terminals under the Internet of things was studied. The results showed that under the action of the Internet of things, the power system terminal showed very good effect, including self-verification and self-security detection of modules before access, combination of SSL protocol and improved SVM algorithm during access for risk assessment, virus defense, isolation, data security transmission, and network attack defense, self-protection, remote control and data destruction of terminals after access. There are also some deficiencies in the research process. Technical and theoretical problems need to be further improved. What's more, there are many
kinds of terminals and different working modes. The Internet of things technology is relatively immature at present, and there will be a lot of unexpected problems in the practical application. These objective factors are not fully considered in the research process, but the results of this research provide a very valuable reference for the follow-up research in this field.

Acknowledgments
This work was supported by State Grid Jiangsu Electric Power Co., Ltd Science and Technology Project (5210EF18002J).

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] 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.
[3] 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.
[4] Botta A, De Donato W, Persico V, et al. Integration of cloud computing and internet of things: a survey. Future generation computer systems, 2016, 56, pp, 684-700.
[5] Yaqoob I, Ahmed E, Hashem I A T, et al. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 2017, 24(3), pp, 10-16.
[6] 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.
[7] 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.
[8] Qiu T, Chen N, Li K, et al. Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks, 2017, 55, pp, 143-152.
[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] Yang A M, Yang X L, Chang J C, et al. Research on a fusion scheme of cellular network and wireless sensor for cyber physical social systems. Ieee Access, 2018, 6, pp, 18786-18794.
[12] 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.