Real Time Implementation of Terminal Security Policies Selection Based on Edge Computing

Aidong Xu¹, Qianru Wang², Yixin Jiang¹, Zhongqi Mao², Wenjing Hou¹, Yunan Zhang¹ and Hong Wen²

¹Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
²School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
Email: sunlike@uestc.edu.cn

Abstract. There are many kinds of terminals in the smart grid system, which have different functions and risks in the system. Different security policies are needed to protect the terminals. At the same time, the terminals will be subject to various attacks in operation. These attacks will change the security protection performance of terminals. Therefore, it is necessary to adjust the security policies in their operation. This paper proposes a real-time implementation method of terminal security policy selection under the edge computing based on the machine learning methods, which makes full use of the computing power of edge devices, adopts offline training and online judgment. The training of machine learning parameters can be completed in the edge side or in the cloud while the security strategies selection continues going on the edge computing side. By this way, the real-time training update and real-time selection of security policy in edge computing system are realized.

1. Introduction
Facing the access of a large number of heterogeneous terminals in the Internet of things (IoT) and the requirements of different applications, the system architecture based on edge computing has emerged, which meets the low delay requirements of industrial real-time control, unmanned driving, virtual reality and other application scenarios [1-6]. Providing the security policies for the terminals is one of the main tasks for the edge system. Different security policies will be proposed to the different terminals according to their functions and risks in the system [7,8]. However, the functions may be extended and the security risks that the terminal faces will change due to the running environment changing. It is necessary to adjust their security policies according to their running situation [9]. Real-time response is essential to the edge computing system, therefore, the training update of the security policies selection system should not influence the security policies selection process to perform on time [10]. By taking advantages of the edge computing resource power and the interaction of the edge side and the cloud, the paper proposes a real-time implementation method of terminal security policy selection under the edge computing based on the machine learning methods.

2. Edge Computing Security Policies Selection Scheme
As shown in Figure 1, the edge computing system includes cloud computing device, edge computing device and terminal device. The connection between edge computing device and cloud and terminal device is wireless connection or wired connection. The security policies selection is carried out in the...
edge side computing devices, and the security policies selector training can be carried out in the edge side or in the cloud, and real-time scheduling can be carried out according to the resource situation of the edge side.

**Figure 1.** Edge computing and physical layer authentication

The quantitative value of security protection for the $i$th terminal among $P$ security policies is [13, 14]:

$$Z_i = [Z_{i1} \ Z_{i2} \ … \ Z_{ij} \ … \ Z_{ip}] \quad (i = 1, 2, \ldots k; \ j = 1, 2, \ldots p)$$  \hspace{1cm} (1)

where $Z_{ij}$ is the quantitative value of security protection, which means $j$th security policy for the $i$th terminal.

Each time the edge device can choose one or several security policies to protect the terminal from $P$ security policies, which will be chosen by the machine learning (ML) algorithms as following.

a) The edge devices will determine the number of security policies $P$ according to the number of the terminals $k$. A security policy is denoted as $y_j^i$ ($i = 1, 2, \ldots k; \ j = 1, 2, \ldots p$), which is $j$th security policy for the $i$th terminal. We combine the Quantitative value of security protection in Eq. (1) with the security policy $y_j^i$ as a data set $D = \{(Z_{i1}, y_{11}), (Z_{i2}, y_{12}), \ldots, (Z_{ip}, y_{1p})\}$.

b) Divide the data set $D$ as two parts. The first $m$ items of the data set is the training set $T$, and the last $n$ items is the test set $S$, where $k = m + n$. In other words, the proportion of training set $T = \{(Z_1, y_1), (Z_2, y_2), \ldots, (Z_m, y_m)\}$ to data set is $\frac{m}{m+n} \times 100\%$, and the proportion of test set $CHE = \{(Z_{m+1}, y_{m+1}), (Z_{m+2}, y_{m+2}), \ldots, (Z_{m+n}, y_{m+n})\}$ to data set is $\frac{n}{m+n} \times 100\%$.

c) The training set $T = \{(Z_1, y_1), (Z_2, y_2), \ldots, (Z_m, y_m)\}$ is used to train the machine learning algorithm until the rate of the safety quantification standard is met. The threshold value $\eta = \{\eta_1, \eta_2, \ldots, \eta_k\}$ is the performance evaluation value of the machine learning algorithm obtained by training and it can be a numerical value or a group of values. When the machine learning algorithm meets the threshold value $\eta$, the machine learning algorithm state is recorded as $\Omega = \{\Phi_1, \Phi_2, \ldots\}$.

d) After the training, the test set $CHE = \{(Z_{m+1}, y_{m+1}), (Z_{m+2}, y_{m+2}), \ldots, (Z_{m+n}, y_{m+n})\}$ is input into the machine learning algorithm to get the corresponding security policy, which is denoted as
Where $RE_i$ represents the security policy $\{j_1,j_2,\cdots\}$ that is selected for the $i$th terminal, and $j_1, j_2$ are one of the P security policies. At this time, the machine learning algorithm state is $\Omega$ and meets the threshold $\eta$. The security policy of the $i$th terminal is obtained by the set training $\{j_1,j_2,\cdots\}$ that is trained by the set $CHE$.

3. The System Update Training Scheme

In the operation, the terminals will be subject to various attacks, which will change the security protection performance of terminals. The function extension of them also will cause requirement of the new security protection. Therefore, it is necessary to adjust the security policies in their operation. The update training scheme as following.

![Figure 2. The system model of PL authentication](image)

As illustrated in Figure 2, when the performance evaluation value of machine learning algorithm can not meet the pre-set threshold value $\eta=\{\eta_1, \eta_2, \cdots, \eta_k\}$, it needs to be retrained. In order to ensure the uninterrupted selection of security policies, it generally needs to start training in advance $\Delta t$ (this value is an advance time when the performance evaluation value of machine learning algorithm may not meet the pre-set threshold $\eta$ ), as follows:

a) Perform offline execution of B), c) and D of Section 2 on the edge side or the cloud, and get the new state of machine learning algorithm as $\Omega_0=\{\Phi_{x,1}, \Phi_{x,2}, \cdots\}$;

b) At the same time, at the edge side, the security policies selection of the terminals still uses the old machine learning algorithm state $\Omega=\{\Phi_{t,1}, \Phi_{t,2}, \cdots\}$;

c) When the training is completed, the security policies selection of the terminals is denoted as:

$$RE_i=\left\{\Omega_0, \eta\left|CHE\right\{j_1,j_2,\cdots\}\right\}$$

(3)

The training samples can be label samples specially prepared for training or real-time samples selected dynamically.
4. Conclusions
The proposed scheme makes full use of the computing power of the edge device, and adopts the way of offline training and online judgment, so that the training of security policies selector can be completed on the edge side or in the cloud. The implementation of security policies selector on the edge device are not interrupted or delay due to training, which realizes real-time selector update and real-time selection of security policies selection of edge computing system. The security protection of the terminals can synchronize with the application environment and avoid to weaken the security performance due to the function extension and the malicious attacking.

5. Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

6. References
[1] Chen S, Wen H, Wu J S et al., 2019 Internet of Things Based Smart Grids Supported by Intelligent Edge Computing, IEEE Access, vol 7 p74089-74102.
[2] McDaniel P and McLaughlin S, 2009 Security and Privacy Challenges in the Smart Grid, IEEE Security & Privacy, vol 7 p 77-77.
[3] Xie F, Wen H, Li Y, Chen S, Hu L, Chen Y, Song H, 2018 Optimized coherent integration-based radio frequency fingerprinting in Internet of Things, IEEE Internet of Things Journal, 5 (5), 3967-3977
[4] Pan F, Pang Z, Luvisotto M, Xiao M, Wen H 2018 Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions, IEEE Industrial Electronics Magazine, vol 12 p 18-27.
[5] Chen Y, Wen H, Song H, Chen S, Xie F, Yang Q, Hu L, 2018 Lightweight one-time password authentication scheme based on radio frequency fingerprinting, IET Communications, vol 12, p 14477-1484.
[6] L Hu, H Wen, B Wu, F Pan, RF Liao, H Song, J Tang, X Wang, 2018 Cooperative jamming for physical layer security enhancement in Internet of Things IEEE Internet of Things Journal 5 (1), 219-228
[7] Yang Q, Jiang Y, Xu A, Wen H, Wang F, Chen L, 2017 A Model Divides the Mobile Security Level Based on SVM, IEEE CNS 2017.
[8] Dan S, Kai Z, Xiang W, et al. 2013 PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Network, IEEE Journal on Selected Areas in Communications, vol 31 p 1817-1827.
[9] Wen H, Ho P H and Wu B 2014 Achieving secure communications over wiretap channels via security codes from resilient functions, IEEE Wireless Communications Letters vol 3 p 273-276
[10] Li Y S, Chen L F, Chen J et al., A Low Complexity Feature Extraction for the RF Fingerprinting Process, CNS2018.
[11] Idrees F, Rajarajan M, Conti M , et al., 2017 PIndroid: A novel Android malware detection system using ensemble learning methods, Computers & Security, vol 2017, p 36-46.
[12] Wen H, Wang Y, Zhu X, Li J and Zhou L, 2013 Physical layer assist authentication technique for smart meter system, IET Communications, vol 7 p 189-197.
[13] Xu A D, Wang Q R, Jiang Y X, Liao R F, Zhang Y N, Chen Y, Wen H, Du J R, 2019 Quantitative selection of secure access policies for edge computing side terminals, ICICTA2019.
[14] Wen H, Xu A D, Wang Q R, Jiang Y X, 2019 Quantitative selection of secure access policies for terminals based on edge computing, Chinese patent, issued no. 2019107543210.
[15] Wen H, Ho P H, Gong G, 2009 A novel framework for message authentication in vehicular communication networks, 2009 IEEE Global Telecommunications Conference, 1-6