New Features of Automatic Meter Reading System:
Based on Edge Computing

Wen-xin LEI¹, Yi-xin JIANG², Hong WEN¹,*, Ai-dong XU², Zhe MING², Wen-jing HOU¹ and Yu-jun YIN¹

¹National Key Lab of Commun., University of Elec. Sci. and Tech. of China, Chengdu 610054, China
²EPRI, China Southern Power Grid Co. Ltd., Guangzhou, China
*Corresponding author

Keywords: Smart Grid, Automated Meter Reading (AMR), Concentrator, Edge computing, Security.

Abstract. In this paper, we focus on edge computing in smart grid and have improved the automated meter reading (AMR) system. In addition, to achieve security processing of a large number of intelligent terminals and massive data in real time and efficient responses, this paper presents an open platform which is developed on the edge of the network close to the power terminal devices or data sources, and proposes a security protection framework of smart grid based on edge computing. As a result, this new AMR system can provide real-time services, possess abilities of efficient data processing and applied intelligence, and effectively resist attacks on smart grid.

Introduction

With the continuous deepening of the reform of the national power system, the power sector has adopted a high-efficiency, low-cost and highly practical meter reading system, namely low-voltage automated meter reading (AMR) system [1].

In recent years, with the advancement of the national “Energy Production and Consumption Revolution Strategy 2016-2030” [2], the sales side is liberalized and the smart power service is promoted. A large number of terminal devices and multiple users on the demand side access the power grid and participate in the interaction. In this context, data flow between electrical devices and control centers, between grid companies and power users in continues to rise [3]. Moreover, with the increasing application range of electrical devices, the time and space distribution of it is more dispersed than the traditional ones, which makes the data collection and analysis face a huge test. In terms of security, the multi-power end-users supply and demand for a variety of interactive electricity, bringing convenience while serious security and confidentiality issues [4]. Therefore, power terminal security protection is unprecedentedly challenged.

Related Work

Edge computing refers to providing an open platform for connection, computing, storage and application near the network edge of terminal devices or data sources, and providing edge intelligent services for the data of power sensor node devices [5]. Based on this, we deploy edge computing models for AMR system as showing in Figure 1, which uses the meter reading concentrator integrated edge computing module to bring some new features. It is geographically close to terminal devices and data sources, able to realize parallel processing and analysis of various acquisition terminals, intelligent devices and power user data in the smart grid at the edge of the information network. The distributed information computing service mode of edge computing with large data volume and fast response can meet the rapid response requirements of equipment and users in smart grid.

According to the edge computing architecture [6], the edge security protection architecture is mainly from the aspects of device domain security, network domain security, data domain security, and application domain security. Security protection, connected by applying a domain cloud
application. Data domain security and application domain security mainly involve data processing and storage security. Device domain security and network security domains mainly involve access and transmission security protection.

For the existing AMR system of smart grid, we propose the specific power terminal security architecture of the edge computing module as shown in Figure 2. The concentrator here analyses the protocol through the edge module, including the following core functions. The core security module of edge computing module can verify and identify the identity information of visiting devices to block the access of malicious node devices, protect the security of data transmission, protect the security of data storage and processing, and protect the real-time attacks. If an attack is detected, control actions are initiated, and a packet blocking command is issued to avoid delay.

Application of Meter Reading Concentrator with Edge Computing Module

Malicious Electricity Behavior Recognition

By collecting the electricity usage of the electricity meter, using the electricity consumption and the time of electricity consumption of each meter, the electricity usage behavior of each meter is
established. Here, the normal electricity consumption behavior is identified by monitoring the electricity consumption behavior of electricity meters triggered by sudden or periodic changes. Then, we assess and record the damages caused by changes in electricity consumption behavior to the power grid, and report the changes in electricity consumption and evaluation results to the management center.

With the physical characteristics of power terminals as a supplement, a lightweight behavior recognition and authentication mechanism [7] for new power terminals based on passwords is designed in a cross-layer manner, as shown in Figure 3.

After the terminal A authenticates the edge B, the two parties start data communication, extract feature information from each received data, and compare with the feature information at the previous moment to determine whether the feature information is legal:

If the feature information is legal, the packet is demodulated to record the legitimate power usage behavior of the user:

$$\Lambda_i = \frac{K_{co} \|H_i(k) - H_{i-1}(k)\|^2}{\|H_{i-1}(k)\|^2} \leq \text{threshold}.$$  

(1)

If the feature information is not legal, the abnormal power consumption information is recorded, and report the change information and evaluation results of the electricity use behavior to the management center.

$$\Lambda_i = \frac{K_{co} \|H_i(k) - H_{i-1}(k)\|^2}{\|H_{i-1}(k)\|^2} > \text{threshold}.$$  

(2)

Real-time Electricity Price Forecast

By collecting the electricity usage of the electricity meter and predicting the real-time electricity price under the national pricing constraint, it can be sent to the user through the APP method for the user to select the power usage time.

A real-time electricity price prediction method [8] based on Long Short Term Memory (LSTM) [9] in the Recurrent Neural Network (RNN) is embedded in the edge computing module as shown below.

The LSTM architecture consists of a set of memory blocks, and each block contains many self-connected memory cells each with an associated state of cell and three gates.

Input gate:

$$i_t = \sum_{i=1}^{L} \omega_{li} x_t^i + \sum_{c=1}^{C} \omega_{ci} c_t^{i-1} + \sum_{b=1}^{H} \omega_{bi} h_t^{i-1}.$$  

(3)
Forget gate:

\[ f'_o = \sum_{i=1}^{I} \omega_{oi}x'_i + \sum_{c=1}^{C} \omega_{oc}x'_{c-1} + \sum_{h=1}^{H} \omega_{oh}b'_{h-1}. \]  

(4)

Output gate:

\[ o'_m = \sum_{i=1}^{I} \omega_{mo}x'_i + \sum_{c=1}^{C} \omega_{mc}x'_{c} + \sum_{h=1}^{H} \omega_{mh}b'_{h}. \]  

(5)

Figure 4. Long Short Term Memory Method for Electrical Price Predict.

Figure 4 shows the result of Long Short Term Memory method for electrical price predicted.

Summary

The new AMR system proposed in this paper adds the ability of edge computing. By deploying the edge computing mode on smart grid, the power of computing is dropped from the main station of power grid system to the edge of the network, realizing new functions such as real-time services, efficient data processing, and applied intelligence. At the same time, the security protection framework of smart grid based on edge computing constructed in this paper effectively avoids the physical, data and time stereo attacks faced by the grid system and meets the different requirements of intelligent power system.

Acknowledgement

This research was financially supported by National Key R&D Program of China (2018YFB0904900, 2018YFB0904905)

References


