Hindawi
Complexity
Volume 2020, Article ID 3186394, 15 pages
https://doi.org/10.1155/2020/3186394

Research Article

A WeChat-Based System of Real-Time Monitoring and Alarming for Power Grid Operation Status under Virtual Private Cloud Environment

Chunjie Lian, Hua Wei, Xiaoqing Bai, and Zhongliang Lyu

Guangxi Key Laboratory of Power System Optimization and Energy Technology, Guangxi University, Nanning 530004, Guangxi, China

Correspondence should be addressed to Chunjie Lian; lianchunjie96@163.com

Received 5 August 2019; Revised 20 September 2019; Accepted 25 September 2019; Published 7 March 2020

Guest Editor: Xuyun Zhang

The existing power grid alarm system using SMS (SMSAS) is complex and suffers some problems such as high latency in data transmission, low reliability, and poor economy. For solving these problems, this paper proposes a WeChat-based system under the virtual private cloud environment to achieve real-time monitoring and alarming for the power grid operation status (WMAS). For WMAS, the WeChat mini program (WMP) is adopted, and it has the dedicated data channel using the Https protocol, which is set up in the WMP and the web API to encrypt the data content to ensure the integrity of the data. Combined with virtual private cloud technology, the hardware resources are virtualized, and the proposed system has strong disaster recovery capability, which significantly improves the flexibility and reliability of the system. Compared with SMSAS, our simulation shows that the time from sending to receiving the information in the proposed system is reduced from 4.9 seconds to 172 milliseconds, with the latency reduced by 28 times. On the contrary, the reliability of the proposed system is as high as 99.9971%, and the annual failure time is 15.24 minutes, which is 380 times lower than 96.51 hours of the SMSAS. The proposed system has been implemented in the Lipu power system in Guangxi, China. More than one year of stable operation indicates that the proposed system is safe, reliable, flexible, and convenient with a bright prospect for future applications.

1. Introduction

Currently, the smart grid has become the future development direction of the power industry [1]. As an essential part of the smart grid, the power grid alarm system (PGAS) is used as advice to system operators relating to problematic operating conditions [2]. Moreover, the operators that run the controlled process can utilize the provided information to make corrective actions [3]. However, with the increasing amount of the information in the power grid and the continuous popularization of mobile technology [4], the operation and monitoring of the power grid is developing towards informatization [5]. The existing PGAS is challenging to cope with the increasingly complex power grid in terms of real-time transmission and reliability in the future. Given the above problems, relevant scholars have carried out a series of studies.

In [6], the fuzzy matching method, single-event reasoning, and multievent reasoning methods are used for reasoning and judging the alarm information. In [7], abductive temporal reasoning algorithms are used for rapid identification and classification of the alarm information such as break alarms, exception alarms, and missing alarms, which have achieved good results. Based on the temporal constraint network, a new analytic model is developed for alarm processing with temporal information being taken into account in [8]. The function of the analysis module is to find out what events cause the reported alarms and to estimate when these events happen and identify abnormal or missing alarms. In [9], an online intelligent alarm-processing system is developed which could determine not only the fault or disturbance cause but also the missing or false alarms as well as the causes of the false alarms. In [10, 11], the specific alarm system is adopted to the wind turbine and the

UHV DC transmission. And in [12, 13], a rigorous anomaly detection scheme and a method to design the alarm deadband width are proposed. However, the systems and methods proposed in the above references are all running on local servers, subject to geographical factors and hardware and software architectures, so these systems and methods are difficult to adapt to the future development needs of the smart grid. Besides, most of the wireless communication applications of the power grid are based on the Short Messaging Service (SMS [14]) transmission protocol. For instance, the authors in [15] have built a system to acquire the remote electrical signals from distribution transformers such as voltage, current, power, and temperature and send these values to a monitoring node via SMS. The system provides a solid basis for load forecasting and fault repairing, but there are inevitable intermittent delays. In [16], the problem that the simultaneous charging of a large number of plug-in electric vehicles [17] will cause the grid to be overloaded at certain times of the day is given. The SMS is used to realize the intelligent control of the power grid when the plug-in electric vehicle is charged, which is economical and practical. However, the short message delivery is performed on a best-effort basis, and no quality of service (QoS [18, 19]) agreement is given. When the network is overloaded or blocked, the network cannot be operated efficiently. In other words, it cannot ensure how long it takes for the message to reach the recipient, and it cannot ensure whether the message has been successfully delivered [20]. In summary, the traditional PGAS running on local servers has limitations. The SMSAS using SMS has a short life cycle. The mobile application of the PGAS urgently needs a new solution, and the WMP emerges at a historic moment. The WMP belongs to the WeChat ecosystem. WeChat is the most significant social software in China, similar to Facebook in the United States. As of the fourth quarter of 2018, WeChat covered more than 94% of smartphones in China, with 1,098.8 million monthly active users, including more than 200 countries and more than 20 languages [21]. WeChat has a significant influence in China.

In recent years, in the field of the power system, the application research of cloud computing technology is also underway. Integrating the smart grid into cloud computing has a bright prospect for future applications [22]. The authors of [23–25] proposed three corresponding solutions based on cloud computing technology to solve the severe challenge of the smart grid in big data processing and achieved excellent results. Yang et al. [26] proposed a virtual private cloud-based power dispatching automation system (VPC-PDAS) and put it into operation in the actual power system. The results show that the system is safe, reliable, and economical. Ma et al. [27] mentioned that ISO New England (ISO-NE) initiated a pilot project to explore the feasibility and implementation of cloud computing for the power system simulation. Research indicates that cloud computing can meet various computing needs in power system planning in a highly reliable, flexible, and convenient way without compromising cybersecurity and data privacy.

Accordingly, this paper presents a WeChat-based system of real-time monitoring and alarming for the power grid operation status under the virtual private cloud environment based on real-time power data and combining mobile technology with cloud computing technology.

The contributions are threefold:

(1) This paper proposes a new architecture of the PGAS based on WeChat and cloud computing technology, which could remedy those drawbacks of the existing PGAS based on SMS: high latency in data transmission, low reliability, and poor economy.

(2) The latency in data transmission and reliability of the proposed system and SMSAS are calculated and analyzed in detail. The results show that the annual failure time of the proposed system is 15.24 minutes, which is approximately 380 times lower than 96.51 hours under the SMSAS. And the latency in data transmission of the proposed system is 172 milliseconds, which is 28 times lower than 4.9 seconds under the SMSAS.

(3) To our knowledge, this is the first paper to apply WeChat which is the state-of-the-art social media platform to the power system. This paper provides a practical and effective solution for the mobile application of the complex system. And the proposed system has been applied to the actual industry and has a significant operation effect.

The rest of this paper is organized as follows: Section 2 describes the advantages of the WMP. In Section 3, the new architecture of the power grid alarm system based on WeChat and cloud computing technology is proposed, including architecture design and architecture contents. Section 4 calculates and analyzes the performance of the existing and the proposed system. Section 5 describes the implementation and advantages of the proposed system in detail and applies it in an actual power system. Finally, Section 6 concludes this paper.

2. Advantages of WeChat Mini Programs

At present, app types can be divided into web app, hybrid app, and native app. The native app has full functions and the best user experience [28]. Different from the native app, the WMP is a new lightweight application development mode, which uses JavaScript to implement logical functions and WXML and WXSS to jointly perform presentation layer functions. The WMP can be used without installation by using the components defined by itself. And the memory of the WMP is tiny. Each WMP does not exceed 1 MB, but it has a user experience that rivals or even surpasses that of the native app. Table 1 gives a comparison of the WMP and native app.

Therefore, the advantages of the WMP can be summarized as follows:

(1) Cost-effective development and maintenance: the WMP has a short development cycle, less development workforce investment, no need to download and install, and a shorter marketing path. The cost of

Table 1: WMP vs. native app.

Properties	WMP	Native app
Programming language	JS/WXSS/WXML	Objective-C/java
Performance	High	High
Cost	Low	High
Productivity	Higher	High
Cross-platform	Enable	Unable
Eclipse RCP	Easy	Hard
Memory usage	Low	High
Development environment	Simple	Complex

the WMP is lower than that of the native app. On the contrary, the version updates do not need to be downloaded and installed again. After developers submit the new version to the WeChat public platform for approval, version cloud push can be realized. Users can complete version updates by reloading the WMP.

(2) Cross-platform: the native app needs to develop multiple versions to adapt to different operating systems. In contrast, the WMP can adapt to various operating systems by developing only one version on the WeChat platform because the WMP can compile the corresponding runnable components of the relevant platform by using the components defined by itself.

(3) Occupying less memory: the WMP requires no installation and shares the memory with WeChat. The memory space occupied is neglected, which significantly compresses memory, liberates the mobile phone space, and improves the mobile phone performance.

(4) Protecting user privacy: the native app involves many behaviors that spy on user privacy, such as getting user SMS records, call logs, and address book lists. In contrast, the WMP does not have the behavior of spying on user privacy, which ensures the security of personal information, because the WMP runs on the WeChat platform and is restricted and regulated by WeChat.

In conclusion, the WMP is superior to the native app and has incomparable advantages over other app types in terms of performance and security. In this paper, using the WMP as the client-side can solve a series of problems faced by the traditional alarm system to realize mobile applications.

3. The Contents of WMAS

In terms of the problems of traditional alarm systems, the WeChat-based system of real-time monitoring and alarming for the power grid operation status is proposed in this paper and applied to an actual power system. The framework of the proposed system is shown in Figure 1.

As shown in Figure 1, the proposed system architecture is divided into three parts: dispatching VPC, alarm WMP, and Internet communication mechanism.

3.1. Dispatching VPC. VPC is a secure, flexible, and high-performance cloud-based proprietary network. Users can quickly build an isolated private network environment on the cloud through the VPC to meet the requirements of high security. And the VPC has three remarkable characteristics:

(i) Network virtualization: the VPC can construct the virtual network on the basis of the physical network based on OverLay Technology.

(ii) Complete isolation between VPCs: the VXLAN protocol is used to isolate each VPC network. And the two-tier logic isolation between VPCs can be guaranteed, and communication cannot be carried out directly.

(iii) Customizable network environment: the VPC can customize the IP address range, network segment, routing table, and gateway to plan and manage the network on demand.

Given the advantages of the VPC, the dispatching VPC is deployed with the app server of WMAS and the VPC-based power dispatching automation system (VPC-PDAS) proposed in reference [26]. WMAS inherits the security of VPC-PDAS and can meet the security protection requirements of the power grid. The alarm data of WMAS come from VPC-PDAS. The VPC-PDAS and alarm WMP client are connected through the dedicated data interface web API in WMAS to process and forward the relevant alarm data. Figure 2 shows the data interaction between web API, VPC-PDAS, and alarm WMP client.

As shown in Figure 2, in the web API, the main body is the Http controller, and the controller performs real-time data interaction with the VPC-PDAS and filters and classifies the alarm information acquired from the VPC-PDAS. When the alarm WMP client initiates a data request to the controller in the Get method of the Http request method, the controller returns to the JSON [29] type of alarm data.

3.2. Alarm WMP Client. To design the alarm WMP client, MINA is adopted as the technical architecture of the WMP, and the functions of the WMP are implemented by modules and layers.

3.2.1. The Technical Architecture of the Alarm WMP. MINA inherits from MVVM [30] (model-view-viewmodel) and has the advantages of low coupling, reusability, independent development, and page testability. As shown in Figure 3, MINA is divided into three parts: view layer, app service layer, and native layer.

(i) View layer: WXML and WXSS are the development languages of the view layer. The former builds the basic view structure of the page, and the latter controls the presentation style of the page. All the function pages presented to the users in WMP can be implemented at this layer, such as the

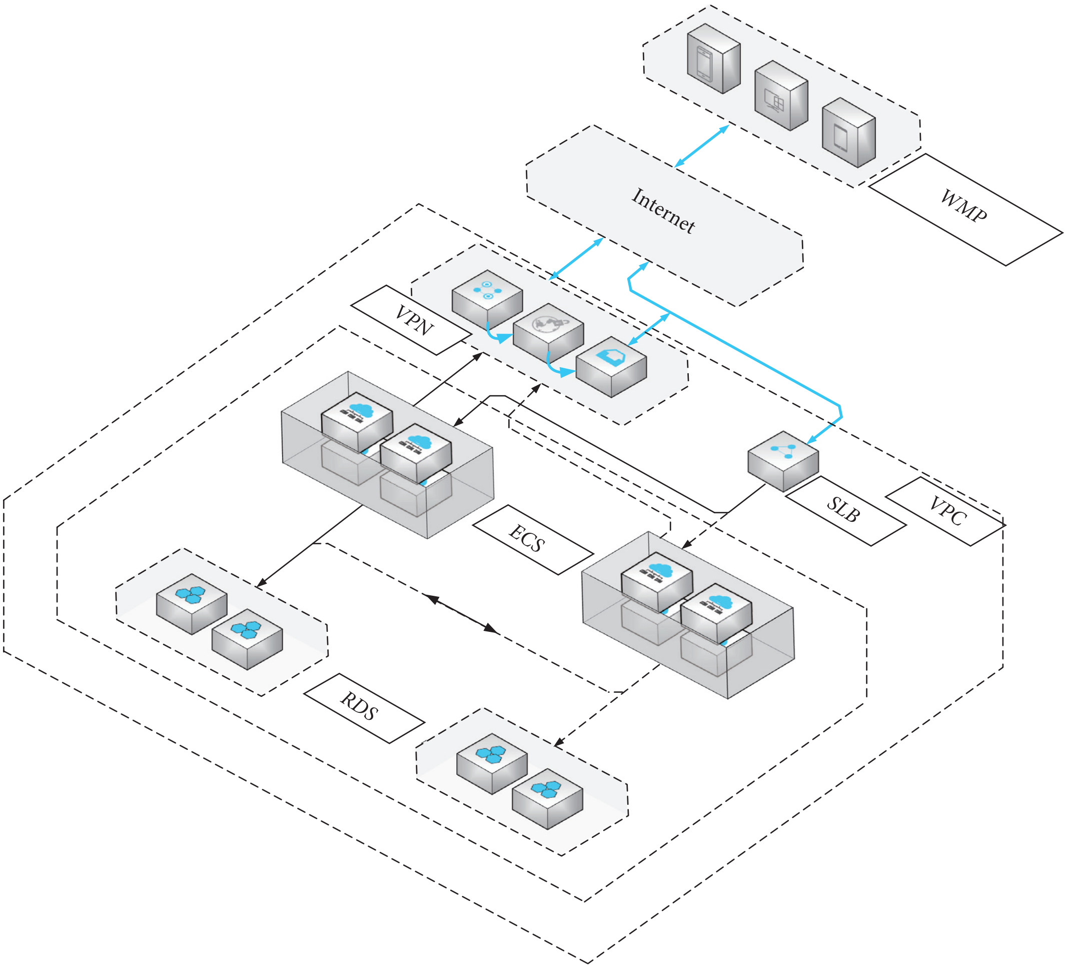


Figure 1: Framework of WMAS.

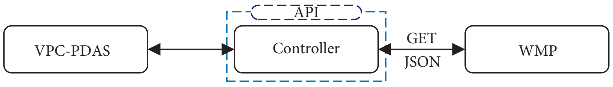


Figure 2: Relationship between API, VPC-PDAS, and WMP.

user login page and alarm information display page.

(ii) App service layer: this is the service center of MINA. Using JavaScript, the page rendering, page interaction, and related data processing are realized by loading and running the asynchronous thread based on WeChat separately.

(iii) Native layer: this contains WeChat capability, file storage, network request, etc. and provides basic functional components for data management, network communication, application life cycle management, and page routing. JSBridge of the native layer is responsible for the connection between the view layer and the app service layer. The app service layer notifies the view layer of the data changes and triggers its page update; the view layer notifies the trigger of the event to the app service layer for business processing.

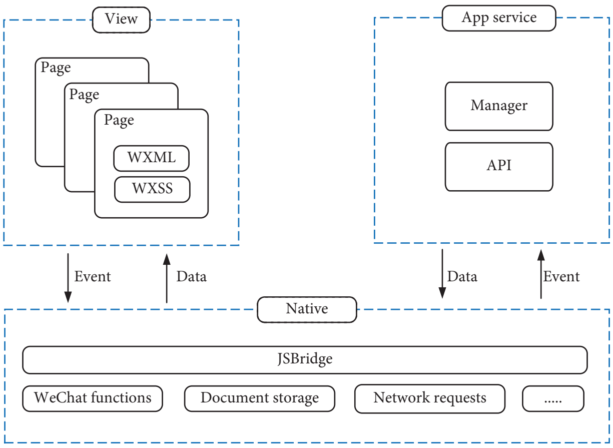


Figure 3: Technical architecture of the WMP.

3.2.2. Functional Modularity of the Alarm WMP. The alarm WMP is divided into four modules based on the MINA architecture, including WMP UI, network request module, business module, and data processing module. Furthermore, the alarm WMP also has global exception handling and permission control. Functional modularity of the alarm WMP is shown in Figure 4.

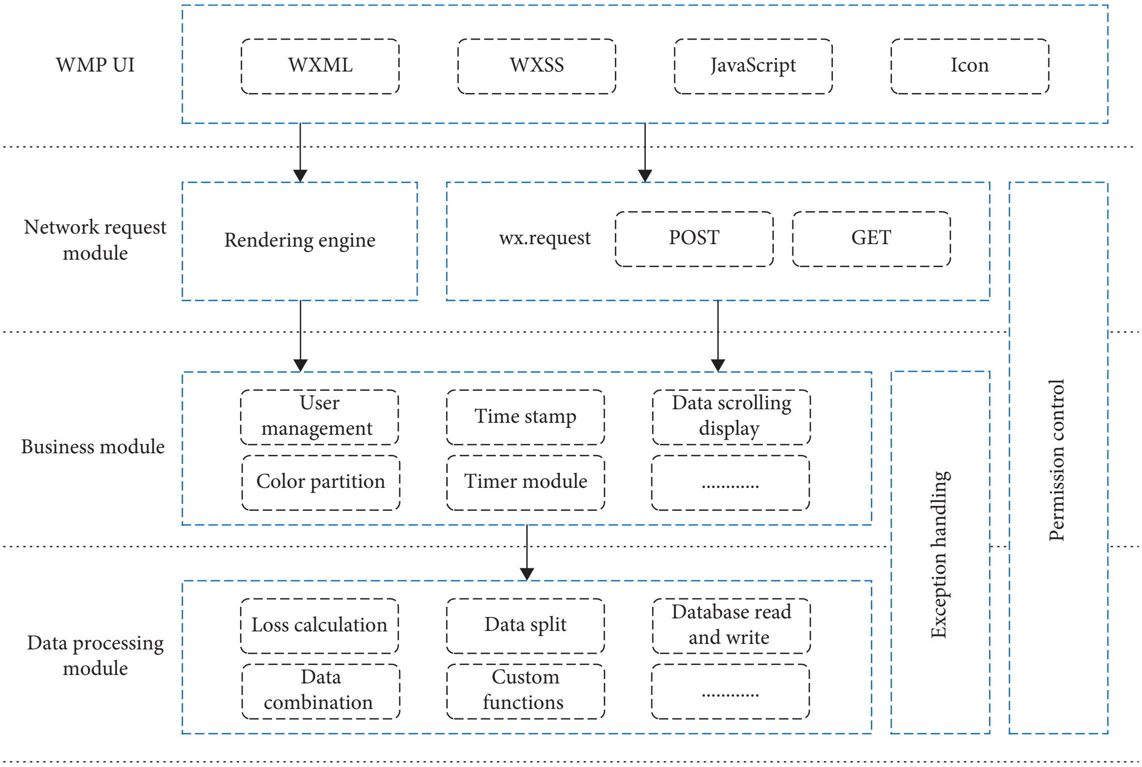


Figure 4: Module functions of the WMP.

(i) WMP UI: WXML, WXSS, and JavaScript are used and icons are combined appropriately to achieve the basic structure of the page.

(ii) Network request module: the web API and various interfaces of the WMP are used to initiate data requests by using the wx.request component of WeChat.

(iii) Business module: this is responsible for the display and management of the page of the alarm WMP, including user management, information time identification, timer, information cycle scroll display, information color display, and other business functions.

(iv) Data processing module: this is responsible for all basic data processing of the alarm WMP, such as power loss calculation, information disassembly and combination, local data reading and writing, and custom functions.

(v) Exception handling: this provides exception handling for the business module and data module, controls and processes illegal inputs in the program to prevent the occurrence of unknown errors, and makes the operation of the alarm WMP more stable.

(vi) Permission control: this provides more fine-grained permission control for the network request module, business module, and data processing module. Users only allow access to authorized resources, ensuring the security of the information.

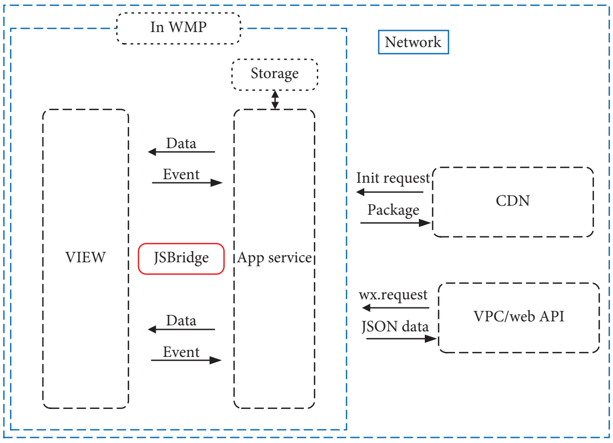


Figure 5: Communication mechanism of WMAS.

3.2.3. The Communication Mechanism of WMAS. The communication mechanism of WMAS is shown in Figure 5.

As shown in Figure 5, outside the alarm WMP, the communication of WMAS is divided into two parts:

(1) When the alarm WMP starts for the first time, an initialization request needs to be initiated to the CDN [31] (content delivery network), and the CDN will return the corresponding program packet to complete the download of resources.

(2) The alarm WMP communicates with the dispatching VPC through the SSLVPN [32] channel. In the SSLVPN, the alarm WMP initiates a network data request to the dispatching VPC through the

wx.request component, and the web API returns the JSON data packet after capturing the network request.

Inside the alarm WMP, JSBridge is used to communicate from the app service layer to the view layer in the way of one-way data binding, and from the view layer to the app service layer in the form of event binding.

4. Performance Comparison between WMAS and SMSAS

4.1. Latency Comparison

4.1.1. Minimum Theoretical Value of SMS Transmission Latency. SMS is transmitted through the dedicated control channel (DCCH), which is a point-to-point bidirectional control channel, including the stand-alone dedicated control channel (SDCCH), the fast associated control channel (FACCH), and the slow associated control channel (SACCH). SMS is delivered in the SDCCH or SACCH; the SACCH is used when the channel is busy, and the SDCCH is used when the channel is idle. The idle mode of the mobile phone of users is for the majority of the usage time of the day, and the transmission delay of the data in the idle mode is lower than that in the busy mode. To make the comparison more representative, the transmission delay in the idle mode is analyzed. SDCCH structures in the idle mode can be divided into two types, including SDCCH/8 and SDCCH/4 [33], as shown in Figure 6, where D is the SDCCH, A is the SACCH, B is the broadcast control channel (BCCH), C is the cell broadcast channel (CBCH), N is empty, ABCD is all four burst pulses, and one N means that a single burst pulse is empty.

The maximum byte capacity of a short message is 140 bytes. During the transmission, it is finally changed into 251 bytes after layers of encapsulation. An SDCCH frame contains two 51 duplicate frames, namely, 51 time-division multiple access (TDMA) frames, and one TDMA frame duration is 4.615 ms. An SDCCH can carry up to 23 bytes of upper information, so $251/23 = 11$ SDCCH frames are required for 251 bytes of data units from the upper layer.

As shown in Figure 6(a), the SDCCH is divided into eight subchannels, SDCCH0–SDCCH7, and the repetition period of the channel is 51 frames, so the shortest time to transmit 251 bytes on the SDCCH/8 structure is

$$11 \times 51 \times 4.615 = 2.6\,\text{s}. \tag{1}$$

As shown in Figure 6(b), the SDCCH is divided into four subchannels, SDCCH0–SDCCH4, and the repetition period of the channel is 102 frames, so the shortest time to transmit 251 bytes on the SDCCH/8 structure is

$$11 \times 102 \times 4.615 = 5.178\,\text{s}. \tag{2}$$

In summary, a 14-byte short message takes at least 2.6 s or 5.178 s to be delivered through the SDCCH, and the congestion rate of the SDCCH and the waiting time of short message queuing in the short message service center (SMSC) are ignored.

4.1.2. Actual Measured Transmission Latency. To make a comparison between the proposed system and the SMSAS fairer, this paper uses web SMS for testing. The data source of the web SMS is the same as that of WMAS, from the VPC-PDAS. The SMS receiving module and the WMP computer client are installed on the same local computer connected to the mobile phone WiFi for receiving the alarm information transmitted from the cloud computer and recording the time when the alarm message is sent and the time of being received. The measured latency is the difference between the above two times.

The test time is from 9:00 to 24:00, and an alarm message is generated and pushed every 9 minutes for a total of 100, and 10:00 to 14:00 and 20:00 to 23:00 are the peak time of the transmission network. The total time for each message transmitted to the mobile terminal is detected. The test is done continuously for 30 days. The specific time distribution is shown in Figures 7 and 8.

Figure 7 shows the time distribution of 100 tests in one day, and Figure 8 shows the time distribution of 3000 tests for 30 consecutive days. The ratio of the time distribution of the two is small, indicating that the test is reasonable and the test data are general. The detailed comparison between the actual test data of SMSAS and WMAS and the theoretical value of SMS transmission is shown in Figure 9.

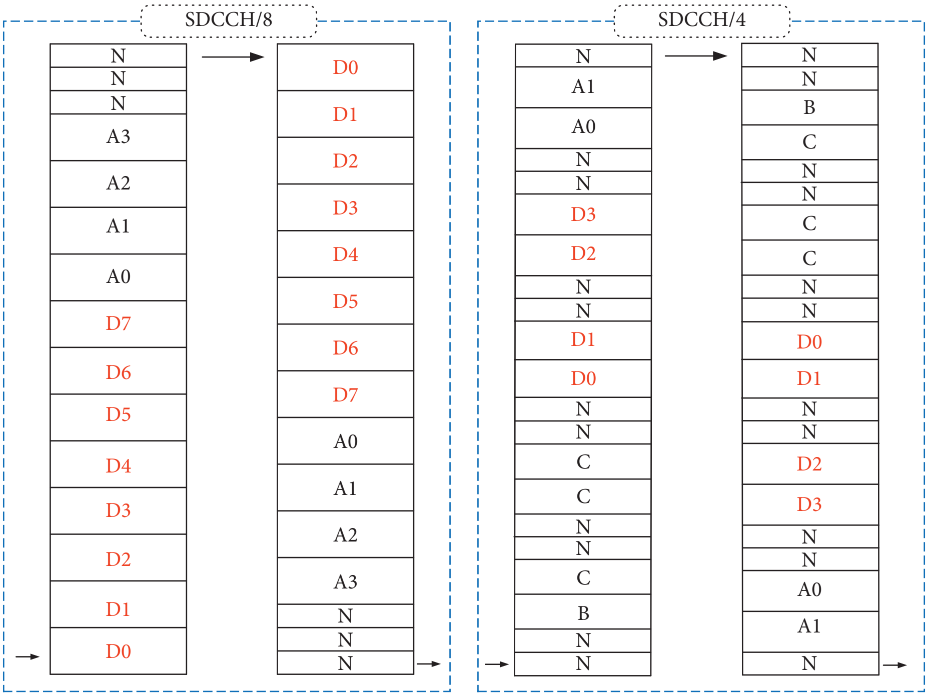
As shown in Figure 9, the actual test latency of WMAS is much smaller than the actual test latency and theoretical latency of SMSAS. The average latency of WMAS is 172 ms. Compared with the average latency of SMSAS of 4.9 s, the average latency is reduced by at least 28 times.

4.2. Reliability Comparison. When the SMSAS sends an alarm message, the alarm message needs to be sent to the SMSC for queuing and finally sent to the specified user via the network. And WMAS is sent directly to the user who initiated the network request through the network without any intermediate process. For convenience, the simplified network structure of SMSAS and WMAS is shown in Figure 10.

This paper uses the full-state enumeration method to analyze the reliability of the network structure. Take SMSAS as an example. The network structure of SMSAS has five actual nodes and one virtual node. The relationship between these nodes can be expressed by the following relation matrix:

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \tag{3}$$

where "0" represents no channel between the two nodes and "1" means that communication between the two nodes is possible.



(a)

(b)

Figure 6: Structure of the SDCCH.

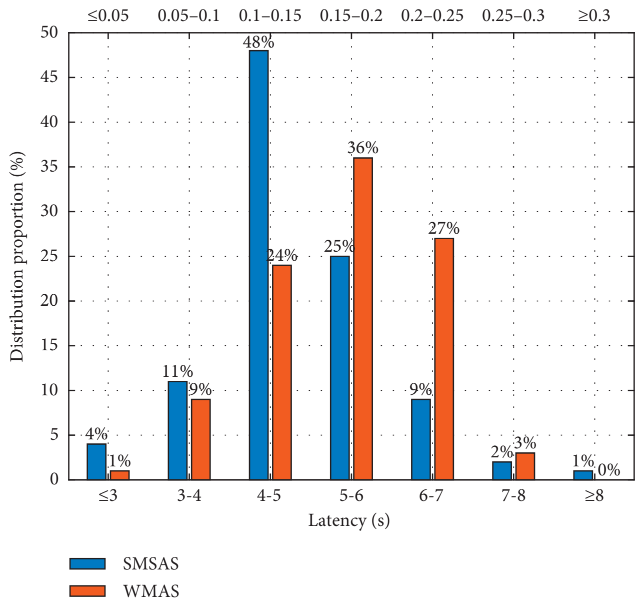


Figure 7: Test data of one day.

When information is transmitted from the SMSAS to the mobile terminal (from node 1 to node 6), there are three cases of information transmission failures: node 1 forming an information island, node 6 forming an information island, and nodes 1 and 6 forming an information island, and the relationship matrix corresponds to the following equations, respectively:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ast & \ast & \ast & 0 \\ 0 & \ast & 0 & \ast & 0 & \ast \\ 0 & \ast & 1 & 0 & \ast & \ast \\ 0 & \ast & 0 & \ast & 0 & \ast \\ 0 & 0 & \ast & \ast & \ast & 0 \end{bmatrix}, \quad (4)$$

$$\begin{bmatrix} 0 & \ast & 0 & 0 & 0 & 0 \\ \ast & 0 & \ast & \ast & \ast & 0 \\ 0 & \ast & 0 & \ast & 0 & 0 \\ 0 & \ast & \ast & 0 & \ast & 0 \\ 0 & \ast & 0 & \ast & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad (5)$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ast & \ast & \ast & 0 \\ 0 & \ast & 0 & \ast & 0 & 0 \\ 0 & \ast & \ast & 0 & \ast & 0 \\ 0 & \ast & 0 & \ast & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad (6)$$

where $\ast$ can be "0" or "1." Assuming that there are n kinds of information islands among nodes, the corresponding probability is P_i $(i \in n)$. Suppose that the reliability of a single channel and a node is α and β, respectively.

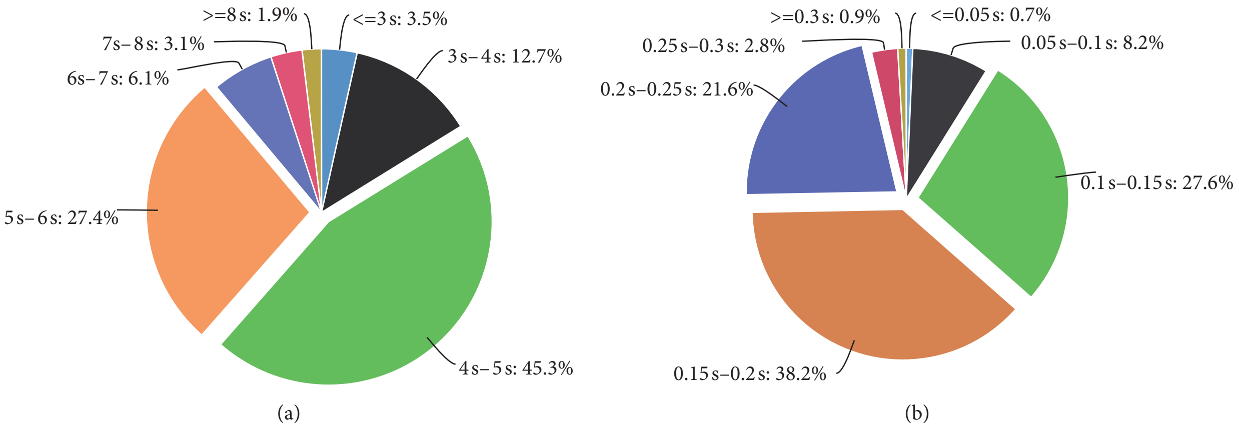


Figure 8: Test data of 30 days. (a) SMSAS. (b) WMAS.

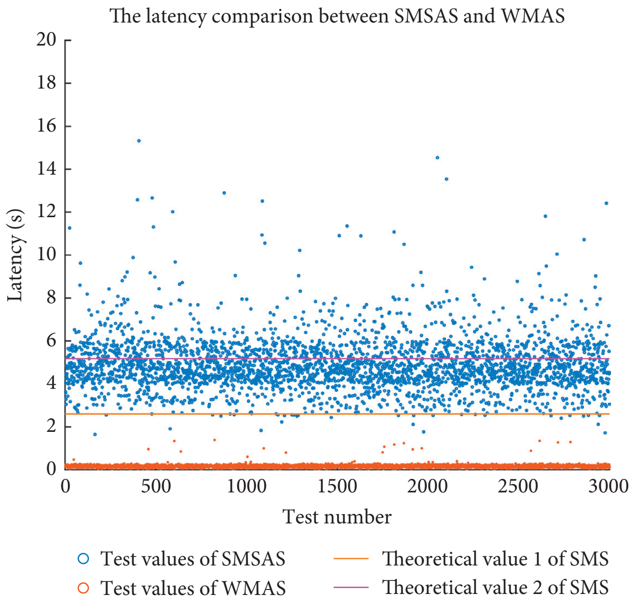


Figure 9: Detailed comparison between the actual test data of SMSAS and WMAS and the theoretical value of SMS transmission.

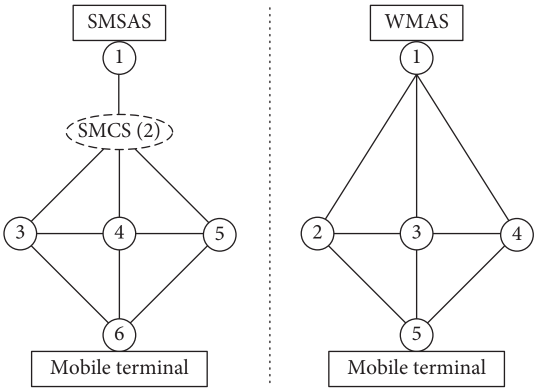


Figure 10: Simplified network structure of SMSAS and WMAS.

The reliability of the network structure of SMSAS and WMAS can be expressed as

$$P=\left(1-\sum_{i=1}^{n}P_i\right)\beta. \tag{7}$$

For the SMSAS network structure, with $n=3$, according to the matrices (4)–(6), P_1, P_2, and P_3 are estimated as

$$P_1=(1-\alpha)\sum_{i=0}^{7}C_8^i\alpha^{8-i}(1-\alpha)^i, \tag{8}$$

$$P_2=(1-\alpha)^3\sum_{i=0}^{5}C_6^i\alpha^{6-i}(1-\alpha)^i, \tag{9}$$

$$P_3=(1-\alpha)^4\sum_{i=0}^{5}C_5^i\alpha^{5-i}(1-\alpha)^i. \tag{10}$$

Similarly, for the WMAS network structure, with $n=3$, P_1, P_2, and P_3 are estimated as

$$P_1=P_2=(1-\alpha)^3\sum_{i=0}^{4}C_5^i\alpha^{5-i}(1-\alpha)^i, \tag{11}$$

$$P_3=(1-\alpha)^6\sum_{i=0}^{2}C_2^i\alpha^{2-i}(1-\alpha)^i. \tag{12}$$

4.2.1. The Calculation of α. All undirected links in the network can be converted into two parallel and reverse-directed links, and the two links can also be considered independent variables, as shown in Figure 11.

As shown in Figure 11, the reliability of a channel can be obtained by separately calculating the reliability of the uplink and downlink of the channel. To calculate the reliability of the uplink and downlink, this paper adopts the path loss model developed by the IEEE802.16 working

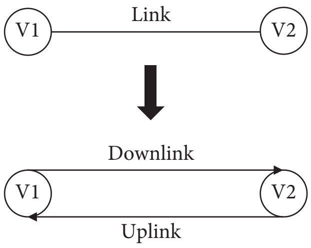


Figure 11: Link conversion.

group [34]. The IEEE802.16 working group divides the path loss model into three categories: A, B, and C, according to differences in the geographical environment. The specific model is as follows:

$$PL_{802.16}(d) = \begin{cases} 20\log_{10}\left(\frac{4\pi d}{v}\right), & d \le d_0, \\ 20\log_{10}\left(\frac{4\pi d}{v}\right) + 10\gamma\log_{10}\left(\frac{d}{d_0}\right) + C_f + C_{RX}, & d > d_0, \end{cases} \tag{13}$$

where d is the actual distance between two nodes; $d_0 = 100\,\text{m}$; v is the wavelength in meters; and γ, C_f, and C_{RX} are characterized as follows.

The path loss exponent γ is a Gaussian random variable over the population of macrocells within each terrain category. It can be written as

$$\gamma = a - bh_{Tx} + \frac{c}{h_{Tx}}, \quad 10\text{m} \le h_{Tx} \le 80\text{m}, \tag{14}$$

where h_{Tx} is the base station antenna height in meters. The values of a, b, and c are shown in Table 2.

C_f is the data associated with the subcarrier frequency f_c. And the value of C_f is

$$C_f = 6\log_{10}\left(\frac{f_c}{2000}\right). \tag{15}$$

C_{RX} is the data associated with the receiving antenna. And the value of C_{RX} is

$$C_{RX} = \begin{cases} -10.8\log_{10}\left(\frac{h_{RX}}{2}\right), & \text{for types } A \text{ and } B, \\ -20\log_{10}\left(\frac{h_{RX}}{2}\right), & \text{for type } C, \end{cases} \tag{16}$$

or

$$C_{RX} = \begin{cases} -10\log_{10}\left(\frac{h_{RX}}{3}\right), & \text{for } h_{RX} \le 3\text{m}, \\ -20\log_{10}\left(\frac{h_{RX}}{3}\right), & \text{for } h_{RX} \ge 3\text{m}, \end{cases} \tag{17}$$

where h_{RX} is the receiving antenna height in meters. The simulation curve of the IEEE802.16 path loss model is shown in Figure 12.

Besides the path loss model, the temporal characteristics of the channel are also subject to the Rice distribution. The probability density function of the Rice distribution is

$$f(r) = \frac{r}{\sigma^2}\exp\left(-\frac{r^2 + r_d^2}{2\sigma^2}\right)I_0\left(\frac{rr_d}{\sigma^2}\right), \tag{18}$$

where r_d is the peak amplitude of the signal, σ is the multipath amplitude, and I_0 is the zero-order Bessel function. And the cumulative distribution function of the Rice distribution is defined as follows:

$$P_{\text{out1}} = 1 - Q\left(\sqrt{2K_0}, \sqrt{\frac{2(1+K_0)}{PL_{802.16}(d)}}\right), \tag{19}$$

where $Q(\cdot)$ is the Marcum Q function and K_0 is the signal factor, which can be calculated by [35]

$$\begin{aligned} K = {} & 10\log_{10}(F_s) + 10\log_{10}(F_h) + 10\log_{10}(F_b) \\ & + \log_{10}(k_0 D^{\gamma}) + 8, \end{aligned} \tag{20}$$

where $k_0 = 10$; $\gamma = -0.5$; when $D = d$, $K = K_0$; F_s is the seasonal factor; F_h is the height factor; and F_b is the beamwidth factor, and the factors are defined as follows:

$$F_s = \begin{cases} 1.0, & \text{summer (leaves)}, \\ 2.5, & \text{winter (no leaves)}, \end{cases} \tag{21}$$

$$F_h = \left(\frac{h}{3}\right)^{0.46} \quad (h \text{ in meters}), \tag{22}$$

Table 2: Values of a, b, and c.

Model parameter	Terrain category		
	A	B	C
a	4.6	4.0	3.6
b	0.0075	0.0065	0.0050
c	12.6	17.1	20.0

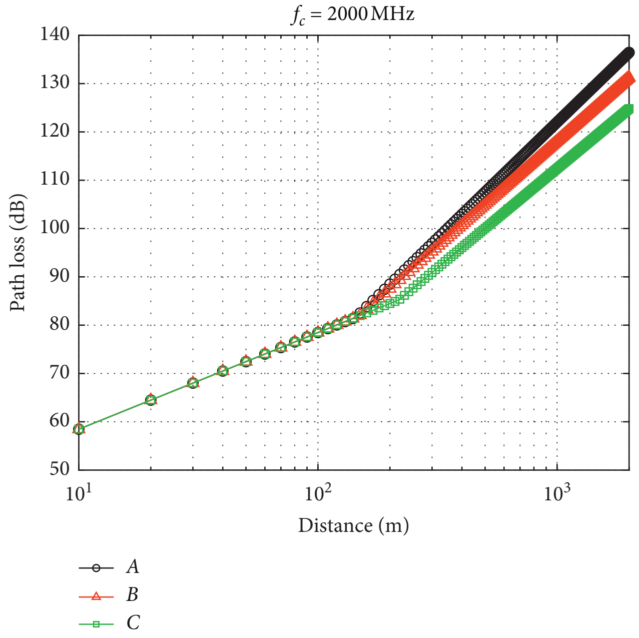


Figure 12: Test results of the IEEE802.16 path loss model.

$$F_b = \left(\frac{b}{17}\right)^{-0.62} \quad (b \text{ in degrees}). \tag{23}$$

The loss rate of path dilution is calculated by the moment generating function of Rice distribution:

$$P_{\text{out2}} = \mathrm{Q}\left(\sqrt{\frac{2K_i\varphi}{b+\psi}}, \sqrt{\frac{2K_0 b}{b+\psi}}\right) - \frac{b}{b+\psi}\exp\left(-\frac{K_i\psi + K_0 b}{b+\psi}\right) \cdot I_0\left(\frac{\sqrt{4K_iK_0\psi b}}{b+\psi}\right), \tag{24}$$

where K_i is the interference factor, $b = \text{SINR}(K_i+1)/(K_0+1)$ (signal-to-interference-plus-noise ratio, SINR), and ψ is the protection rate of the SINR.

The failure rate of the uplink and downlink can be obtained by their respective P_{out1} and P_{out2} from the following equation:

$$P^{\text{up}} \text{or } P_{\text{down}} = P_{\text{out1}} + P_{\text{out2}} - P_{\text{out1}}P_{\text{out2}}. \tag{25}$$

The link failure rate between the two nodes is

$$P_{\text{link}} = 1 - \left(1 - P^{\text{up}}\right)\left(1 - P_{\text{down}}\right). \tag{26}$$

In summary,

$$\alpha = 1 - P_{\text{link}}. \tag{27}$$

Assume that the distance between node 1 and node 2 of the WMAS network architecture is 500 m. The interference source of node 1 is 1200 m away from node 1, and the interference source of node 2 is 1000 m away from node 2. According to equations (13)–(27), $\alpha = 99.9479\%$.

4.2.2. The Calculation of β. The calculation of β can be equivalent to the calculation of the reliability of the master station system of SMSAS and WMAS. And the reliability of the master station system of SMSAS and WMAS can be analyzed by the full-probability formula.

The existing SMSAS consists of a front-end machine, SCADA server, and GSM modem. The front-end machine and the SCADA server belong to the master station system of the traditional PDAS, and each consists of two parallel machines to achieve redundancy to ensure system reliability. The role of the GSM modem is to queue alarm messages and send them to the designated users in sequence via SMS. The reliability block diagram of SMSAS is shown in Figure 13.

The proposed WMAS is composed of elastic compute service (ECS), relational database service (RDS), and web API in series. ECS and RDS have the computer cluster mechanism, which can be expanded flexibly according to the system demand. Under the premise of a parallel connection of m servers, they can withstand the abnormal situation of $m-1$ servers. The combination of the two constitutes the master station system of VPC-PDAS. The web API runs on ECS. It can automatically extend the instance along with the ECS and interact with RDS through ECS. Therefore, the web API and VPC-PDAS master station system can be equivalent to a series relationship. The reliability block diagram of WMAS is shown in Figure 14.

The reliability of the master station system can be represented by the availability R of the system [36, 37]:

$$R = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{\mu}{\lambda + \mu}, \tag{28}$$

where MTBF is the mean time between failures, MTTR is the mean time to repair, λ is the failure rate, and μ is the repair rate. λ and μ can be estimated by (8760 hours a year)

$$\lambda = \frac{8760}{\text{MTBF}}, \tag{29}$$

$$\mu = \frac{8760}{\text{MTTR}}. \tag{30}$$

For the system with two different parts in series, the failure rate and repair rate can be expressed as

$$\lambda_s = \lambda_1 + \lambda_2, \tag{31}$$

$$\mu_s = \frac{\lambda_s\mu_1\mu_2}{\lambda_1\lambda_2 + \lambda_1\mu_1 + \lambda_2\mu_2}. \tag{32}$$

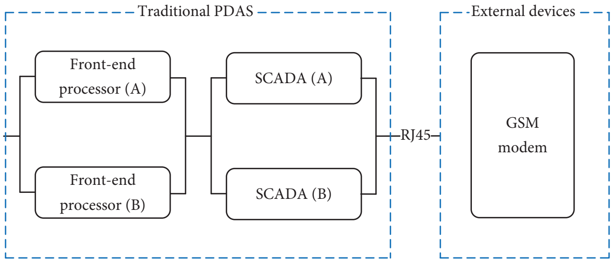


Figure 13: Reliability block diagram of SMSAS.

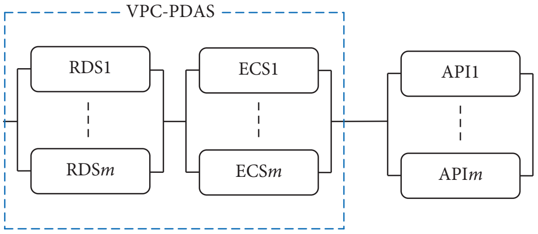


Figure 14: Reliability block diagram of WMAS.

For the system with n $(n > 2)$ parts in series, after equivalent transformation, the failure rate and repair rate can be estimated as

$$\lambda_s = \sum_i^n \lambda_i, \tag{33}$$

$$\mu_s = \frac{\lambda_s}{\sum_i^n \lambda_i/\mu_i}. \tag{34}$$

For the system with n parallel connections of the same components, the failure rate and repair rate can be estimated as

$$\lambda_s = n\lambda^n \left(\frac{\text{MTTR}}{8760}\right)^{n-1}, \tag{35}$$

$$\mu_s = \sum_i^n \mu_i. \tag{36}$$

According to the Performance Testing Service (PTS) [38] and Application Real-Time Monitoring Service (ARMS) [39] tests provided by Alibaba Cloud Computing Co., Ltd. (https://www.alibabacloud.com), the related reliability parameters of the front-end machine, SCADA server, RDS, ECS, web API, and GSM modem are shown in Table 3.

According to Figures 13 and 14, Table 3, and equations (29)–(36) and letting $m = 2$, the failure rate and repair rate of WMAS and SMSAS can be calculated as follows:

$$\begin{cases} \lambda_{\text{WMP}} = 4.575 \times 10^{-4}, \\ \mu_{\text{WMP}} = 1767.04, \\ \lambda_{\text{SMS}} = 0.43824, \\ \mu_{\text{SMS}} = 875.9. \end{cases} \tag{37}$$

Table 3: Device parameters.

Item	MTBF (h)	MTTR (h)
Front-end machine	42000	12
SCADA server	42000	12
GSM modem	20000	10
RDS	120000	8
ECS	120000	8
Web API	20000	10

R of WMAS and SMSAS can be calculated by substituting the above results into equation (28):

$$\begin{cases} \beta_{\text{WMP}} = R_{\text{WMP}} = 99.999974\%, \\ \beta_{\text{SMS}} = R_{\text{SMS}} = 99.949992\%. \end{cases} \tag{38}$$

Finally, the reliability of SMSAS and WMAS can be obtained according to equations (7)–(12) and α, β_{SMS}, and β_{WMP}:

$$\begin{cases} P_{\text{WMAS}} = 99.9971\%, \\ P_{\text{SMSAS}} = 98.8983\%. \end{cases} \tag{39}$$

On the premise of 8760 hours a year, the annual failure time of WMAS and SMSAS is

$$\begin{cases} h_{\text{WMAS}} = (1 - 99.9971\%) \times 8760 \times 60 = 15.24\,\text{min}, \\ h_{\text{SMSAS}} = (1 - 98.8983\%) \times 8760 \times 60 = 96.51\text{h}. \end{cases} \tag{40}$$

The WMAS reliability is as high as 99.9971%, and the annual failure time is 15.24 minutes, which is about 380 times lower than 96.51 hours of SMSAS.

In summary, WMAS is superior to SMSAS, and the performance difference between the two is shown in Table 4.

5. Implementation and Running Effect of WMAS

The proposed system runs on Ali Cloud in China. The ECS configuration is Windows Server 2016 R2 standard, 4-core 16GB ROM, and the RDS configuration is Microsoft SQL Server 2008 R2, 4-core 8GB ROM, 100GB storage. The implementation of WMAS includes two parts: web API and alarm WMP. The specific implementation methods are as follows.

5.1. The Implementation of Web API. The implementation of the web API consists of the following steps:

Step 1: using Visual Studio 2017 ASP.NET based on C#, the Http controller is created to realize the function of alarm data processing.

Step 2: the SSL digital certificate issued by the international digital certificate authority (CA) is deployed on the dispatching VPC.

Step 3: using Internet Information Services (IIS) to publish the web API on the network, the data

Table 4: WMAS vs. SMSAS.

Properties	WMAS	SMSAS	Multiples
Latency	172 ms	4.9 s	28
Annual failure time	15.24 min	96.51 h	380

transmission method of the web API is implemented as the Https protocol.

Step 4: the Https-based web API URL is bound to the server domain name of the WeChat control background, and the SSLVPN remote secure access channel is established between the web API and the mobile device.

Step 5: the ECS running the web API is bound to the server load balancer (SLB), the traffic is distributed to multiple ECS instances, the external service capability of the application system is expanded, and the usability of the application system is improved.

5.2. The Implementation of Alarm WMP. With the WeChat web developer tool version 1.02, the implementation of the alarm WMP includes the following steps:

Step 1: apply for WeChat unique identification and recognition APPID on the official website of Tencent and bind this APPID to the WMP project.

Step 2: determine the technical architecture of the alarm WMP, as detailed in Section 3.

Step 3: modularize the functionality of the alarm WMP, as detailed in Section 3.

Step 4: combine WXML + WXSS + JavaScript, write the code, and realize the function of each module.

Step 5: after the program is compiled, scan the Quick Response Code preview with the mobile phone to make sure it can normally run on the mobile terminal.

Step 6: after the functional test is completed without any error, submit the alarm WMP to Tencent for review and release. After passing the review, the alarm WMP can be used for regular search.

5.3. The Operation Effect of WMAS. WMAS has two function pages: user login page and alarm page.

5.3.1. The User Login Page. To ensure the security of the power grid data, a user login function has been developed, as shown in Figure 15.

The user login page has the following characteristics:

After entering the username and password and clicking login, the page initiates a network request for query validation to the web API. In the process of data transmission, the input password is hidden and encrypted by the MD5 mode in the background, which ensures the security of the user password.

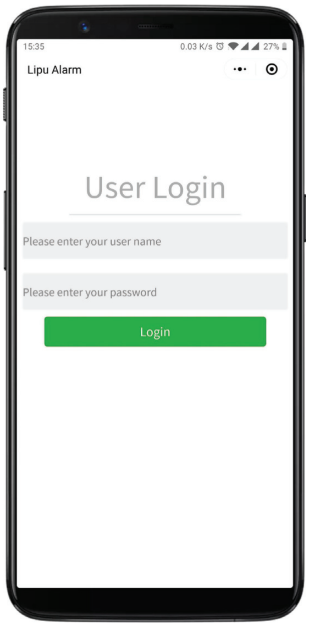


Figure 15: User login of the WMP.

If the data returned by the web API show that the username and password are both correct, the username and password are stored in the cookies of the mobile phone, which avoids the problem that the user needs to input personal user information many times and prompts the user to input correctly and jump to the next function page.

The specific effect of the above characteristics is shown in Figure 16.

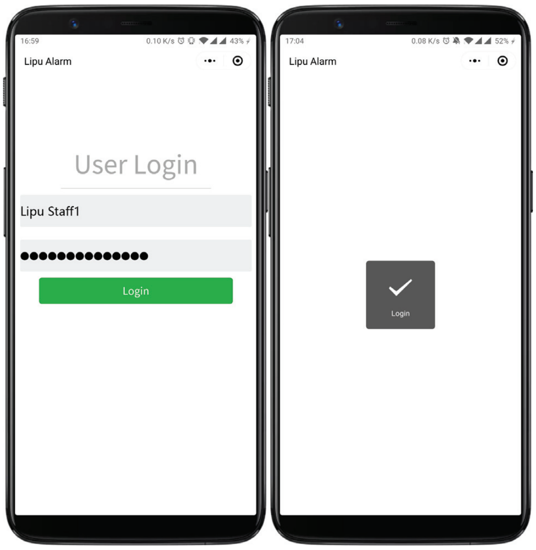
5.3.2. The Alarm Page. The alarm page is not allowed to be executed until the user login page has been verified successfully. In the beginning, the alarm page will initiate a query request for the latest alarm information to the web API through the SSLVPN. After receiving the request, the web API interacts with the RDS through ECS and returns the original alarm data to the alarm WMP. The alarm page will split and combine these original data and bind with the front end of the page. Finally, the alarm information will be displayed in realtime.

WMAS can achieve the cross-platform operation, as shown in Figures 17 and 18, respectively, which show the operation effects of WMAS running on the Apple IOS system and Google Android system.

As shown in Figures 17 and 18, the alarm information has the following characteristics:

The screened alarm information comes from the important breakers in the power grid. These breakers' faults will cause certain economic losses to the local power grid.

The alarm information is marked with an accurate time sequence, which is accurate to the second level. The dispatcher can know the specific time when the fault occurs and take corresponding measures in time.


16:59

Lipu Alarm

User Login

Lipu Staff1

●●●●●●●●●●●●●●

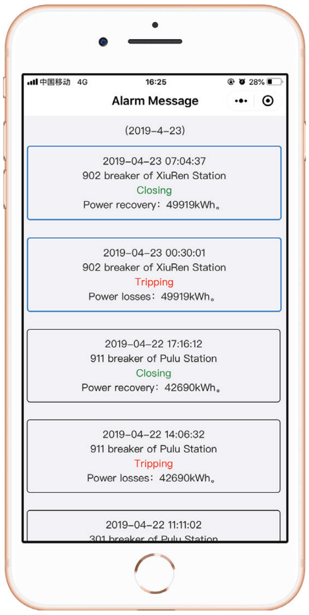
Login

17:04

Lipu Alarm

Login

Figure 16: Running effect of the login page.


中国移动 4G 16:25 28%

Alarm Message

(2019–4–23)

2019–04–23 07:04:37
902 breaker of XiuRen Station
Closing
Power recovery：49919kWh。

2019–04–23 00:30:01
902 breaker of XiuRen Station
Tripping
Power losses：49919kWh。

2019–04–22 17:16:12
911 breaker of Pulu Station
Closing
Power recovery：42690kWh。

2019–04–22 14:06:32
911 breaker of Pulu Station
Tripping
Power losses：42690kWh。

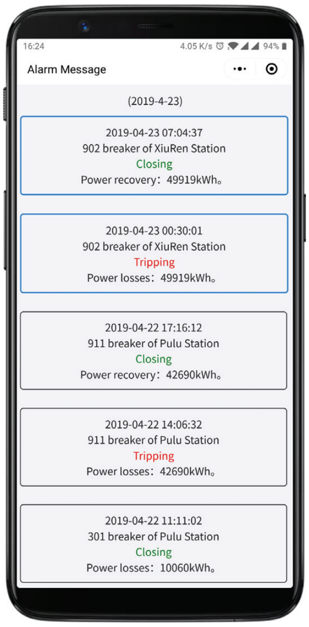
2019–04–22 11:11:02
301 breaker of Pulu Station

Figure 17: Alarm WMP running on IOS.

The alarm information distinguishes the state of the breakers by color. The tripping is red, and the closing is green. It avoids the dispatcher misreading the alarm information and brings unnecessary losses to the power grid.

The alarm information is divided in the time scale. The border color of the alarm information in the day is blue and the border color for the rest of the time is gray, which improves the work efficiency of the dispatcher.

The alarm information includes daily power recovery and daily power loss. Based on this, the dispatcher can not only know the economic loss and benefit brought by the breakers tripping and closing at a glance but also judge the influence degree of the breaker fault on the power grid and select the fault with the deepest influence degree to repair first.


16:24

Alarm Message

(2019-4-23)

2019-04-23 07:04:37
902 breaker of XiuRen Station
Closing
Power recovery：49919kWh。

2019-04-23 00:30:01
902 breaker of XiuRen Station
Tripping
Power losses：49919kWh。

2019-04-22 17:16:12
911 breaker of Pulu Station
Closing
Power recovery：42690kWh。

2019-04-22 14:06:32
911 breaker of Pulu Station
Tripping
Power losses：42690kWh。

2019-04-22 11:11:02
301 breaker of Pulu Station
Closing
Power losses：10060kWh。

Figure 18: Alarm WMP running on Android.

6. Conclusions

This paper presents a WeChat-based system of real-time monitoring and alarming for the power grid operation status under the virtual private cloud environment. First, a systematic model with components such as WMP, SSLVPN, and VPC is constructed. Then, the latency of the WMAS and SMSAS is tested by means of the stress test. Furthermore, the full-state enumeration method and the improved path loss model are used to calculate the reliability of the WMAS. And the results indicate that the proposed system is particularly excellent not only in terms of latency but also in terms of reliability. The proposed system meets the safety protection requirements of the power system in network security and data transmission reliability and has been implemented in the Lipu power system in Guangxi, China. More than one year of stable operation shows that the proposed system is safe, reliable, flexible, and convenient with a bright prospect for future applications.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Chu and A. Majumdar, “Opportunities and challenges for a sustainable energy future,” *Nature*, vol. 488, no. 7411, Article ID 294303, 2012.

[2] J. W. Stahlhut, G. T. Heydt, and J. B. Cardell, “Power system “economic alarms”,” *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 426–433, 2008.

[3] A. W. Al-Dabbagh and T. Chen, “Sounding off on industrial alarm systems,” *IEEE Potentials*, vol. 37, no. 2, pp. 24–28, 2018.

[4] L. Qi, W. Dou, W. Wang, G. Li, H. Yu, and S. Wan, “Dynamic mobile crowdsourcing selection for electricity load forecasting,” *IEEE Access*, vol. 6, pp. 46926–46937, 2018.

[5] T. Zhong-Zhong, L. Wen-Bin, S. Yang-Zi, and W. Ze-Yong, “Analysis and practice of mobile field operation information platform for power grid enterprises,” in *Proceedings of the 2018 China International Conference on Electricity Distribution (CICED)*, pp. 1833–1837, Tianjin, China, September 2018.

[6] X. Yang and S. Sun, “Construction of regional grid intelligent alarm system,” in *Proceedings of the 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pp. 144–147, Offenburg, Germany, October 2015.

[7] T. Kang, W. Wu, and B. Zhang, “Temporal abductive reasoning based intelligent alarm for power system,” in *Proceedings of the 2010 Asia-Pacific Power and Energy Engineering Conference*, pp. 1–5, Chengdu, China, March 2010.

[8] W. Guo, F. Wen, Z. Liao, L. Wei, and J. Xin, “An analytic model-based approach for power system Alarm processing employing temporal constraint network,” *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2435–2447, 2010.

[9] L. Wei, W. Guo, F. Wen, G. Ledwich, Z. Liao, and J. Xin, “An online intelligent alarm-processing system for digital substations,” *IEEE Transactions on Power Delivery*, vol. 26, no. 3, pp. 1615–1624, 2011.

[10] S. Gu, J. Wang, M. Wu, J. Guo, C. Zhao, and J. Li, “Study on lightning risk assessment and early warning for UHV DC transmission channel,” *High Voltage*, vol. 4, no. 2, pp. 144–150, 2019.

[11] K. Leahy, C. Gallagher, P. O’Donovan, and D. T. J. O’Sullivan, “Cluster analysis of wind turbine alarms for characterising and classifying stoppages,” *IET Renewable Power Generation*, vol. 12, no. 10, pp. 1146–1154, 2018.

[12] G. Anagnostou, F. Boem, S. Kuenzel, B. C. Pal, and T. Parisini, “Observer-based anomaly detection of synchronous generators for power systems monitoring,” *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 4228–4237, 2018.

[13] Z. Wang, X. Bai, J. Wang, and Z. Yang, “Indexing and designing deadbands for industrial alarm signals,” *IEEE Transactions on Industrial Electronics*, vol. 66, no. 10, pp. 8093–8103, 2019.

[14] W. Zhou, Z. Li, Y. Cheng, and H. Wang, “Synchronization algorithms for sms based wireless distributed system for electric grid monitor,” in *Proceedings of the 2009 International Conference on Communication Software and Networks*, pp. 696–700, Macau, China, February 2009.

[15] M. A. E. A. E. Hayati and S. F. Babiker, “Design and implementation of low-cost sms based monitoring system of distribution transformers,” in *Proceedings of the 2016 Conference of Basic Sciences and Engineering Studies (SGCAC)*, pp. 152–157, Khartoum, Sudan, February 2016.

[16] C. Hochgraf, R. Tripathi, and S. Herzberg, “Smart grid charger for electric vehicles using existing cellular networks and SMS text messages,” in *Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications*, pp. 167–172, Gaithersburg, MD, USA, October 2010.

[17] C. Wei, M. Benosman, and T. Kim, “Online parameter identification for state of power prediction of lithium-ion batteries in electric vehicles using extremum seeking,” *International Journal of Control, Automation and System*, vol. 17, no. 11, pp. 2906–2916, 2019.

[18] R.-T. Sheu and J.-L. C. Wu, “Performance analysis of rate control with scaling qos parameters for multimedia transmissions,” *IEE Proceedings—Communications*, vol. 150, no. 5, p. 361, 2003.

[19] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, “A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems,” *World Wide Web Journal*, 2019.

[20] R. Pries, T. Hobfeld, and P. Tran-Gia, “On the suitability of the short message service for emergency warning systems,” in *Proceedings of the 2006 IEEE 63rd Vehicular Technology Conference*, vol. 2, pp. 991–995, Melbourne, Australia, May 2006.

[21] Tencent’s fourth quarter 2018 results, https://www.tencent.com/zh-cn/articles/8003551553167294.pdf.

[22] Y. Xie, Y. Jiang, R. Liao et al., “User privacy protection for cloud computing based smart grid,” in *Proceedings of the 2015 IEEE/CIC International Conference on Communications in China—Workshops (CIC/ICCC)*, pp. 7–11, Shenzhen, China, November 2015.

[23] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 233–244, 2015.

[24] Y. Simmhan, S. Aman, A. Kumbhare et al., “Cloud-based software platform for big data analytics in smart grids,” *Computing in Science & Engineering*, vol. 15, no. 4, pp. 38–47, 2013.

[25] A. A. Munshi and Y. A. I. Mohamed, “Data lake lambda architecture for smart grids big data analytics,” *IEEE Access*, vol. 6, pp. 40463–40471, 2018.

[26] D. Yang, H. Wei, Y. Zhu, P. Li, and J.-C. Tan, “Virtual private cloud based power-dispatching automation system-architecture and application,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1756–1766, 2019.

[27] F. Ma, X. Luo, and E. Litvinov, “Cloud computing for power system simulations at ISO new england-experiences and challenges,” *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2596–2603, 2016.

[28] Y. Ma, X. Liu, Y. Liu, Y. Liu, and G. Huang, “A tale of two fashions: an empirical study on the performance of native apps and web apps on android,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 990–1003, 2018.

[29] M. Kleppmann and A. R. Beresford, “A conflict-free replicated json datatype,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 10, pp. 2733–2746, 2017.

[30] X. Li, D. Chang, H. Pen, X. Zhang, Y. Liu, and Y. Yao, “Application of MVVM design pattern in MES,” in *Proceedings of the 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 1374–1378, Shenyang, China, June 2015.

[31] G. Xie, Z. Li, M. A. Kaafar, and Q. Wu, “Access types effect on internet video services and its implications on CDN caching,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1183–1196, 2018.

[32] A. Alshalan, S. Pisharody, and D. Huang, “A survey of mobile VPN technologies,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016.

[33] N. Agarwal, L. Chandran Wadia, and V. Apte, “Capacity analysis of the GSM short message service,” in *Proceedings of the National Conference on Communications (NCC)*, Bangalore, India, January 2004.

[34] V. Erceg, L. J. Greenstein, S. Y. Tjandra et al., “An empirically based path loss model for wireless channels in suburban

environments," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 7, pp. 1205–1211, 1999.

[35] L. J. Greenstein, S. S. Ghassemzadeh, V. Erceg, and D. G. Michelson, "Ricean *K*-factors in narrow-band fixed wireless channels: theory, experiments, and statistical models," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4000–4012, 2009.

[36] W. G. Schneeweiss, "Computing failure frequency, MTBF & MTTR via mixed products of availabilities and unavailabilities," *IEEE Transactions on Reliability*, vol. 30, no. 4, pp. 362-363, 1981.

[37] P. A. Kullstam, "Availability, MTBF and MTTR for repairable M out of N system," *IEEE Transactions on Reliability*, vol. 30, no. 4, pp. 393-394, 1981.

[38] 3 Key Products that Powered Dongqiudi during the 2018 Fifa World Cup, https://www.alibabacloud.com/blog/594159?spm=a2c5t.10695662.1996646101.searchclickresult.376c2097tn65p9.

[39] Arms: Business Monitoring Capabilities with Real-Time Response—Alibaba Cloud, https://www.alibabacloud.com/product/arms?spm=a2c5t.10695662.1996646101.searchclickresult.31307311eLoFb8.