Security Situation Awareness and Interference Control Method for Power Wireless Private Networks Based on Dynamic Baseline

Jin Huang[1], Weiwei Miao[1], Junzhong Yang[2], Xinglong Wang[2], Linshan Shi[3], Zhengyuan Liu[4], and Peng Yu[4(✉)]

[1] State Grid Jiangsu Electric Power Co., Ltd., Information & Telecommunication Branch, Nanjing 210024, China
[2] State Grid Jiangsu Electric Power Co., Ltd., Taizhou Power Supply Branch, Taizhou 225307, Jiangsu, China
[3] State Grid Chongqing Electric Power Company, Chongqing 404100, China
[4] Beijing University of Posts and Telecommunications, Beijing 100876, China
yupeng@bupt.edu.cn

Abstract. The interference of the power wireless private network will directly affect the service quality of the power business, and then affect the stable operation of the power distribution network. Therefore, it is of great value to study the security situation awareness and interference control technology of electric power wireless private network. Existing research has seldom considered security situational awareness and control methods for power wireless private networks. Firstly, according to the signal-to-noise ratio data obtained by the network management system, combined with the upper and lower baselines and user proportion, the interference is identified. According to the interference scenario, the corresponding power adjustment scheme is proposed according to the different scale of users to ensure the stability of the system. In view of the influence of power adjustment, the dynamic change method of interference identification baseline is proposed, which provides reasonable interference control requirement standard for base station to adjust transmission power control interference, and improves the flexibility of service performance guarantee.

Keywords: Power wireless private network · Interference monitoring · Interference identification · Interference control

1 Introduction

With the widespread application of power wireless private network, convenient access methods are provided for control services such as power distribution automation, source-network load-storage interaction, and management services such as electricity information collection, mobile operations, video surveillance and so on [1]. The power wireless private network inherits the advantages of wireless network, such as flexible networking, convenient construction, and mature application. At the same time, the dedicating of

M. Cheng et al. (Eds.): SmartGIFT 2020, LNICST 373, pp. 77–92, 2021.
https://doi.org/10.1007/978-3-030-73562-3_7

frequency band, equipment, and network avoiding the limitations of the wireless public network in terms of bandwidth, delay, service interruption rate, safety and reliability. It can effectively supplement the wired transmission network and efficiently solve the "last mile" access problem of power communication, open up the "nerve endings" of the power communication network, and have the incomparable advantages of traditional wired communication and wireless public network communication [2].

However, with the rapid increase of the number of power wireless private network access terminals, in the scenario of unified access of various mixed services such as source network load storage, distribution monitoring, mobile applications, etc., the current centralized processing method through the core network can not meet the real-time requirements of load control power services. At the same time, power wireless private network also inherits the wireless system's channel opening, network sharing, terminal mobility and other characteristics, which also poses a huge challenge to the security of power services. Since power wireless private network carries a large number of electric power dedicated services, it is easy to cause service transmission interruption under the condition of wireless interference, which will affect the stable operation of the power system. Therefore, in view of the communication architecture of "terminal base station core network master station" of power wireless private network, this paper carries out security situation awareness on the electromagnetic space of power wireless private network and analyzes the potential interference risk, it is very important to monitor the flow and service quality of power wireless private network terminal and control the interference of wireless private networks for power systems [3, 4].

The existing research on interference of power wireless private network mainly includes two aspects: internal interference control and external interference control. For internal interference in the system, interference coordination and power control are often used to realize the control. For the external interference sources, the data analysis and other devices are used to locate the interference source. However, there are fewer studies on interference threshold control methods. When the interference is found, how to optimize the specific interference control parameters and minimize the influence of the network is also lack of limited analysis [5, 6] (Fig. 1).

Based on the above analysis, this paper proposes a dynamic baseline-based power wireless private network security situation awareness and interference control method. In this method, the interference monitoring and identification method is firstly proposed, and then the interference control method based on power adjustment is proposed. Finally, a dynamic adjustment method for the interference identification baseline is given. Based on this method, only through the scheduling of the base station side, the interference control of the network can be realized and the service quality of the service can be improved.

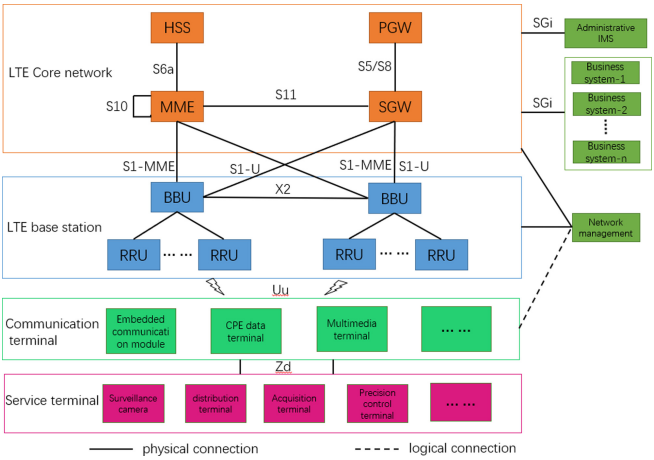

Fig. 1. LTE wireless private network architecture.

2 Research Background and Related Work

In the paper [3], after analyzing the influence of strong interference sources outside the power wireless private network, in view of the problem that the interference source in the power wireless private network cannot be confirmed, a fault tracking and positioning method for LTE power wireless private network external interference is proposed. The method first determines the range of the interfered base station, and then confirms the search range of the interference source; performs 3D scene modeling for the search range, then planning the Drive Test (DT) path for drive test, extracting the data characteristics of the Drive Test, analyzing and approaching interference area; finally, through forward ray tracing, the actual interference source location is evaluated and screened out.

The paper [5] draws lessons from the public network operation and maintenance standards to establish interference judgment indicators. It is considered that higher than −120 dBm means interference exists, higher than −110 dBm means that the interference begins to worsen various indicators, higher than −105 dBm means that the interference is more serious. The system external disturbances such as blocking interference, intermodulation interference, stray interference and LTE network interference are analyzed respectively. Finally, the confirmation methods and interference treatment methods for these interferences are given.

This paper [6] designs a progressive, step-by-step measurement and step-by-step approach interference location method based on the principle of radio direction finding and manual interference checking and positioning process. Firstly, the interference source search range is determined according to the disturbed cell, equipment terminal, frequency sweep/Drive Test point, and user complaint point in the network; then, the interference source search range is modeled in three-dimensional scene; then, the iterative search mechanism is used to plan the Drive Test path and implement the Drive Test, extract and analyze the characteristics of the Drive Test data, and use multiple heuristic rules to gradually compress and approach the interference source; finally, when the

interference source search area is compressed enough, the beam tracking wireless propagation model is used to quickly evaluate the candidate interference source location, and the interference source location results are given.

The paper [7] firstly analyzes the broadband interference of the 230 MHz full frequency band and the narrowband interference of high-power data transmission station. According to the distribution of the interference frequency and the impact on the service, it can be divided into three levels: broadband full-frequency interference (high), narrowband co-channel interference (medium) and narrow-band adjacent frequency interference (low). The causes and effects of broadband full frequency interference and narrowband co-frequency interference are analyzed. For broadband full frequency interference, due to the use of dual-antenna technology in 230 MHz power wireless private network, the UHF filter bank interference suppression algorithm is used in the uplink to suppress the interference, and the user-level power control algorithm is used in the downlink to increase the signal strength of specific users. For narrowband co-channel interference, random and fast frequency hopping methods are used to avoid narrowband co-channel interference.

The paper [8] is oriented to the dense urban environment and the network coverage area is divided into multiple geographical scenes by using spatial clustering technology. According to the terrain and feature information provided by the three-dimensional electronic map, the scene-oriented ray tracing propagation model is used to analyze the outdoor wireless signal coverage distribution; in order to solve the analysis error caused by the uncertainty of model parameters, a scene-oriented propagation model parameter correction is proposed. By using the Drive Test data, the multi-objective optimization model of propagation model parameters for scene is established, and multi-objective evolutionary algorithm is used to optimize the direct radiation, reflection, and diffraction coefficients of the model.

The paper [9] introduces dynamic spectrum sensing and spectrum planning and management schemes in LTE230 system, and proposes a sensing-based interference avoidance method. The authorized frequency points are separated to a certain extent by the system, that is, the 230 MHz frequency band is divided into multiple resource groups, and multiple systems conduct spectrum sensing based on resource groups to obtain available resource group resources and realize resource sharing. In order to ensure the normal operation of the sensing system and high real-time and high reliability service transmission, new authorized frequency points are redistributed within the limited range of each resource group. Finally, tests were carried out for co-channel interference and adjacent channel interference.

This paper [10] mainly analyses the situation that the power wireless private network developed on 230 MHz spectrum resources may share the same frequency band with 230 MHz data transceivers in the application process. In order to ensure that the two systems operate stably and efficiently at the same time, a trust-based cooperative spectrum sensing algorithm is proposed. According to the user behavior characteristics, the users are divided into trusted users, invalid users and interfering users, and corresponding judgment methods are given to untrusted users. At the same time, the relationship between the local detection results of the trusted users and the users participating in the cooperation and the signal-to-noise ratio of the communication channel are analyzed, and then the weight of each user's credibility is defined. On this basis, a cooperative spectrum sensing algorithm based on trust degree is proposed. The simulation results show that compared with the traditional hard-decision cooperative spectrum detection method, the cooperative sensing algorithm based on sensing user trust can obtain higher detection performance.

Although the existing schemes can monitor, identify and control the interference to a certain extent, there are still some problems. (1) Additional hardware and software are required; (2) The threshold for interference determination is relatively fixed, and there is a lack of consideration of the impact after dynamic control; (3) The specific control method for the interference frequency band is not considered; (4) The identification method of interference is not considered, and the requirements for the base station are very high, so some additional hardware modules need to be upgraded. The method proposed in this paper is mainly based on the network management system data to realize the effective judgment of the existence of interference, and through the power adjustment and the adjustment of the corresponding interference baseline, to achieve the effective control of the terminal interference, without additional hardware support. At the same time, it has both flexibility and effectiveness, which can effectively improve service transmission efficiency and ensure the reliability of power communication systems.

3 Security Situation Awareness and Control Method Based on Heuristic Algorithm

The process of the interference control mechanism of the LTE power wireless private network mainly includes three stages of monitoring, analysis and adjustment. The flow chart is shown below, the three processes form a closed loop process (Fig. 2).

A detailed description of each of the above stages is as follows.

3.1 Interference Signal Analysis Based on Network Monitoring

The monitoring stage is mainly to obtain the required network system parameter information through various methods, and calculate the terminal service quality. The data can be obtained from the interface of network management system and LTE power wireless private network terminal. The data and definitions that need to be obtained include:

$P_i^l(t)$: The transmission power of the i-th base station on the l-th subcarrier at time t.

$G_{ij}^l(t)$: The channel gain from the i-th base station to the j-th user's l-th subcarrier at time t.

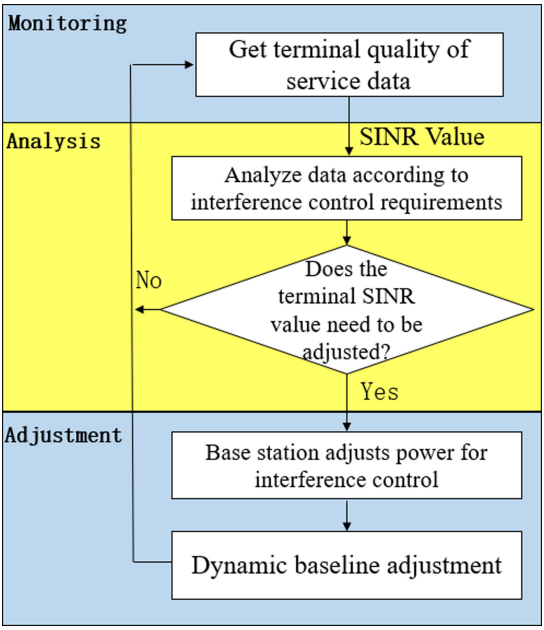

Fig. 2. Analysis of interference control flow.

$N_0(t)$: Noise power spectral density at time t.

W: Self-channel bandwidth.

$SINR_{ij}^{l}(t)$: The signal-to-noise ratio of the l-th subcarrier from the i-th base station to the j-th user at time t. The calculation formula is:

$$SINR_{ij}^{l}(t) = \frac{P_i^l(t)G_{ij}^l(t)}{\sum\limits_{j\in U} P_i^l(t)G_{ij}^l(t) + N_0(t)W} \tag{1}$$

$SINR_{ij}(t)$: The signal-to-noise ratio of the j-th user. The calculation formula is:

$$SINR_{ij}(t) = \sum_{l\in L} SINR_{ij}^{l}(t) \tag{2}$$

Where L is the set of subcarriers.

After obtaining these data through the network management system, it enters the analysis stage.

3.2 Analysis of Cyberspace Interference Situation Based on Baseline

In the analysis stage, by comparing the terminal signal-to-noise ratio data obtained in the monitoring stage with the preset baseline, the initial upper and lower baselines of acceptable SINR are set to γ_{max} and γ_{min} respectively, and the base station i is judged. Whether the served terminal has strong interference, the identification index $f_i(t)$ is defined as follows:

$$f_i(t) = Card\{i|SINR_{ij}(t) < \gamma_{\min}\}/|U_i| \tag{3}$$

The $card\{\cdot\}$ part represents the number of base station i whose signal-to-noise ratio is not higher than the minimum threshold, and U_i is the number of users served by base station i. $f_i(t)$ shows the proportion of users whose current signal-to-noise ratio is affected. According to this proportion, the process of interference identification technology to be adopted is as follows:

Step 1: Calculate the proportional value $f_i(t)$ for each base station i. If $f_i(t) = 0$, it is judged that there is no interference and no control will be given and return to the monitoring stage; if $0 < f_i(t) < \beta$, β is the proportion threshold, it is considered that the number of terminals subject to interference is small, and then proceed to step 2; if $\beta < f_i(t) < 1$, it is considered that a large number of terminals are interfered, and proceed to step 3.

Step 2: Determine the interfered terminal set U'_i and the corresponding subcarrier set L'_i through the analysis of the network management system, determine the base station transmission power P_i and the maximum transmission power P_{max}, and enter the adjustment stage.

Step 3: Analyze the network management system to determine the interfered terminal set U'_i, determine the base station's transmission power P_i and the maximum transmission power P_{max}, and enter the adjustment stage.

3.3 Dynamic Baseline Adjustment Based on Long Short Memory Model

According to interference control requirements, for terminals whose signal-to-noise ratio is based on the system baseline value, the base station accessed by the terminal during

the adjustment phase needs to adjust its transmit power to the connected user terminal to perform interference control to improve terminal service performance. The specific steps are as follows:

1) For the scenario of $0 < f_i(t) < \beta$, the power P_i^l of the subcarrier set L'_i is increased according to a uniform step size Δd, make $P_i \leftarrow P_i + |U'_i|\Delta d$; for the scenario of $0 < f_i(t) < \beta$, make $P_i \leftarrow P_i + \Delta e(\Delta e > \Delta d)$;
2) Determine whether P_i is less than P_{max}. If it meets the requirements, determine whether the user SINR in the adjusted terminal set U'_i are all greater than γ_{min} and less than γ_{max}. If so, the adjustment ends, the dynamic baseline update is performed, and return to the monitoring stage; otherwise return to step 1), if the power constraint is not satisfied, go to step 3;
3) Report the interference alarm to the network management system, after the adjustment is completed, return to the monitoring stage.

In step 2), the dynamic baseline update process is as follows:

The baseline γ_{max} and γ_{min} are used to indicate the relatively stable value of the SINR value over a period of time. The determination of the baseline is a key issue: if the baseline is too strict, the base station will frequently adjust the power; on the contrary, if the baseline is set too wide, the related service quality degradation cannot be dealt with in time, resulting in poor reception of the user terminal. The baseline calculation algorithm should be simple to implement, but with a high degree of confidence, in order to well reflect abnormal changes in business performance, that is, the extent to which the terminal service quality is affected by signal interference.

We set the baseline value of the acceptable signal-to-noise ratio SINR of the terminal in the system. This project will use the dynamic baseline algorithm, that is, after the power is adjusted, the corresponding baseline will be increased accordingly. With real-time monitoring of terminal service quality and timely detection of business performance abnormalities and interference control as the goal, this report adopts a dynamic method and the specific algorithm is described as follows:

1) Initialize the static baseline values γ_{max} and γ_{min};
2) For the relevant user j after the adjustment, it is assumed that a total of N SINR data are obtained, which are respectively recorded as $X_1, X_2, X_3, \ldots, X_i, \ldots, X_N$, suppose there are N' data of terminal SINR that are more severely interfered ($X_i < \gamma_{\min}$), calculate the average value $\overline{X} = \frac{1}{N'} \sum_{i=1}^{N} (X_i - \gamma_{\min})$ $(X_i < \gamma_{\min})$ of the data below the static baseline value.
3) For the current SINR of the interfered terminal, the SINR set $\boldsymbol{D}'(t) = \{D_1(t), D_2(t), \ldots, D_m(t)\}$ for different terminals i in space at time t, the goal is to predict the next parameter $\boldsymbol{D}(t+1)$. The core of LSTM is the hidden layer sequence $\boldsymbol{h} = \{h1, h2, \ldots, h_n\}$, the output is the predicted time series value $\boldsymbol{Z_t} = \{z_1(t), z_2(t), \ldots, z_n(t)\}$, its calculation method as follows:

$$\boldsymbol{z}_t = \boldsymbol{W}_{hz}\boldsymbol{h}_t + \boldsymbol{b}_y \tag{4}$$

The calculation process of the hidden layer sequence $\boldsymbol{h}_t$ at time t is as follows:

$$\boldsymbol{h}_t = \boldsymbol{o}_t \tanh(\boldsymbol{c}_t) \tag{5}$$

$$\boldsymbol{o}_t = \sigma(\boldsymbol{W}_{\boldsymbol{Lo}}\boldsymbol{L}(t) + \boldsymbol{W}_{\boldsymbol{ho}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\boldsymbol{co}}\boldsymbol{c}_t + \boldsymbol{b}_{\boldsymbol{o}}) \tag{6}$$

$$\boldsymbol{c}_t = \boldsymbol{f}_t\boldsymbol{c}_{t-1} + \boldsymbol{i}_t \tanh(\boldsymbol{W}_{\boldsymbol{Lc}}\boldsymbol{L}(t) + \boldsymbol{W}_{\boldsymbol{hc}}\boldsymbol{h}_{t-1} + \boldsymbol{b}_{\boldsymbol{c}}) \tag{7}$$

$$\boldsymbol{f}_t = \sigma(\boldsymbol{W}_{\boldsymbol{Lf}}\boldsymbol{L}(t) + \boldsymbol{W}_{\boldsymbol{hf}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\boldsymbol{cf}}\boldsymbol{c}_{t-1} + \boldsymbol{b}_{\boldsymbol{f}}) \tag{8}$$

$$\boldsymbol{i}_t = \sigma(\boldsymbol{W}_{\boldsymbol{Li}}\boldsymbol{L}(t) + \boldsymbol{W}_{\boldsymbol{hi}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\boldsymbol{ci}}\boldsymbol{c}_{t-1} + \boldsymbol{b}_{\boldsymbol{i}}) \tag{9}$$

Where $\boldsymbol{W}$ is the weight coefficient matrix of each layer, $\boldsymbol{b}$ is the bias vector of each layer, $\boldsymbol{i}, \boldsymbol{f}, \boldsymbol{c}$, and $\boldsymbol{o}$ are input gate, forget gate, cell state, and output gate respectively; σ and tanh are sigmoid and hyperbolic tangent, respectively activation function.

In order to ensure the accuracy of the model, the training process of the LSTM model is as follows:

Step 1: Calculate the output value of LSTM cell according to (4)–(9);

Step 2: Calculate the error term of each LSTM cell, including two back propagation directions according to time and network level;

Step 3: Calculate the gradient of each weight according to the corresponding error term;

Step 4: Apply gradient-based optimization algorithm to update weights.

In view of the above training process, this project will compare and analyze different hidden layer cell structures and different gradient optimization algorithms, and analyze the rationality of the prediction results. At the same time, compare the LSTM prediction model of this project with other neural network algorithms, S-ARIMA and other time series algorithms to verify its accuracy and effectiveness, so as to obtain the most accurate observation parameter results.

4) The baseline value is adjusted to $\gamma'_{\min} = \gamma_{\min} + \frac{1}{2}(\overline{X} + \sum_i \frac{z_i(t)}{|z(t)|})$, then enter the next stage for interference control and enter the monitoring stage.

4 Simulation and Implementation Analysis

In this chapter, the security situation awareness and interference control method proposed in the previous chapter will be verified by simulation, and the performance of the algorithm will be analyzed by comparing with other algorithms. The experiment is completed in the MATLAB simulation platform.

4.1 Simulation Environment Settings

In the simulation scenario, the network area is 1 000 m × 1 000 m, including 19 macro base stations with 57 cells and 80 terminals which are randomly deployed in the network (Fig. 3).

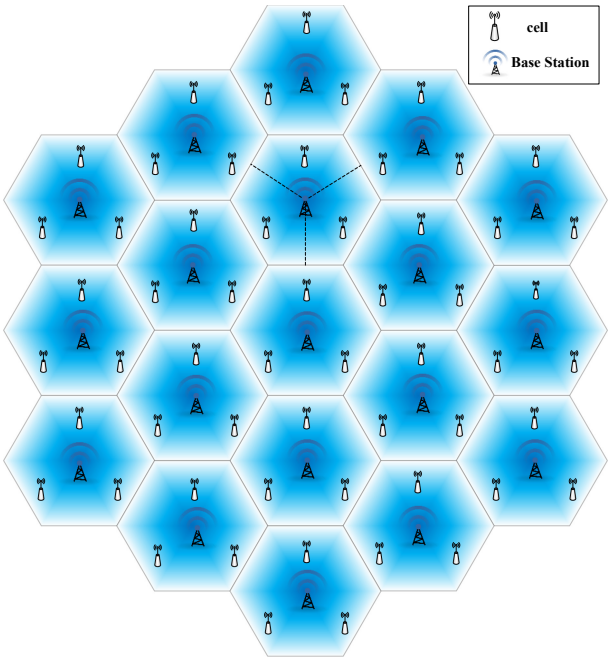

Fig. 3. Simulation scenarios.

The parameter values used in the simulation process are shown in Table 1 below.

Table 1. Simulation parameters

Parameters	Value	Unit
Antenna gain	10	dBi
Road loss model	$135.88 + 37.6\log_{10}$d	dB
power spectral density	−118.4	dBm
bandwidth	180	kHz
Speed requirement	0.5–1.5	Mb/s
RB amount	80	-
β	0.9	-
Maximum base station power	500	W
Δd	0.1	dBm
Δe	0.2	dBm
$P_{user-\min}$	−120	dBm
$\gamma_{\min}$	−10	dB
$\gamma_{\max}$	60	dB

Based on the simulation parameters given above, the simulation results of the distributed algorithm are given below.

4.2 Analysis of Simulation Results

With the simulation analysis, the interval distribution of SINR get by terminals with different signal is shown in the figure below. We can find that BS number 13 and 18 are affected with interferences (Fig. 4).

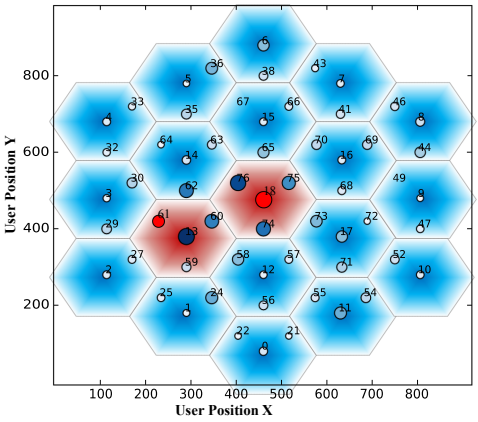

Fig. 4. Distribution interval diagram of signal strength.

Next, we use the time-varying noise as the experimental environment, as shown in Fig. 5 below, respectively set up three groups of simulation experiments, corresponding to high, medium and low noise environment. We find that SINR decreases with the increase of noise, so we need a control method to maintain network service quality.

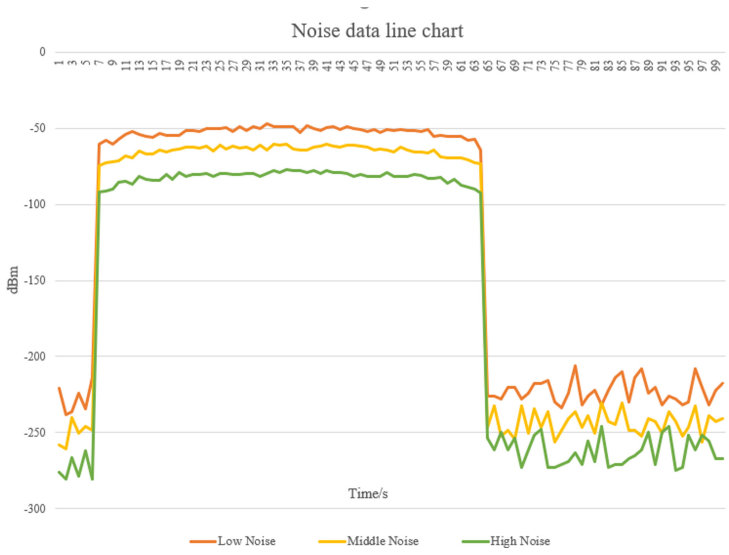

Fig. 5. Noise environment change chart.

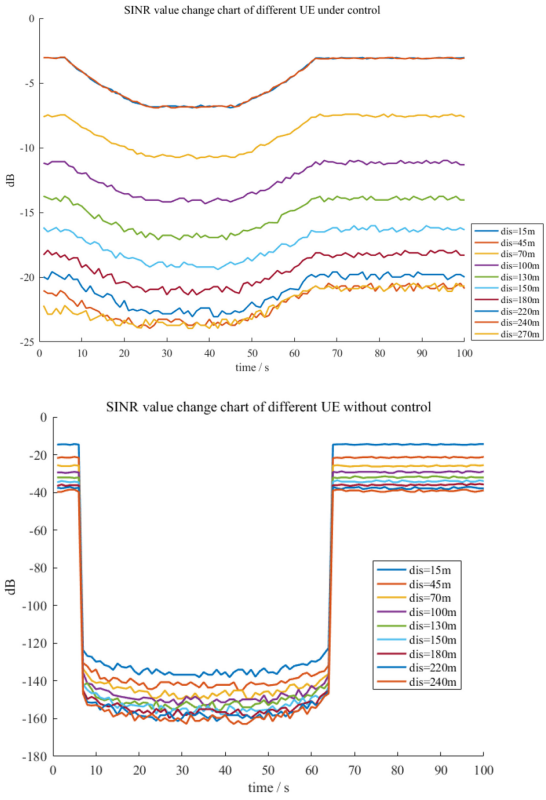

Fig. 6. Comparison of SINR simulation results under low noise environment.

Figure 6, Fig. 7 and Fig. 8 show the comparison of SINR values of several UE devices under controlled and uncontrolled conditions when the ambient noise is low, medium and high. It can be seen that no matter the environmental noise is high, medium and low, the fluctuation of SINR value in the controlled situation is much less than that in the uncontrolled situation, and the network also has better quality of service. Therefore, this algorithm can better maintain the network quality of service at a better level by dynamically adjusting the power of the base station in the case of large environmental noise.

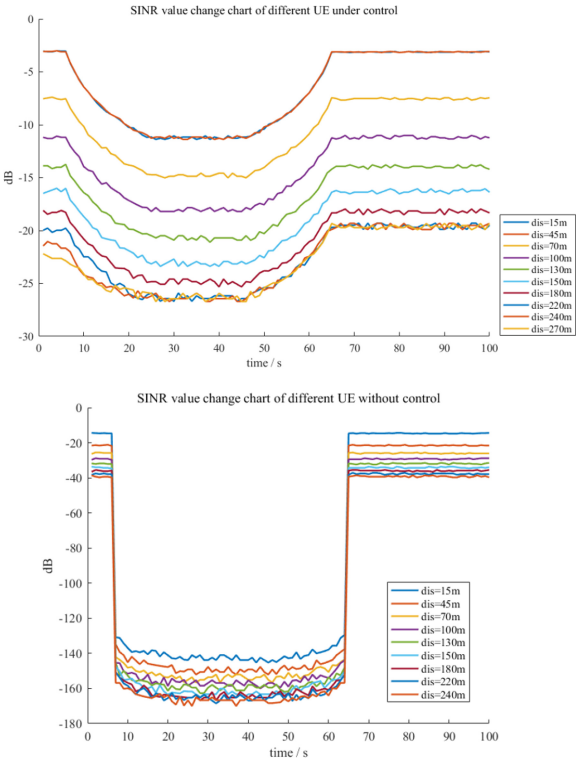

Fig. 7. Comparison of SINR simulation results under medium noise environment.

5 Conclusion

After fully investigating the existing network interference detection, interference analysis and interference control algorithms, this paper presents the advantages and disadvantages of each algorithm for different algorithms. At the same time, this paper proposes a dynamic baseline based security situation awareness and interference control algorithm for power wireless private network, and builds an experimental simulation and Simulation for the algorithm using MATLAB software The real results show that the continuous enhancement of noise will continue to reduce the network quality of service and the SINR value will continue to decrease. That is, the algorithm can maintain the SINR of all user devices to a certain extent.

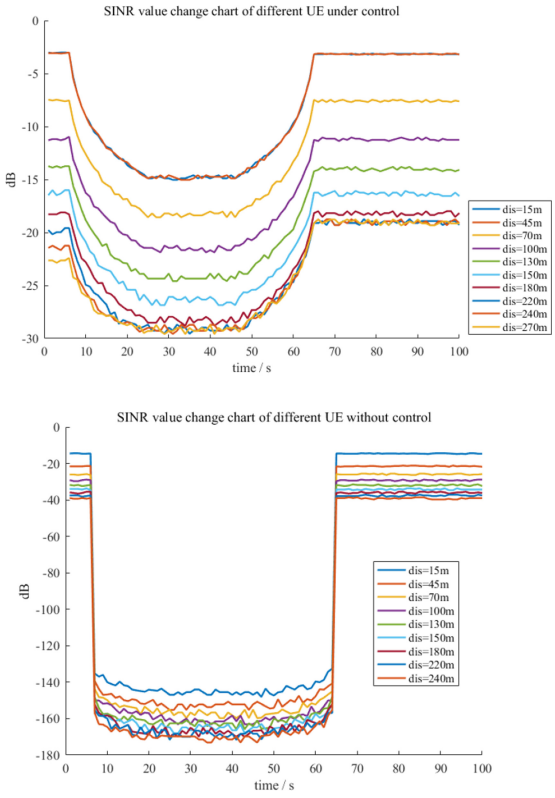

Fig. 8. Comparison of SINR simulation results under high noise environment.

Acknowledgement. This work is supported by Science and Technology Project from of State Grid Corporation of China: "Key technology Research and Application for Ubiquitous Inter-networking Security for Power wireless private network services (5700-201918229A-0-0-00)".

References

1. Cao, J., Liu, J., Li, X.: A power wireless broadband technology scheme for smart power distribution and utilization networks. Autom. Electric Power Syst. **37**(11), 76–80 (2013)
2. Sun, S., Cheng, Y.: Research on LTE power wireless private network for service coverage. Power Inf. Commun. Technol. **13**(4), 6–10 (2015)
3. Wang, H., Gu, S., Wanyan, S., et al.: Tracking and locating method of interference source in power wireless private network. Guangdong Electric Power **32**(6), 86–93 (2019)
4. Liu, R., Yu, J., Zhao, G., et al.: High reliability planning method for power wireless private network with low self interference. Power Syst. Autom. **42**(17), 162–167 (2018)
5. Kong, W., Luo, X., Liu, Y., et al.: Interference analysis of power wireless private network. Commun. Technol. **52**(01), 122–128 (2019)
6. Yin, J.: Research and application of location technology of unknown interference source outside LTE power wireless private network. Beijing University of Posts and Telecommunications (2019)

7. Tong, J., You, Q., Sun, C., et al.: Research on interference avoidance strategy of 230 MHz power wireless private network. Power Inf. Commun. Technol. **18**(3), 27–33 (2020)
8. Teng, J.: Research and application of high precision coverage interference sub technology in TD-LTE power wireless private network. Beijing University of Posts and Telecommunications (2019)
9. Zheng, W., Fang, J., Chen, P., et al.: Implementation and verification of an automatic interference avoidance method based on dynamic sensing. In: Proceedings of the Third Smart Grid Conference, pp. 507–513+520 (2018)
10. Cao, J., Li, W., Zhang, Y.: A trust based cooperative spectrum sensing algorithm for power wireless private networks. Telecommun. Sci. **31**(3), 136–141 (2015)