Hindawi
Security and Communication Networks
Volume 2023, Article ID 9845485, 1 page
https://doi.org/10.1155/2023/9845485

Retraction

Retracted: Information Processing Methods of Electronic Warfare Events Based on Communication Technology

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Mao, "Information Processing Methods of Electronic Warfare Events Based on Communication Technology," *Security and Communication Networks*, vol. 2022, Article ID 9309710, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9309710, 11 pages
https://doi.org/10.1155/2022/9309710

Research Article

Information Processing Methods of Electronic Warfare Events Based on Communication Technology

Hongyan Mao

Shenyang Institute of Engineering, Shenyang 110136, China

Correspondence should be addressed to Hongyan Mao; maohy@sie.edu.cn

Received 7 September 2021; Revised 26 October 2021; Accepted 6 November 2021; Published 4 January 2022

Academic Editor: Jian Su

Traditional electronic countermeasure incident intelligence processing has problems such as low accuracy and stability and long processing time. A method of electronic countermeasure incident intelligence processing based on communication technology is proposed. First, use the integrated digital signal receiver to identify various modulation methods in the complex signal environment to facilitate the processing and transmission of communication signals, then establish an electronic countermeasure intelligence processing framework with Esper as the core, and flow the situation to the processing conclusion through the PROTOBUF interactive format Redis cache. The data can realize the intelligent processing of electronic countermeasure incidents. The experimental results show that the method proposed in this paper increases the recall rate by 5 to 20% compared with other methods. This method has high accuracy and stability for electronic countermeasure incident intelligence processing and can effectively shorten the time for electronic countermeasure incident intelligence processing.

1. Introduction

Electronic warfare intelligence analysis system needs to process the information obtained by various sensors to obtain accurate battlefield situation intelligence [1]. For example, through electronic support measures to receive, sort, process, identify, and give omnidirectional warning to enemy radar or communication signals, at the same time, we need to take into account the enemy's target behavior obtained by our own sensors, enemy force deployment, and so on, to complete the threat warning of the enemy's attack, so as to carry out the subsequent electronic attack and defense process [2]. The task of modern electronic warfare is to weaken and destroy the enemy's electronic equipment and protect the effectiveness of one's own electronic system to be able to function normally [3]. In order to complete this task, the accuracy and integrity of intelligence information are particularly important. Therefore, in the face of various and incomplete information obtained from different platforms, how to carry out effective data fusion processing to maximize the accuracy of information and reduce information redundancy is the research focus in this field.

The electronic countermeasure situation processing system receives real-time target reconnaissance streaming data reported by the external intelligence information system and electronic reconnaissance equipment, and then through the three-layer extraction processing and correlation fusion of signals, radiation sources, and electronic targets, the electronic countermeasure situation processing conclusion is formed. At present, the research on intelligence information data processing has also made great progress. Reference [4] uses differential data processing methods to reduce the scale of wireless sensor intelligence information network transmission data. Based on the differential data processing of the node identification and the cluster head, the initially collected aggregate data is transmitted to the cluster head for comparison, and then the difference is transmitted to the cluster head. Use the reference data transmitted to the cluster head to perform differential processing on the collected data, and compare the low-energy adaptive clustering hierarchy and differential data processing performance. This method can reduce the energy consumption of data transmission in the intelligence information network. Reference [5] considers that electronic

countermeasure drones form an additional wireless network to assist the existing fixed base stations of the mobile wireless access network, using FSO and network control 6G drones and optimizing communication time constraints and processing time constraints. Considering the time limit, control the relationship between the number of intelligence data streams, input data rate, the number of working nodes, and errors that occur during communication and data processing. This method can effectively meet the time constraints of UAV control and wireless access network services. However, the above methods have the problems of low accuracy and stability of intelligence data processing and long processing time.

In view of the above problems, this paper puts forward the information processing method of electronic countermeasure events based on communication technology. The sampling signal is processed by frequency conversion, the subband signal is analyzed by spectrum, the sampling data of communication signal to be identified is preprocessed, the characteristic communication signal is extracted, and the modulation mode is identified. Use communication signal modulation and recognition to build an electronic countermeasure event model, use EPL language to describe the model for engine calculation, and build an electronic countermeasure intelligence processing framework with Esper as the core to realize electronic countermeasure event intelligence processing. It can effectively improve the accuracy and stability of electronic countermeasure incident intelligence processing and shorten the time of electronic countermeasure incident intelligence processing.

Mobile computing is a new technology emerging with the development of mobile communication, Internet, distributed computing, and other technologies. Mobile computing technology will make a computer or other pieces of information intelligent terminal equipment for data transmission in wireless environment and resource sharing; the information is passed to the remote server technology under a distributed computing environment; it can be useful, accurate, and timely information provided to any customer at any time and any place, to provide them with a ubiquitous mobile computing environment. This will greatly change the way people live and work.

Our contribution is threefold:

(1) Aiming at the problems of low accuracy and stability of electronic countermeasure incident intelligence processing and long processing time in current electronic countermeasure incident intelligence processing methods, an electronic countermeasure incident intelligence processing method based on communication technology is proposed.

(2) The FFT sampling rate is obtained by spectrum analysis of each subband signal. By preprocessing the sampling data of the communication signal to be identified, the characteristic communication signal is extracted, and the modulation mode is identified according to the envelope classification, the amplitude, phase and frequency changes, and the symmetry of the signal spectrum.

(3) The experimental results show that the proposed method has high accuracy and stability for electronic countermeasure incident intelligence processing and can effectively shorten the time for electronic countermeasure incident intelligence processing.

2. Communication Technology

2.1. Principles of Communication Signal Recognition. As important equipment of the satellite communication reconnaissance system, the main function of the receiver is to identify various modulation modes in the complex signal environment to facilitate the processing and transmission of communication signals. Satellite communication requires many effective components. The functional structure of the receiver is shown in Figure 1.

The 100 M~3 GHz RF signal received by the antenna is converted into an IF signal with a center frequency of 200 MHz by analog frequency conversion. After transforming the A/D converter into a digital signal, FFT transformation and modulation recognition are realized in the digital processing unit [6]. The communication digital receiver adopts the hardware platform of an integrated digital signal processor and realizes the corresponding functions by loading different FPGA and DSP programs. The process of communication signal modulation recognition is shown in Figure 2.

The verification equipment is composed of a test computer, which can realize the control of the upper computer, spectrum analysis, identification parameters, channelized data reception, spectrum display, BER test, and system overall function and index test.

2.2. Principle of Digital Downconversion and Digital Channelization

2.2.1. Digital Downconversion and Filtering. In order to realize the recognition, the sampling signal needs to be downconverted to complete the sampling rate change and get the appropriate sampling rate. As far as the actual system is concerned, if the decimation coefficient is required to be large, the excessive bandwidth of the designed digital filter will be very narrow [7]. If the order of the filter needs to reach thousands, the delay of the filter will be very large. Therefore, the multistage filter sampling structure is adopted; that is, the classical cascaded integral comb filter and half-band filter are used for filtering, and the polyphase filter bank is used for the last stage, which can reduce the amount of computation and the delay time of the system. Analog and digital modulation signals are implemented on an FPGA chip. Therefore, the signal sampled by AD is shaped first. After digital mixing, filtering decimation is carried out, and the first-stage decimation of data is realized by cascaded integral comb filter. The second-stage decimation is realized by a two-stage half-band filter. FIR filter is used to realize the third-stage decimation. In this paper, a three-stage cascaded integrator comb filter is used. The decimation multiple of the cascaded integrator comb filter can be determined by CIC,

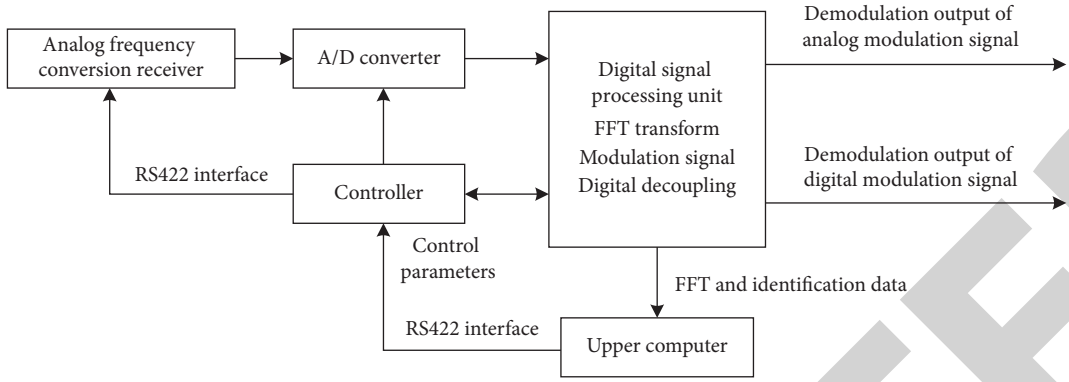


Figure 1: Functional structure of the receiver.

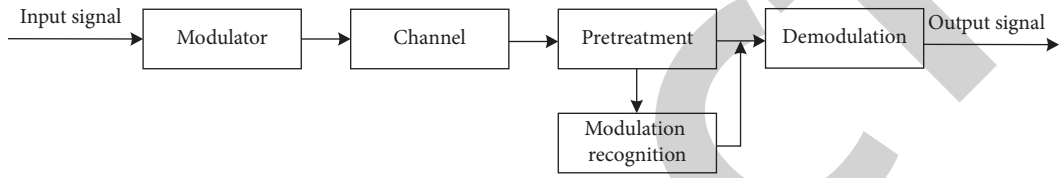


Figure 2: Communication signal modulation identification process.

SEL can be set, and the gain of cascaded integrator comb filter can be adjusted accordingly.

2.2.2. Frequency Band Channelization. Digital channelization is to divide the signal into several subband signal outputs. The high-speed sampling data can be decomposed into multichannel low-speed data, each output corresponding to different subbands, and then the frequency spectrum of each subband signal can be analyzed. The frequency band channelization structure is shown in Figure 3.

2.3. Spectrum Analysis. After digital downconversion, the signal sampled from AD is processed to get the appropriate FFT sampling rate. The implementation structure of spectrum analysis is shown in Figure 4.

Digital downconversion (DDC) has three main functions: digital mixing, low-pass filtering, and sampling rate conversion. The digital IF signal to be processed is multiplied by the quadrature LO signal generated by the numerically controlled oscillator (NCO) through the digital mixer. The out-of-band signal is filtered by a low-pass filter to extract the useful signal, and the signal is filtered and shaped according to the system requirements. Finally, the sampling rate of the signal is reduced to reduce the processing pressure of the subsequent DSP [8]. The decimation filter structure of the digital downconverter is shown in Figure 5.

The first stage of decimation filter adopts a cascaded integral comb filter, which can realize integer decimation. The filter can work in a high-speed environment without a multiplier, usually in the first stage of decimation or the last stage of interpolation in multirate signal processing. After that, the n-stage HB filter is cascaded to achieve 2N times decimation. Nearly half of the coefficients of the HB filter are zero, which can save resources in FPGA implementation. After the decimation of the above two filters, the sampling rate can be reduced to a very low level. At this time, let the signal pass through an FIR filter for filtering and shaping, and then FFT analysis can be carried out.

2.4. Modulation Recognition Principle of Communication Signal. Communication signal modulation recognition is a process of communication signal detection. In the spectrum monitoring receiver, the process of communication signal is usually divided into two steps: signal preprocessing and signal modulation recognition.

2.4.1. Communication Signal Preprocessing. The preprocessing of the sampled data of the communication signal to be identified should go through the following steps: first, judge whether the signal exists, then estimate the bandwidth and center frequency, correct the carrier frequency offset, and filter the noise. In the module of determining whether the signal exists or not, the noise threshold can be set according to the condition of the signal-to-noise ratio and compared with the power spectral density of the observed signal. If it is determined as a signal, the next step will be carried out; otherwise, the next sampling data will be received.

The estimation of signal bandwidth and signal power spectrum module is calculated by setting another threshold by noise power module [9]. Next, the carrier frequency is moved to the center frequency to simply correct the frequency offset. Finally, a filter corresponding to the estimated bandwidth is used to remove the out-of-band noise. In this process, the threshold setting has a direct impact on the final judgment result. The signal bandwidth and center frequency

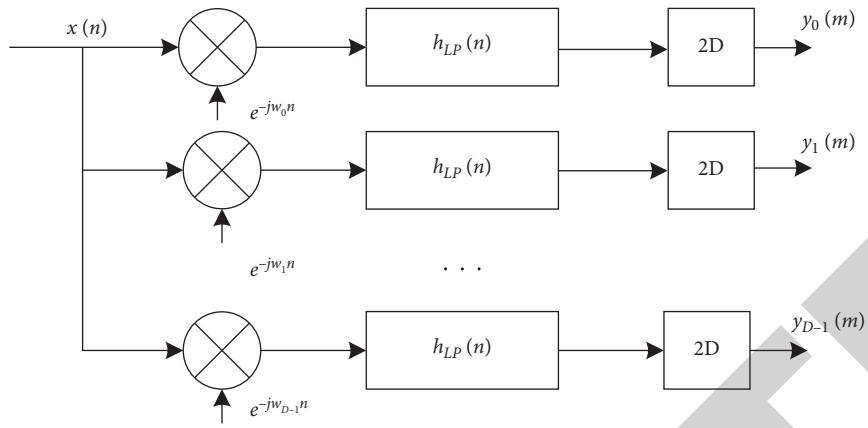


Figure 3: Band channelization structure.

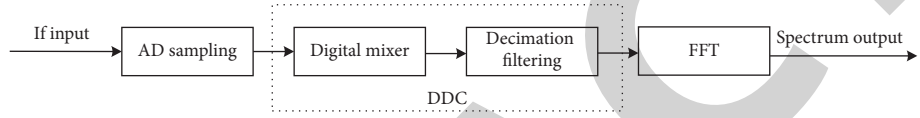


Figure 4: Implementation structure of spectrum analysis.

Figure 5: Decimation filter structure of digital downconverter.

can be estimated in frequency band spectrum scanning mode for setting in parameter measurement mode.

2.4.2. Feature Communication Signal Extraction. All kinds of estimators used in the process will use the instantaneous characteristics of the signal, the carrier frequency of the signal, and the symbol rate of the digital signal [10]. Therefore, the selection of appropriate methods to estimate these basic parameters is the premise of identifying the signal modulation style. The extraction and estimation methods of these basic parameters will be briefly introduced in the following.

According to the orthogonal transformation algorithm, the signal is orthogonally decomposed, the in-phase component $I(t) = a(n)\cos(\omega_c t)$ and the orthogonal component $Q(t) = a(n)\sin(\omega_c t)$ of the baseband signal can be obtained, and the instantaneous amplitude $a(n)$, instantaneous phase $\varphi(n)$, and instantaneous frequency $f(n)$ of the signal can be calculated:

$$a(n) = \sqrt{I^2(n) + Q^2(n)},$$
$$\varphi(n) = \arg\tan\frac{Q(n)}{I(n)}. \quad (1)$$

When using the formula to calculate the instantaneous phase, since the value range of the arctangent function is $[-\pi/2, +\pi/2]$ and the actual phase range should be $[0, 2\pi]$, there is phase convolution of $\pm\pi/2$ and $\varphi(n)$ must be phase unconvoluted. The method of deconvolution operation is to first determine the values of the in-phase component $I(n)$ and the quadrature component $Q(n)$, then discuss the quadrant where the instantaneous phase is located according to the signs of $I(n)$ and $Q(n)$, and adjust the value of $\varphi(n)$ accordingly, . So it expresses the value of $\varphi_{2\pi}(n)$ in the range $[0, 2\pi]$.

Use the difference sequence of the main value of $\varphi_{2\pi}(n)$ to find the discontinuity of the phase, and then correct $\varphi_{2\pi}(n)$. Then, the sequence phase after deconvolution is

$$\varphi(n) = \varphi_{2\pi}(n) + C(n). \quad (2)$$

In formula (2), $C(n)$ is the modified sequence. There is a linear phase component in the deconvoluted phase sequence, and the carrier frequency is the main reason for the existence of the linear phase component. In addition, in a modulated signal segment, noise and modulated signal also have some influence on the linear phase component. Therefore, it is necessary to process $\varphi(n)$ to remove the linear phase component to obtain a real phase sequence $\varphi_{\mathrm{NL}}(n)$.

Assuming that the carrier frequency f_c is accurately known, the nonlinear phase component can be calculated by formula (3) and expressed as

$$\varphi_{\mathrm{NL}}(n) = \varphi(n) - \frac{2\pi f_c n}{f_c}. \quad (3)$$

Assuming that the carrier frequency f_c is unknown, the least mean square algorithm can be used to calculate. First, let $(c_1 + c_2)$ represent the unknown linear phase component, minimize the sum of squares, and then find the values c_1 and c_2. The nonlinear phase at this time can be expressed as

$$\varphi_{\mathrm{NL}}(n) = \varphi(n) - c_1 n - c_2. \tag{4}$$

Since the carrier frequency is also unknown in advance, the second method is used to calculate the instantaneous nonlinear phase [11]. It can be obtained by deriving the obtained instantaneous phase:

$$f(t) = \frac{1}{2\pi} \frac{\mathrm{d}\varphi_{\mathrm{NL}}(t)}{\mathrm{d}t}. \tag{5}$$

There are two specific algorithms: one is to calculate the Fourier transform of $f(t)$ through frequency-domain calculation:

$$F(f) = -jf\Phi_{\mathrm{NL}}(f). \tag{6}$$

In (6), $\Phi_{\mathrm{NL}}(f)$ is the Fourier transform of $\varphi_{\mathrm{NL}}(t)$, and the instantaneous frequency can be expressed as

$$f(n) = \mathrm{IFFT}\left[-jf\Phi_{\mathrm{NL}}(f)\right]. \tag{7}$$

In formula (7), IFFT$[\cdot]$ is the inverse Fourier transform. Another method is to use the phase difference method of the signal. The difference algorithm mainly includes the following:

Forward difference formula:

$$f(n) = \frac{f_c}{2\pi}\left[\varphi_{\mathrm{NL}}(n+1) - \varphi_{\mathrm{NL}}(n)\right]. \tag{8}$$

Central difference formula:

$$f(n) = \frac{f_c}{4\pi}\left[\varphi_{\mathrm{NL}}(n+1) - \varphi_{\mathrm{NL}}(n-1)\right]. \tag{9}$$

Backward difference formula:

$$f(n) = \frac{f_c}{2\pi}\left[\varphi_{\mathrm{NL}}(n) - \varphi_{\mathrm{NL}}(n-1)\right]. \tag{10}$$

The frequency-domain method has better smoothness than the phase difference method, but the amount of calculation is too large, which affects the real-time performance, so in engineering applications, the phase difference method is generally used to calculate. From the above formula, it can be seen that, in the above three difference algorithms, the central difference algorithm has higher accuracy than the other two algorithms, but in practical application, it needs to go through the central normalization to obtain higher accuracy.

2.4.3. Communication Signal Modulation Identification Process. For FM, AM, FSK, BPSK, QPSK, OQPSK, MSK, 16QAM, 32QAM, and other modulation modes, the modulation modes are classified according to the envelope, and then the modulation modes are identified according to the changes of amplitude, phase and frequency, and the symmetry of signal spectrum. For the threshold of corresponding statistical eigenvalues, 16QAM and 32QAM can be further identified according to the instantaneous amplitude and phase eigenvalues. Digital modulation PSK, FSK (MSK), QAM, and other methods of recognition are not ideal, so it is necessary to use the improved algorithm for recognition.

(1) FSK, MSK, and FM: for FSK, MSK, and FM modulated signals, it is to distinguish baseband signals with two frequency values and continuously changing frequency values through statistical characteristics. First, the instantaneous frequency is calculated from the preprocessed zero-IF signal, and then according to the characteristics of FSK and MSK with two frequency values, the instantaneous frequency is, respectively, centralized transformed to make the frequency more centralized [12]. Finally, the frequency jump points of FSK and MSK modulation signals are determined. The flowchart of FSK and FM improved algorithms is shown in Figure 6.

As can be seen from Figure 6, the dotted line box contains the additional baseband signal waveform transformation required by the improved algorithm, and the corresponding FSK modulation modes, such as FSK and MSK, can be distinguished each time, so the statistical feature μ_{42}^{f} (compactness of zero center normalized instantaneous frequency) can be omitted. The waveform transformation of baseband signal should aim at the specific modulation mode. For example, the waveform transformation of FSK can be realized by the symmetrical flip of two frequency values and the substitution of jump points. FSK and MSK can be distinguished according to the phase continuity or the proportional relationship between symbol rate and carrier frequency.

(2) PSK: for BPSK, QPSK, and OQPSK modulated signals, it is to distinguish several phase values of baseband signal by statistical characteristics. First, the instantaneous phase is calculated from the preprocessed zero-IF signal, then the instantaneous frequency is obtained after phase deconvolution, and the residual carrier is calculated from the nonweak signal, which is caused by the carrier estimation error during preprocessing. The phase is decoiled, then the linear phase is removed, and the phase of the jump point is replaced by the previous nonjump phase to remove the phase jump point [13]. Finally, according to the characteristics of BPSK and QPSK phase values, the instantaneous phase is transformed intensively to make it more concentrated, and then it can be realized according to the statistical characteristics of the phase. The flowchart of PSK and QAM improved algorithms is shown in Figure 7.

As can be seen from Figure 7, in the dotted box is the baseband signal waveform transformation required by the improved algorithm, and the corresponding PSK modulation mode is obtained by each identification. QPSK and OQPSK can be distinguished by phase hopping. Because the improved algorithm increases the waveform transformation and omits the compactness (fourth-order moment) feature extraction of instantaneous amplitude and frequency, it will not adversely affect the complexity. Detailed analysis needs more careful calculation and comparison.

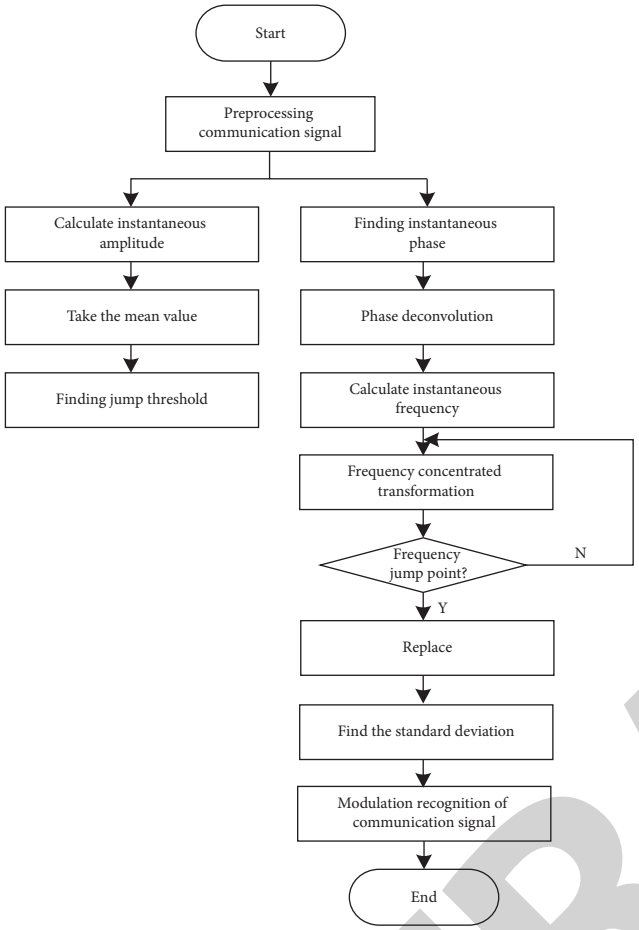


Figure 6: Flowchart of FSK and FM improved algorithms.

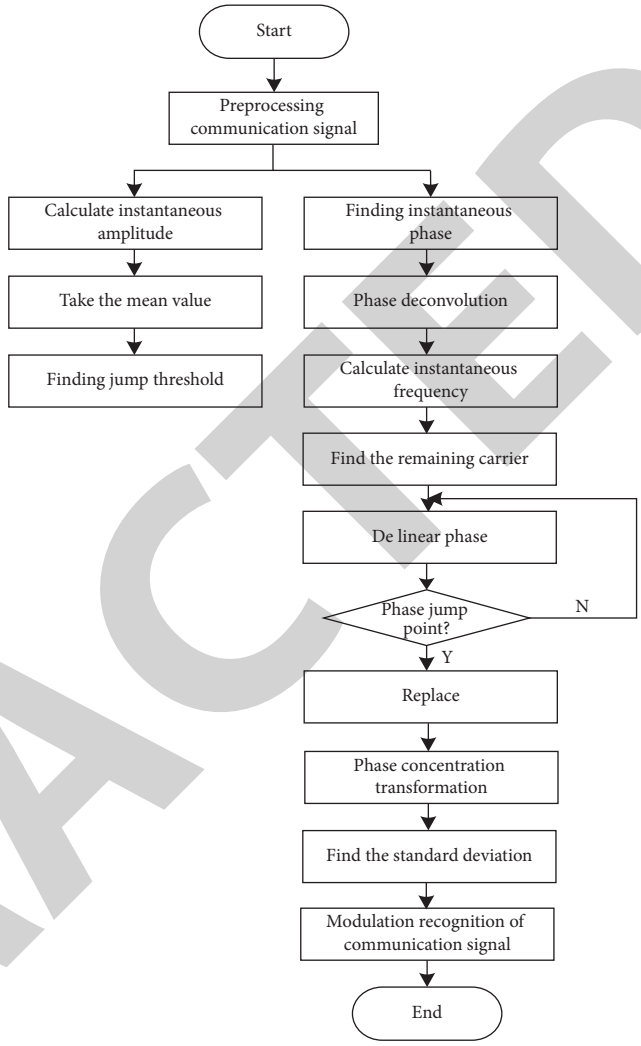


Figure 7: Flowchart of improved PSK and QAM algorithms.

3. Information Processing Method of Electronic Countermeasure Events

3.1. Electronic Countermeasure Event Model. In the event processing process, simple events are extracted through goals and simple event rules, and multiple simple events are extracted according to complex event rules to extract complex events. Therefore, the use of communication signal modulation recognition and the construction of electronic countermeasure event models are also divided into simple event models and complex event models to describe separately.

(1) Simple event model: In the field of reactance, ECM events are described as the status, tasks, anomalies, alarms, and predictions of electronic targets and transmitters and reconnaissance equipment in time, space, and frequency domain, and environment. The simple event model of electronic countermeasures describes the various elements of the event and the conditions that need to be met. It is mainly composed of event information, target information, environmental information, and event rules. The target information includes basic target information, time information, spatial information, interception information, emitter usage, and emitter parameters [14]. The simple event model of electronic countermeasures is shown in Figure 8.

The electronic countermeasure event model can be defined as a four-tuple:

$$\langle \text{Event; Target; Environmet; Stimulation} \rangle. \quad (11)$$

In formula (11), Event is basic event information, including event identifier, event category, event name, and time of occurrence. Target is the target information. Environmet is the environmental information used to describe other environmental factors that have an impact on the event. Stimulation is an event rule, which mainly describes the target and environmental conditions when a specific event is triggered.

(2) Complex event model: simple events can be defined as atomic events that extract complex events. A large number of atomic events enter the complex event processing engine in a certain time series to form an atomic event flow. Complex events will be generated when complex events are processed on the atomic

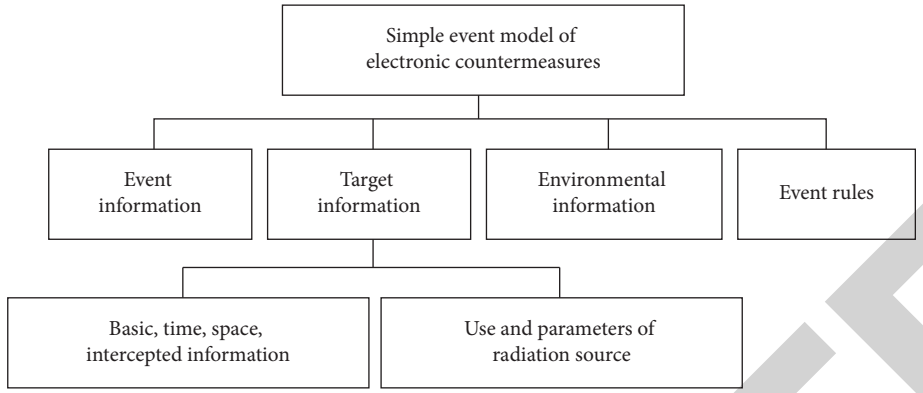


Figure 8: Simple event model of electronic countermeasures.

event flow. Assume that E is a limited set of atomic events that can be detected by the complex event processing engine; namely,

$$E = \{en | n = 1, 2, \ldots, n\}. \quad (12)$$

In formula (12), e is an event instance belonging to the set E. Suppose C is the complex event detected and output by the complex event processing engine. Here, a triple event model is used to represent the complex event; namely,

$$C = \langle C\_\text{Event}; E; \text{Rules} \rangle. \quad (13)$$

In formula (13), C_Event represents the basic information of a complex event, including identifiers, event types, event names, and event occurrence time, E represents a limited set of event streams that satisfy a certain relationship pattern, and Rules represents the rules for detecting complex events. Use the relationship model between events. The electronic countermeasure complex event model is shown in Figure 9.

Among them, the common rules of complex event extraction can be described as three kinds: time sequence, causality, and aggregation. Taking the reconnaissance mission carried out by the reconnaissance aircraft as an example, considering the airport location, mission area, aircraft location, aircraft altitude, radar working mode, and other pieces of information, the atomic events that can be detected include aircraft take-off, aircraft going to the mission area, reconnaissance in the mission area, aircraft return, and landing [15]. By detecting atomic events, combined with timing extraction rules, we can extract a complete description of complex events of reconnaissance aircraft.

3.2. Framework and Process of Electronic Countermeasure Incident Intelligence Processing. After the event model is defined, the EPL language is used to describe the model, and the model described in the EPL language can be directly used for engine calculation. The electronic countermeasure intelligence processing framework built with Esper as the core is shown in Figure 10.

According to Figure 10, the framework is mainly composed of three parts: data conversion agent, event

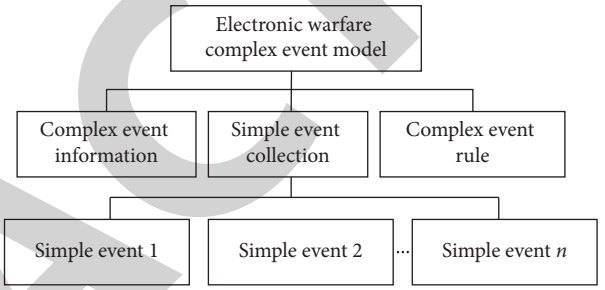


Figure 9: Electronic countermeasure complex event model.

intelligence data bus, and event intelligence processing engine. Among them, the data conversion agent realizes the conversion between the data of different technical systems and the PROTOBUF format. The event intelligence processing engine is the core component of the system, which realizes the integration of event intelligence detection and processing algorithms. The event intelligence data bus provides cross-platform high-speed caching through Redis and implements a subscription distribution mechanism. The main flow of electronic countermeasure incident intelligence processing is shown in Figure 11.

According to Figure 11, firstly, EW events are defined based on prior knowledge and expert experience, and event rules are symbolized as an event description language. Then, load the event description language into the event processing engine and register the corresponding listener for each type of event, access the electronic countermeasure situation processing conclusion streaming data through the PROTOBUF interactive format Redis cache, and perform data cleaning in the data preprocessing module and event format conversion. Then start the event processing engine to detect electronic countermeasures. After detecting the event, the corresponding listener is triggered, and subsequent processing and event management are performed in the listener. Finally, the event processing results are sent to the electronic countermeasure situation processing system through the PROTOBUF interactive format and Redis cache to form electronic countermeasure event intelligence to serve for combat command decision-making.

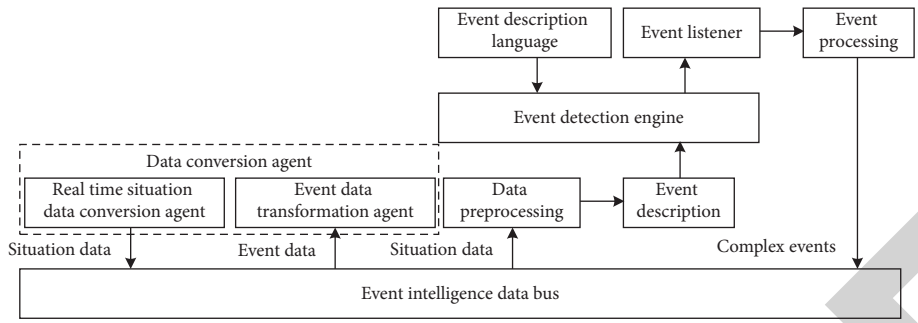


Figure 10: Electronic countermeasure incident intelligence processing framework.

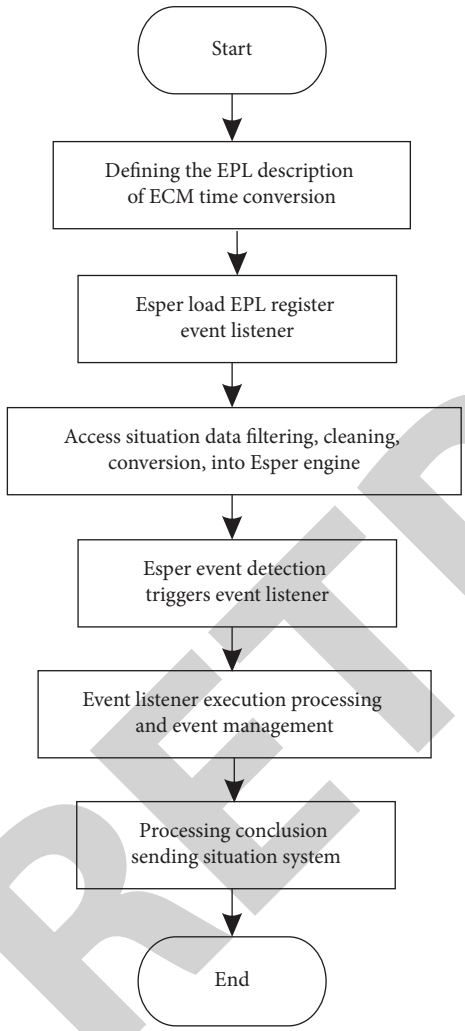


Figure 11: Information processing flow of electronic countermeasure events.

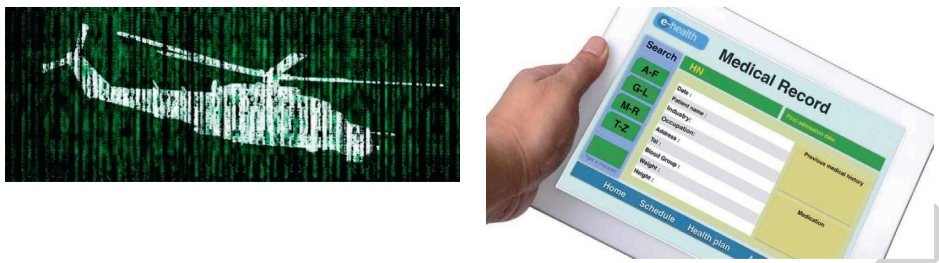
This approach could be used for a wide range of applications, such as stealth fighter detection and even medical care. Stealth fighters often have a very strange appearance and the general millimeter-wave radar is not easy to find them, but in the long-wave radar or multibase radar array, it is nowhere to hide. And we know that the ionosphere of the atmosphere can also reflect radar waves if radar cannot find the plane, but its shadow on the ionosphere is not wiped. The precision of some special detection components in medical equipment can be improved if electronic countermeasure technology is used. The photos of applications of the proposed research are shown in Figure 12.

4. Experimental Simulation and Analysis

4.1. Set Up the Experimental Environment. In order to verify the effectiveness of the electronic countermeasure incident intelligence processing method based on communication technology, the experimental environment used in this paper is Intel Core i5-3470 processor with 4.00 GB memory. The entire experimental system is developed in Java language, and the server is configured with RedHat Advanced Server 3.0 operating system. The event generator is used to generate the event stream to simulate the event stream in actual applications. There are 25 atomic event types in the event generator, and each event contains 5 attributes.

4.2. Stability Comparison of Information Processing Results of Electronic Countermeasure Incidents. Based on the electronic countermeasure event intelligence data, the proposed method, reference [4] method, and reference [5] method are used to process the electronic countermeasure event intelligence, and the comparison results of the stability of the electronic countermeasure event intelligence processing results of different methods are obtained as shown in Figure 13.

It can be seen from Figure 13 that as the electronic countermeasure event intelligence data increases, the signal-to-noise ratio of the electronic countermeasure event intelligence processing results of different methods decreases. When the electronic countermeasure event intelligence data is 5000 MB, the signal-to-noise ratio of the electronic countermeasure event intelligence processing result of reference [4] method is 24.8 dB, and the signal-to-noise ratio of the electronic countermeasure event intelligence processing result of reference [5] method is 23.4 dB. The signal-to-noise ratio of the electronic countermeasure event intelligence processing result of the proposed method is 30 dB. It can be seen that the signal-to-noise ratio of the electronic countermeasure event intelligence processing result of the proposed method is larger, and the electronic countermeasure event intelligence processing result is more stable.



(a) (b)

Figure 12: The photos of applications of the proposed research. (a) Stealth fighter detection. (b) Healthcare.

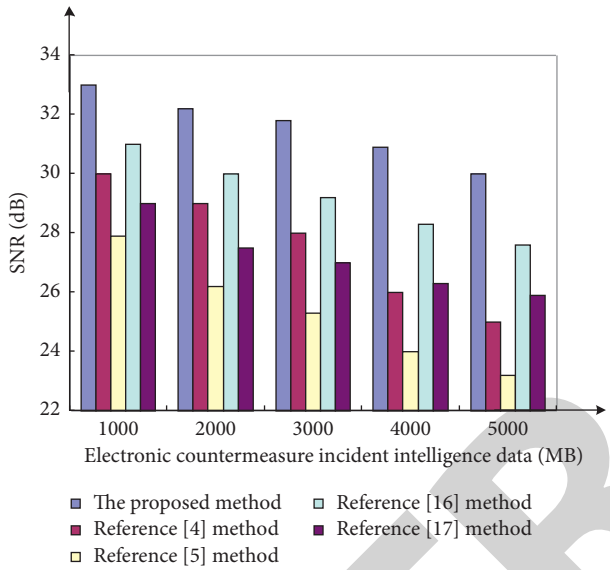


Figure 13: Comparison of the stability of the results of electronic countermeasure incident intelligence processing by different methods.

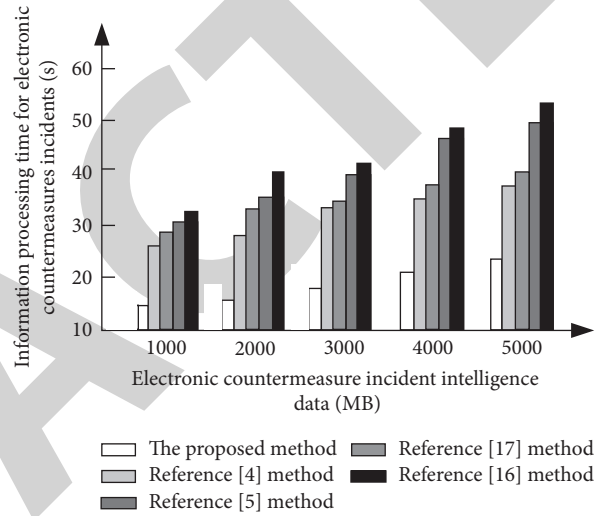


Figure 14: Comparison results of different methods of electronic countermeasure incident intelligence processing time.

4.3. Comparison of Information Processing Time of Electronic Countermeasure Incidents. On this basis, in order to further verify the electronic countermeasure event information processing time of the electronic countermeasure event information processing method based on communication technology, the proposed method, reference [4] method, and reference [5] method are used to process electronic countermeasure event intelligence. The comparison results of the information processing time of electronic countermeasure events obtained by different methods are shown in Figure 14.

It can be seen from Figure 14 that, with the increase of electronic countermeasure event intelligence data, the processing time of electronic countermeasure event intelligence in different methods increases. When the electronic countermeasure event intelligence data reaches 5000 MB, the electronic countermeasure event intelligence processing time of reference [4] method is 37s, the electronic countermeasure event intelligence processing time of reference [5] method is 50 ms, and the electronic countermeasure event intelligence processing time of the proposed method is only 23 ms. It can be seen that the electronic countermeasure incident intelligence processing time of the proposed method is relatively short.

4.4. Comparison of Intelligence Processing Accuracy of Electronic Countermeasure Incidents. In order to further verify the processing accuracy of the electronic countermeasure event intelligence processing method based on communication technology, three performance indicators, namely, accuracy, recall ratio, and F-test value, are selected to detect the accuracy of the electronic countermeasure event intelligence processing. The performance index is expressed as follows:

(1) Accuracy: this performance index can reflect the percentage of correct results in the intelligence processing results of electronic countermeasure incidents. Its expression is

$$\mathrm{ACC} = \frac{S_c}{S_z} \times 100\%. \tag{14}$$

In formula (14), S_c represents the number of correct electronic countermeasure incident intelligence processing and S_z represents the total number of electronic countermeasure incident intelligence processing.

Table 1: Comparison results of different methods of electronic countermeasure incident intelligence processing accuracy.

Performance index	The proposed method	Reference [4] method	Reference [5] method	Reference [16] method	Reference [17] method
Accuracy (%)	90	74	82	79	85
Recall rate (%)	80	69	75	72	78
F-test value (%)	85	65	74	75	81

(2) Recall ratio: this performance index can reflect the percentage of correct results in the total number of information processing of such electronic countermeasure incidents in the results of the information processing of electronic countermeasure incidents. Its expression is

$$\mathrm{RR} = \frac{S_c}{S_l} \times 100\%. \tag{15}$$

In formula (15), S_l represents the total amount of intelligence processing of this type of electronic countermeasure event.

(3) F-test value: the two indicators of accuracy and recall reflect two different aspects of the processing results. There is a new evaluation index F-test value, which can comprehensively evaluate the effect of electronic countermeasure incident intelligence processing. The larger the F-test value, the higher the accuracy of electronic countermeasure incident intelligence processing. Its expression is

$$F = \frac{\mathrm{ACC} \times \mathrm{RR} \times 2}{\mathrm{ACC} + \mathrm{RR}} \times 100\%. \tag{16}$$

We use the above formulas to calculate the three performance indicators of accuracy, recall, and F-test value for the proposed method, reference [4] method, and reference [5] method, and the comparison results of the accuracy of electronic countermeasure event intelligence processing of different methods are obtained as shown in Table 1.

According to the data in Table 1, the accuracy, recall, and F-test values of reference [4] method are 74%, 69%, and 65%, respectively; the accuracy, recall, and F-test values of reference [5] method are 82%, 75%, and 74%, respectively; and the accuracy, recall, and F-test values of the proposed method are 90%, 80%, and 85%, respectively. It can be seen that the accuracy rate, recall rate, and F-test value of the proposed method are relatively large, which can effectively improve the accuracy of electronic countermeasure incident intelligence processing.

5. Conclusion

The information processing method of electronic countermeasure events proposed in this paper can effectively improve the accuracy and stability of electronic countermeasure event information processing and shorten the time of electronic countermeasure event information processing. The writing contributions of this paper include the following:

(1) Propose an electronic countermeasure incident intelligence processing method based on communication technology.

(2) Use the integrated digital signal receiver to identify various modulation methods in the complex signal environment to facilitate the processing and transmission of communication signals, and then establish an electronic countermeasure intelligence processing framework with Esper as the core.

(3) Cache the situation flow to the processing conclusion through the PROTOBUF interactive format Redis

However, this paper does not involve specific electronic countermeasure incident intelligence examples. Therefore, in the following research, it is necessary to conduct in-depth research in conjunction with more areas of intelligence data examples to better adapt to the characteristics of high dimensions and large data volume of material data in intelligence work so as to further improve the efficiency of intelligence processing results and accuracy. For future research, how to overcome the impact of electronic interference at different time points is a research focus.

Data Availability

The datasets of this work are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest in publishing this article.

Acknowledgments

This work was supported by the Science and Technology Plan Project of Liao Ning (2019JH8/10100083) and the Natural Science Foundation of Liao Ning (2019-ZD-0523).

References

[1] K. Premchand and P. H. Krishna, "A miniaturized multi-octave Vivaldi antenna for electronic warfare systems," *Electromagnetics*, vol. 40, no. 1, pp. 1–14, 2019.

[2] Y. Sun, Z. Tian, M. Li, C. Zhu, and N. Guizani, "Automated attack and defense framework toward 5G security," *IEEE Network*, vol. 34, no. 5, pp. 247–253, 2020.

[3] D. Chatterjee and S. K. Mazumder, "Switching-sequence control of a higher order power-electronic system driving a pulsating load," *IEEE Transactions on Power Electronics*, vol. 35, no. 1, pp. 1096–1110, 2020.

[4] K. K. Lim, J. Park, and J. G. Shon, "Differential data processing technique to improve the performance of wireless sensor

networks," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4489–4504, 2019.

[5] S. Seo, D. E. Ko, and J. M. Chung, "Combined time bound optimization of control, communication, and data processing for FSO-based 6G UAV aerial networks," *ETRI Journal*, vol. 42, no. 5, pp. 700–711, 2020.

[6] M. Weilenmann and R. Colbeck, "Self-testing of physical theories, or, is quantum theory optimal with respect to some information-processing task?" *Physical Review Letters*, vol. 125, no. 6, pp. 349–355, 2020.

[7] N. C. W. Treleaven, M. Staufer, A. Spencer, A. Garmory, and G. J. Page, "Application of the PODFS method to inlet turbulence generated using the digital filter technique," *Journal of Computational Physics*, vol. 415, Article ID 109541, 2020.

[8] M. Pelusi, T. Inoue, and S. Namiki, "Brillouin amplifier noise characterization by a coherent receiver and digital signal processing," *Journal of Lightwave Technology*, vol. 38, no. 16, pp. 4221–4236, 2020.

[9] P. Pace, G. Fortino, Y. Zhang, and A. Liotta, "Intelligence at the edge of complex networks: the case of cognitive transmission power control," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 97–103, 2019.

[10] Y. H. You and J. H. Paik, "Suboptimal maximum likelihood detection of integer carrier frequency offset for digital terrestrial television broadcasting system," *IEEE Transactions on Broadcasting*, vol. 66, no. 1, pp. 195–202, 2019.

[11] S. V. Palacio and R. A. Herrera, "Dispersive wave and four-wave mixing generation in noninstantaneous nonlinear fiber solitons," *Applied Optics*, vol. 58, no. 10, pp. 2736–2744, 2019.

[12] P. H. R. D. Silva, C. Rondinoni, and R. F. Leoni, "Non-classical behavior of the default mode network regions during an information processing task," *Brain Structure and Function*, vol. 225, no. 8, pp. 2553–2562, 2020.

[13] C. Wang, J. Zhou, Y. Zhao, Y. Chen, B. Yu, and L. Lu, "Measurement of the feedback coefficient by monitoring the power difference at power jump point in self-mixing vibration signal," *Current Applied Physics*, vol. 19, no. 5, pp. 646–650, 2019.

[14] W. Ye, Z. Yu, H. Wang, and K. Zhang, "Recognition algorithm of emitter signals based on CNN," *Computer Simulation*, vol. 36, no. 9, pp. 33–37, 2019.

[15] H. Aygun and O. Turan, "Exergo-economic analysis of off-design a target drone engine for reconnaissance mission flight," *Energy*, vol. 224, no. 3, Article ID 120227, 2021.

[16] S. J. Kwon, B. Kang, C. Choi, and T. G. Kim, "Adaptive discrete event simulation systems to embrace changes of requirements using event control models," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 3, pp. 1147–1160, 2017.

[17] L. Maruster and A. Alblas, "Tailoring the engineering design process through data and process mining," *IEEE Transactions on Engineering Management*, vol. 5, pp. 1–15, 2020.