Simulation Study on Iterative Detection of Abnormal Attack Characteristics in Optical Fiber Communication Networks

Wang Lei

Nanjing College of Information Technology, Nanjing, Jiangsu, China

Keywords: Optical Fiber Communication Network, Exception attack, Features, Iterative detection, Simulation.

Abstract: Accurate detection of abnormal signals in optical fiber communication network can effectively maintain the security of network operation and improve the efficiency of internal system operation. However, at present, the distribution of network nodes in optical fiber communication network is relatively scattered, and the faults are random and uncontrollable, which directly affects the operation security of optical fiber communication network. Under the measurable model, the traditional autonomous sensing analysis method can not accurately determine the abnormal attack signal in the fiber-optic communication network, which leads to low detection efficiency. Therefore, based on the iterative detection principle of abnormal attacks in optical fiber communication networks, this paper studies the iterative detection process of abnormal attacks in optical fiber communication networks, and gives a brief overview of the detection steps, and gives the corresponding training methods, which has important reference value for improving the detection efficiency.

1. Research background

1.1 Literature review

Huang Yong and others pointed out the necessity of network maintenance in view of the power failure of optical fiber network. On this basis, according to the breakpoint detection method and the self-induction analysis and playback, under different network structures, through the judgment of the network nodes, and then detect the reasons for the low efficiency of the network. Therefore, a breakpoint detection model of neural network optical fiber communication network is proposed. By storing a large amount of information data in distributed detectors, and putting forward corresponding training methods, it is found that this method has high detection efficiency (Huang et al,2014). Under the background of high-tech development, all-optical network, as a major trend of communication network development, has incomparable advantages compared with other networks. By introducing the advantages of all-optical networks and the possible attack modes, Yang Hua discussed the method of detecting attack targets in all-optical networks using optical fiber network sensors, which is of great practical significance to the research in related fields (Yang,2012). Zhou Yingjie et al. proposed an anomaly flow detection method to solve the problem that the existing network traffic characteristic parameters cannot detect and identify distributed denial of service and denial of service. Through the comprehensive analysis of this method, we can judge whether the abnormal behavior belongs to distributed denial of service or denial of service. While ensuring the timeliness of detection, we can also accurately identify the network traffic related to attacks (Zhou et al,2013). Optimal laser sensor points are selected for optical fiber communication network after being intruded by network hackers. It can effectively inhibit the intrusion of similar hackers. However, the traditional laser sensor node selection technology still has a big problem, which cannot distinguish the advantages and disadvantages of the system, and is not conducive to the effective application of network optical fiber. He yuan and Xie linxu put forward the simulation algorithm of the optimal laser sensor node based on the problem of selecting the laser sensor node. By selecting the analysis method on the optimal laser sensor node after hacker intrusion, they can effectively shorten the time of network intrusion detection and improve the reliability of network

  DOI: 10.25236/scmc.2019.048

monitoring (He and Xie, 2018). Li Yanyan and He Yong put forward a new method of using optical power value to monitor optical fiber fault diagnosis in the process of studying the fault diagnosis of optical fiber network. By using the corresponding fault curve, the accurate optical fiber fault location can be obtained finally, which can provide theoretical data basis for fault location and greatly improve the accuracy of the diagnosis results (Li and He,2014).

1.2 Purpose of research

With the rapid development of big data, Internet of Things and other emerging technologies, the Internet has gradually been widely used in people's lives. While improving the efficiency of network communication, it can also effectively improve the speed of data conversion (Wang,2019). In the Internet, if the optical fiber interrupts, or the optical transmission equipment has a big fault, the large-scale optical fiber network circuit related services will also be interrupted, which will bring greater hidden dangers to the safe operation of the network, and also cause the enterprise to suffer greater economic losses. In the practical application process, large-scale optical fiber communication network is disturbed by different factors, resulting in breakpoints with great volatility and randomness. In general, large-scale breakpoints in optical networks will directly affect communication, while a single breakpoint will not directly affect communication. Under the traditional detection method of autonomous induction analysis, it is impossible to judge the fault breakpoints of large-scale networks through different detection nodes. It is necessary to detect different network nodes one by one, and establish the correlation between different nodes, then carry out fault detection. The overall detection process has the problems of difficult detection and low efficiency, which is not conducive to improving the utilization efficiency of optical network. Therefore, aiming at the problem of abnormal attacks in optical fiber communication networks, this paper proposes a feature iteration detection method, which is of great significance to troubleshooting of large optical fiber networks.

2. Iterative detection principle of abnormal attack in optical fiber communication network

According to the data detection principle of anomaly attacks in optical fiber communication networks, anomaly attacks mainly include feedback data, historical records and fault data. In general, the optical fiber communication network has high stability in the specific work process. The internal current and voltage will not cause strong changes in the system, and the internal communication is relatively normal. When the optical fiber network works for a period of time, a node in the network will produce energy exhaustion, which will eventually lead to network breakpoints. In this case, the abnormal attack in optical fiber communication network is attacked into the network, resulting in a larger problem in the operation of a node of the network, which greatly reduces the efficiency of network operation. On this basis, a self-induction principal component algorithm is proposed. The algorithm mainly reflects the interference effect of the network internal model on the related elements of nodes through feedforward and later feedback, and then obtains the characteristics of each node in the optical fiber network.

In optical network, anomaly attack diagnosis system mainly includes three levels. Among them, the first layer is data acquisition layer, which mainly uses OTDR to detect the characteristics of each node in the optical fiber communication network, and then obtains the corresponding optical fiber curve. Finally, according to the degree and length of optical fiber weakness, anomalous attack diagnosis is carried out. After the diagnosis is completed, the data is transferred and transformed again according to the corresponding process. The second layer is the background service layer, which mainly provides basic service support for the system. Background service layer generally includes database, electronic map and control program. In the specific operation, after the background service layer detects the abnormal signal in the optical fiber communication network, it sends the test command to RTU, and then uses the switch to transmit the corresponding test data to the abnormal optical fiber communication network. In the communication network, by judging the abnormal attack signal, the specific location of the signal can be determined, and the corresponding warning information can be sent to the data server to ensure the reliability of the network data. The

third layer is for the client, mainly in the optical fiber network, with the help of the client for data browsing and service response, to realize the switch of different map interfaces at any time, to prevent multiple customers from accessing a hardware device at the same time, thus causing data conflicts in the system.

Abnormal attack signal detection in optical fiber communication network is an independent testing system, which can provide standard service interface for back-end servers and realize internal data exchange. In the process of internal system operation, abnormal attack signal detection in optical fiber communication network, on the one hand, can query the source of abnormal signal, and accurately locate the location of abnormal signal. On the other hand, by extracting the corresponding information, the system can combine all kinds of application nodes to achieve internal resource sharing, and then improve the overall system operation efficiency.

3. Iterative detection simulation of abnormal attack characteristics in optical fiber communication network

In the iterative detection of abnormal attack characteristics in optical fiber communication networks, it is necessary to collect the corresponding OTDR curves after the optical network is passed through. Then, the curves are analyzed to determine whether the bending and fracture of the whole optical fiber exists. In order to detect the abnormal attack signal of optical fiber communication network accurately, it is necessary to filter the internal noise of the system effectively and obtain the effective signal. Therefore, in this process, the data in OTDR curve need to be processed by wavelet transform. Then, using the trend of wavelet transform, we can get any details of the signal. According to the change of different details, some weak and abnormal signals are processed to eliminate the abnormal attack signals in the optical fiber communication network. Therefore, this method can iteratively detect abnormal attack characteristics in optical fiber communication networks. The specific iteration detection methods are as follows:

First, Set OTDR curve signal as $f(x)$,The wavelet transform coefficients corresponding to signal scale j are $W_i f(t)$. The product of wavelet transform coefficients on scale j and adjacent scale $j+1$ is $D(j,t)$. According to the corresponding representative variables, the following formulas can be obtained:

$$D(j,t) = \mathrm{sgn}(W_i f(t))\left|W_i f(t) W_{j+1} f(t)\right|$$

According to the characteristic coefficients of abnormal signals in different optical fiber communication networks, more obvious detection methods are needed for some cross-scale signal features. Therefore, in order to make the cross-scale anomalous attack signal more obvious, we need to multiply the corresponding coefficient k in the above formula, and then get the following formula:

$$D(j,t) = \mathrm{sgn}(W_j f(t)k)\left|W_i f(t) W_{j+1} f(t)\right|$$

By calculating the above formulas, it is found that the calculation results can effectively increase the range of the wavelet values on the corresponding scales. However, the corresponding energy criteria can not be effectively met in the actual iterative detection process of abnormal attack characteristics in optical fiber communication networks. Therefore, the corresponding coefficients need to be treated as follows:

First, By calculating the energy $E_j = \sum (W_j f(t))^2$ of wavelet coefficients on different scales. At the same time, it is necessary to calculate the energy of the product of the wavelet coefficients of the corresponding scale and the adjacent scale. The specific formula is $E_D = \sum_x (D(j,t))^2$.

Second, The ratio of energy E_j to energy E_D is obtained by a certain calculation process, and the specific formula is expressed as $r_E = \sqrt{E_j / E_D}$.

Third, By multiplying $D(j,t)$ and r_E, the corresponding wavelet coefficients, namely $W_j^* f(t)$, can be obtained.

Through the data processing and calculation of the above three steps, the energy of the enhanced optical fiber communication signal in the wavelet domain can be kept unchanged in a certain range. Moreover, according to the calculation results, processing the related nodes in the system can effectively eliminate the system noise, obtain the abnormal attack signal in the optical fiber communication network, and then determine the corresponding OTDR curve. Finally, on the basis of OTDR curve, signal recognition and processing are carried out inside the system to maximize the reduction of abnormal attack signals in optical fiber communication networks. Or with the help of the corresponding degree of operation, the system can weaken and eliminate signals, exclude some bad signals, and then ensure the good operation of the system, improve the quality and efficiency of optical fiber communication network operation.

References

[1] Huang Y., Wang Y., Liu Z.l.(2014). Simulation and Analysis of Breakpoint Detection Model for Large Optical Fiber Communication Network, Computer simulation, 31 (11),183-186.

[2] Yang H.(2012). An All-Optical Network Attack Detection Using Optical Fiber Sensors, Optical Communication Technology, 36 (7),22-24.

[3] Zhou Y.J., Jiao C.B., Chen H.N, et al.(2013). Traffic behavior characteristics DOS & DDoS attack detection and abnormal flow identification, Computer Applications, 33 (10),2838-2841.

[4] He Y., Xie L.S.(2018). The optimal laser sensor node selection after the fiber optic communication network is invaded, Laser Magazine, 39 (4), 129-133.

[5] Li Y.Y, He Y.(2014). Simulation of Optimal Fault Diagnosis Method in Optical Fiber Communication Network, Computer simulation, 31 (9),221-224.

[6] Wang Z. H.(2019). Analysis and Maintenance of Optical Transmission Technology in Optical Fiber Communication System, Computer Knowledge and Technology, 15 (12),47-48.