Simulation Research on Iterative Detection of Abnormal Attack Characteristics in Optical Fiber Communication Network

Fan Yu

Jiangsu Open University, Nanjing, Jiangsu, 210000, China

Keywords: Optical Fiber, Communication Network, Iterative Detection, Anomaly Attack, Simulation Research

Abstract: as an Important Communication Tool for Social Production and Life, Optical Fiber Communication Network is Conducive to the Further Development of Society. However, Due to Network Anomaly Attacks, Communication Tools Will Be Paralyzed, and Then Unable to Work. in This Context, It is of Great Significance to Explore the Specific Ways of Abnormal Attacks in Optical Fiber Communication Networks and to Provide Detection Methods. Therefore, This Paper First Analyses Two Ways of Anomaly Attack in Optical Fiber Communication Network, and Then Discusses the Iterative Detection Process and Simulation Scheme of Anomaly Attack in Optical Fiber Communication. the Results Show That the Iterative Detection Algorithm Has a Good Effect, and Has a Good Application Prospect in Real Life.

1. Introduction

1.1 Literature Review

At Present, the Accurate Detection of Optical Fiber Network in Network Security is Conducive to Maintaining the Normal Operation of Communication Facilities and Equipment, Thus Playing an Important Role in Social Life. At Present, Large-Scale Optical Fiber Communication Network Nodes Have Randomness and Scattered Distribution, Such as the Occurrence of Random Breakpoints Will Not Affect the Normal Network Communication (he and Xie, 2018). Traditional Autonomous Induction Analysis Method is Difficult to Realize the Optimization and Perfection of Network Communication through Node Judgment. Accordingly, Many Studies Have Been Carried out in Detail. Some Scholars Have Pointed out That a Breakpoint Detection Model Based on Neural Network for Optical Fiber Communication Network Can Be Trained to Analyze the Specific Breakpoints of Optical Fiber Communication Network (Zhang et al, 2014). At the Same Time, the Neural Network Detector is Constructed According to the Principle of Immune Recognition, and the Storage Content is Distributed in the Detector. When Abnormal Phenomena Occur in Optical Fiber Communication Network, the Detector is Activated by Sample Matching. the Author Also Finds That the Breakpoint Detection Model of Optical Fiber Communication Network Can Accurately Detect Breakpoints and Has High Detection Efficiency (Cai, 2019). Some Scholars Have Proposed a New Distributed Network Anomaly Attack Detection Method for the Vulnerability of Anomaly Attack Detection Methods. It is Found That Abnormal Data Can Be Classified Normally by Iterative Clustering of Data in Distributed Network, and Particle Density Function Can Be Established in Matrix by Preliminary Comparison of Abnormal Data (Zhao, 2016). Finally, the Authors Weighted the Validation Data and Found That the Optimized Distributed Network Anomaly Attack Detection Can Accurately Detect the Attacking Anomaly Data in the Case of Interference, and Has Stability (Zheng, 2017). Some Scholars Have Carried out in-Depth Research and Found That the Selection of the Optimal Laser Sensor Node Can Continuously Improve the Security of Optical Fiber Communication. However, the Traditional Selection Technology Can Not Distinguish the Advantages and Disadvantages of Laser Sensors, Which Makes It Difficult to Solve the Security Problems (Geng, et al, 2017). Sensor Splitting in Database Network Nodes Based on Ip Address and Pi Value Can Achieve Optimal Performance. in This Case, the Optimal Laser Sensor Node is Dynamically Identified after the Network Communication of

  DOI: 10.25236/ISMHI.2019.086

Optical Fiber Communication is Attacked. Compared with the Traditional Node Selection Method, the Scheme Proposed by the Author Can Help to Reduce the Error of Network Attack Identification and Improve the Recognition Rate Continuously.

1.2 Purposes of Research

Network security has always been the focus of attention. In the current optical fiber communication network, it is often attacked by abnormal signals, which interferes with the network communication and has a negative impact on social production and life. In the research of fault diagnosis of optical fiber communication networks, it is necessary to detect the breakpoints of optical fiber faults and the characteristics of abnormal attacks in time. However, signal attenuation will occur to a large extent in long-distance optical fiber communication, and abnormal attack signal will change greatly, which will cause the distortion of fault signal curve. With the rapid spread of Internet information, the Internet has become an important tool of social production. However, with the devastating activities such as abnormal attacks and virus intrusion, it has brought great negative impact on people's Internet life. Network security has become the focus of people's attention. How to reduce the breakpoints caused by abnormal attacks in optical fiber communication networks and to detect them iteratively are the key issues to be studied. In view of this, this paper analyses the characteristics of abnormal attacks in optical fiber communication network in detail, as well as the specific detection scheme and simulation, in order to provide useful reference for more scientific development.

2. Abnormal Attacks in Optical Fiber Communication Networks

The security of optical network has a direct impact on the performance of communication network. The operation of network services will fluctuate due to the changes of optical network. Relevant research shows that the traditional communication network has the security problem of network attack, and it also exists in optical network. As an important medium of communication transmission, optical fiber has high security. But because the optical signal can also be eavesdropped by various devices, it will also be attacked abnormally. Generally speaking, there are several kinds of abnormal attacks in optical fiber communication networks.

2.1 Denial of Service Attack

Disk Operating System (DOS) aims to make the communication network unable to work properly, which is extremely harmful. In all-optical networks, although the transmission of optical signals in optical fibers is more disturbed than that in traditional media, it is inevitably damaged (Chang, 2018). In this case, injecting noise into the optical fiber can effectively prevent service attacks. At the same time, if the optical fiber encounters play, then there will be a certain loss in the optical fiber, and then there will be network interruption. In specific attacks, four-wave mixing can produce crosstalk and lead to distortion of attack signal. Erbium-doped fiber amplifier can also effectively prevent attacks by amplifying optical signals. Therefore, the fraudulent signal with energy amplitude greater than the normal signal is injected into the optical fiber, which can weaken the normal signal and amplify the attack signal (Wan, et al, 2015). At this time, the normal signal in an amplifier produces abnormal response, which makes the whole network system unable to operate normally.

2.2 Wiretapping Attack

There is no electromagnetic radiation in all-optical network. It is difficult to wiretap by traditional electromagnetic induction. But at the same time, because distance transmission is the biggest weakness of optical fiber, if the transmission distance exceeds the optical fiber transmission distance, then we need to use certain equipment to amplify the optical signal. The process of signal amplification and replication follows the principle of “optical signal electrical signal optical signal”. If the attacker monitors the components, he will get the transmission signal and attack the whole network. At the same time, very small signals will be recovered after theft, so such attacks are

difficult to prevent.

3. Iterative Detection Process and Simulation of Abnormal Attack Based on Optical Fiber Communication

3.1 Iterative Detection Process

By analyzing all kinds of abnormal subgraph patterns in optical fiber communication network graph, the abnormal attack behavior of abnormal network is identified. Aiming at this kind of abnormal attack, we need to adopt the iterative detection scheme further. The specific flow chart is shown in Figure 1.

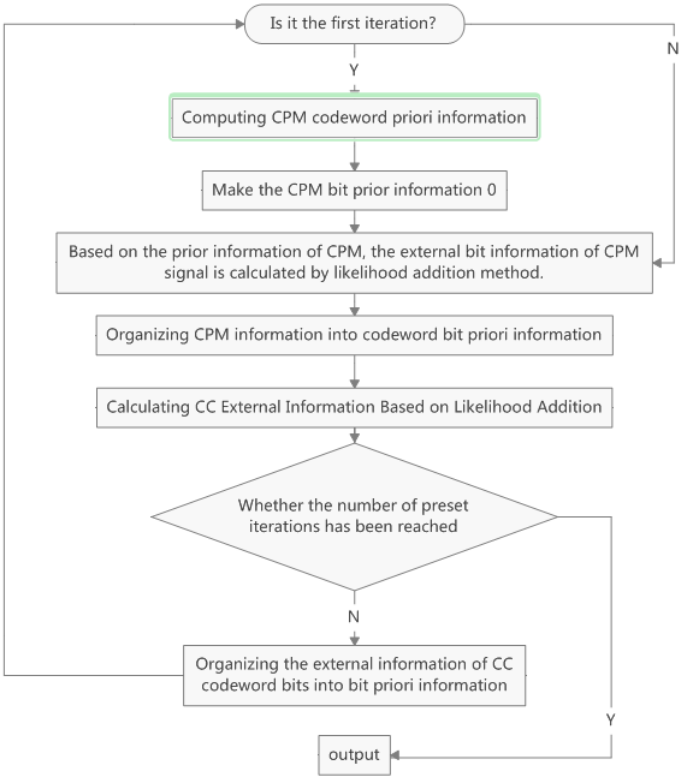

Fig.1 Iterative Detection Scheme

Step1: Check whether the first iteration of abnormal attack in optical fiber communication network is carried out.

Step2: Answer “Yes”, go to the next step, and calculate the CPM codeword priori information. If the answer is no, then go directly to the fourth step.

Step3: Another CPM bit prior information is “0”.

Step4: At this time, according to the prior information of CPM, the external bit information of CPM signal is calculated by likelihood method.

Step5: Organize CPM information into codeword bit priori information.

Step6: Calculate CC external information based on likelihood addition.

Step7: Determine whether the number of iterations reached the preset number, the answer is “yes”, then output the test results directly. The answer is “no”, then the external information of CC codeword bits is organized into the prior information of the bits, and then start from the first step.

Although the security of all-optical networks is many times higher than that of traditional networks, there is still a risk of attack. Therefore, it is necessary to use optical fiber sensors for monitoring. At the same time, as a sensing cut-off, optical fiber can enhance the optical signal adjustment of transmission cut-off, and then enhance the judgment of optical signal. In addition, when an attacker attacks the all-optical network, the optical signal will be changed. In order to use iterative detection algorithm to get the abnormal attack of optical fiber communication network, it is

necessary to judge whether the network is attacked or not according to the change of optical power. If we use optical fiber sensor to detect, we need to judge whether the communication network is attacked, otherwise, it will improve the resistance of the attack.

When using iterative algorithm to test this time, we need to do it from two aspects. One is based on bandwidth power detection. This scheme mainly detects the changes of optical signals received in broadband optical broadband networks. In view of the change between the calculated received signal power and the expected received optical signal power, more time needs to be extended. Therefore, in terms of receiving power, the attacker can not extract detailed information accordingly, even if the power is very slight, it is difficult to determine the attacked. The second is the detection of spectral analysis. When using spectrum analyzer, optical signal of optical fiber communication network needs to be measured. In this case, we can determine whether the communication network is attacked mainly by detecting whether the bandwidth power can bring more narcissism and whether the network is in normal or not. It should be noted that spectral analyzer can detect more information, but usually requires some average parameters, which leads to more attacks on the detection network.

3.2 Simulation and Implementation

According to the calculation flow of the above iteration algorithm, the maximum concurrent user of abnormal attack in optical fiber communication network should be taken as the input value of the iteration algorithm. On this basis, the dichotomy method is used to iteratively test the current optical fiber communication network. The specific test algorithm is as follows.

STEP1: The parameters of the iteration algorithm are initialized and calculated in detail as follows.

$UMax = UserMax = 50$; $UMin = UserTest = UMax / 2 = 25$

$UMax = UserMax = 50$

$UMin = UserTest = UMax / 2 = 25$

STEP2: The system monitoring performance should be added to the $UserTest$ test.

STEP3: If there are no abnormalities in the three key parameters of the system, there will be $UserTest = (UserTest + UMax) / 2$, which extends downward.

STEP4: However, if one anomaly is found in three key parameters of the system, there will be $UserTest = (UserTest + UMin) / 2$, and the range of values will extend downward.

STEP5: Repeat the above iteration algorithm until the critical value of abnormal parameters in optical fiber communication network is less than 2, from which the maximum concurrent users can be obtained. At the same time, the maximum number of concurrent users that the system can carry is 36, which is calculated by using $UserMa = 50$ as iteration.

4. Conclusion

Through the above algorithm, we can see that the iterative algorithm adopted in this paper can detect the abnormal attack characteristic risk of optical fiber communication network, and achieve good results. Therefore, in the network environment, the abnormal attack of optical fiber communication network needs to be analyzed by iterative algorithm, in order to get the specific value, and then give the specific application program.

References

[1] He Y., Xie L.X. (2018). Optimal Choice of Laser Sensor Nodes after The Optical Fiber Communication Network Is Invaded. Laser Magazine, 39 (4): 129-133.

[2] Zhang Y.F., Ren S., Wang P, et al. (2014). Research Progress on the Impact of High-Power Signals on Optical Networks and Protection Technology. Progress in Laser and Optoelectronics, 51 (10): 21-29.

[3] Cai X. (2019). Research on the Present Situation and Defensive Measures of Power Network Security Management. Network Security Technology and Application, 218(2): 83+87.

[4] Zhao Y.P. (2016). A Security Analysis Model of Large-Scale Optical Fiber Communication Network Based on Pattern Recognition. Journal of Inner Mongolia Normal University (Natural Chinese Edition), 45 (4): 497-499.

[5] Zheng G.C. (2017). Design of Purification Method for Intrusion Signals in Optical Fiber Communication Network under Wave State.Laser Magazine, 38 (12): 146-149.

[6] Geng J.C., Zang M., Shang C.Z., et al. (2017). Methods and Defense Measures of Optical Fiber Communication Network Eavesdropping. Information Recording Materials, 18 (8): 101-102.

[7] Chang J. (2018). Research on the Current Situation and Key Technologies of Network Security Defense in the Era of “Internet+Internet”. Network Security Technology and Application, 215 (11): 9+29.

[8] Wan B.W., Gan H.H., Dong X.M. (2015). 802.1x Port Authentication Defects and Improvements. Optical Communication Research, 41 (1): 23-25.