Crosstalk Attack Location Algorithm Based on Gray Theory
Fang Li*, Qi-wu Wu, Hao Chen and Yang Zhou
Engineering University of PAP, Xi’an, 710086, P. R. China
*Corresponding author

Keywords: Optical network, Gray theory, High-power signal, Crosstalk attack.

Abstract. The characteristics of the three kinds of attacks, such as the intra-channel crosstalk attack, the inter-channel crosstalk attack and the gain competition, which affect the optical network, and the characteristics of the gray theory are analyzed. A crosstalk attack location algorithm based on gray theory is proposed, the algorithm is verified by the known partial attack information, and the location of the attack source is determined according to the characteristics of the high-power attack. The simulation results show that this algorithm can locate the attack source accurately when the attack information is incomplete.

Introduction
With the rapid increase from internet users, and the emergence of a variety of network applications, having a large capacity, high speed, flexibility and scalability of the optical network satisfies a growing demand for network transmission, while the transparency of optical networks makes it more vulnerable attack of high-power signal for service destruction [1]. As the amount of traffic carried by the optical network is increasing day by day, even if the destruction time is short, a large amount of information will also be lost. Under such circumstances, whether the attack source can be located at a relatively short time can be the key issue to be solved urgently.

In recent years, many scholars at home and abroad have studied the attack location method and algorithm in optical network. Foreign countries such as the literature [2, 3] on the all-optical network fault and attack management were studied, mainly on the difference between failure and attack analysis and monitoring based on the consideration of localization; the domestic literature [4, 5], etc. mainly use the distributed positioning algorithm or two-parameter comparison algorithm. There are two major problems in the above research: First, there is no single, serious and careful study of high-power crosstalk attacks. Second, the method used can not be cost-effective and accurate positioning of the source of the attack.

At present, new security features in optical network has many unique features, which due to the transparency of the optical network makes high-power optical crosstalk resulting network service disruption attacks can spread rapidly through the network, causing additional problems and trigger more alerts, you must pinpoint the source of their attacks at any point in the network that may occur. On the basis of analyzing the characteristics of gray theory, this paper proposes a crosstalk attack location algorithm based on gray theory. Experiments on VPI simulation platform show that the algorithm can locate the source attack accurately when the attack information is incomplete.

Related Basics

Gray Theory
Gray theory [6] was founded by Professor Deng Ju-long, a Chinese scholar in 1982. It is a new method to study the problem of few data, poor information and uncertainty. Based on the small sample of "some information is known and some of the information is unknown", "poor information" as the research object. By generating, developing and extracting valuable information about the "part" of the known information, the correct description and effective monitoring of the operating behavior and evolution law of the system can be realized. This is very similar to the research on the indeterminate attack points of high-power crosstalk attack in optical networks and
the complexity of attack information caused by attack propagation. Therefore, the gray theory can be used to study the high-power crosstalk attacks.

**Intra-channel Crosstalk Attack**

Intra-channel crosstalk attack is due to the same wavelength high-power attack signal with the user signal into the optical switch, the optical switching device manufacturing technology is not mature enough, the power leakage of the high-power attack signal affects the normal transmission of its adjacent user signals. It mainly occurs at the optical cross connector (OXC), and the core unit that forms the OXC is a plurality of optical switch modules, which have two forms of parallel connection and cross connection.

**Inter-channel Crosstalk Attack**

Inter-channel crosstalk attack is caused by the interaction and crosstalk between high-power attack signals of different wavelengths and user signals at the optical fiber. Because optical networks are formed by optical fibers, during their long-distance, high-speed and large-capacity transmission of information, there will be optical fiber self-phase modulation, cross-phase modulation and four-wave mixing and other nonlinear characteristics, these are the root cause of out-of-band crosstalk.

**Gain Competition**

In optical networks, the role of optical amplifier is mainly to compensate for the optical signal energy consumed in the transmission process, it is a very important relay device. When the high-power attack signal and the normal user signal enter the same optical amplifier, the attack signal will "plunder" the gain of the user signal, because the power value of the attack signal is much larger than that of the user signal, and the gain obtained increases according to the larger-power wavelength signal, which belongs to the user signal gain is weakened, the impact on the user, this is the gain competition.

![Figure 1. A schematic diagram of the impact of high-power crosstalk attacks on Optical Networks.](image-url)

**Attack Location Algorithm**

In optical networks, the three main types of attack are intra-channel crosstalk, inter-channel and gain contention [7], the "place of occurrence" and the impact on the normal user when it occurs are the external symptoms "Symptoms" show.
From the table above, we already know the main places and symptoms of high-power crosstalk attacks. In optical network, if a high-power crosstalk attack occurs and can not be located in time, the performance of the optical network will be greatly affected, and the service quality of normal communication will be greatly reduced or even unavailable. In order to ensure the normal communication, this paper proposes a crosstalk attack location algorithm based on gray theory.

**Algorithm Ideas**

The purpose of this algorithm is to determine the location of the attack source and the location of the node where the attack source is located by using the alarm information sent by the ONMS. Based on the intra-channel crosstalk attack, inter-channel crosstalk attack and gain competition in the optical network, the locations and symptoms of these weakly known attack information, the attack scene and the attack model are used to analyze the attack location algorithm.

In this paper, OXC as the node model and optical fiber and gain amplifier as secondary nodes are mainly studied. Tx1 to Tx7 are the seven incoming user signals, OXC1 to OXC7 are seven optical cross-connect connectors, F1 to F5 are five optical fibers, EDFA1 is an optical amplifier, and SA1 to SA7 are seven check points as shown in Figure 2.

In Figure 2, we set the attack signals at the input A1 of the OXC1 and the input A2 of the OXC7 to inject high-power attack signals. Through the information transmission, the attacks propagate along the optical path, and the attack alarms are found and located at SA3.

**Algorithm Implementation Method**

When alarm information is sent out at SA3, two optical paths entering OXC6 are detected.

(1) The node EDFA1 and the node OXC7 are both found to have attack conditions, and the optical paths entering the nodes EDFA1 and OXC7 continue to be detected.

(2) If the eye pattern in SA7 is found to be less affected, then the source attack is not caused by Tx6, and Tx7 is a source attack input.

(3) Through the SA6 test, we found that the eye diagram is clearer, indicating that the attack is not caused by Tx5, and the node OXC5 is ruled out as the source attack node.
(4) Through the detection of SA5, node OXC3 can be ruled out as the source attack node.
(5) By SA1 and SA2 detection, it was found that the eye of SA1 obviously suffered severe attack, while SA2 had little effect, indicating that the source attack node is from Tx2.

In this attack scenario and attack model, we see how the algorithm based on gray theory locates the source attack node using a small amount of attack alert information. The alarm information sent by SA3 finally finds out that the source attack nodes are Tx2 and Tx7.

**Simulation Experiments and Analysis**

**Simulation Experimental Chart and Parameter Settings**

In the VPI simulation platform, set up the above-mentioned optical network location algorithm simulation experiment, as shown in Figure 3. The experimental transmission frequency was 193.1 THz, 193.2THz, the frequency interval of 100GHz, the signal transmission power of 50mW, the attack signal power is set to 500mW.

![Simulation Experimental Chart](image)

Figure 3. Source attack point positioning experiment simulation.

The basic parameters set as shown in Table 2.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Numerical values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit-rate Default</td>
<td>10GHz</td>
</tr>
<tr>
<td>Time Window</td>
<td>64/10e9s</td>
</tr>
<tr>
<td>Sample Rate Default</td>
<td>160e9bit/s</td>
</tr>
<tr>
<td>Attenuation</td>
<td>0.2e-3dB/m</td>
</tr>
<tr>
<td>Dispersion</td>
<td>2.0e-9s/m2</td>
</tr>
<tr>
<td>Dispersion Slope</td>
<td>0.08e3s/m3</td>
</tr>
<tr>
<td>Nonlinear Index</td>
<td>2.5e-20m2/w</td>
</tr>
</tbody>
</table>

**Experimental Results and Analysis**

According to the analysis of the positioning algorithm and the analysis of the VPI simulation platform, the results are shown in Figure 4.

![Experimental Results](image)

(a) SA1

(b) SA2
As can be seen from the various eye diagrams in FIG. 3, SA3 and SA4 are the locations where the attack is more serious and the location where the alarm information is sent. SA5, SA6, and SA7 are the detected locations of the attacked nodes that are suspected of being attacked. The quality of eye patterns can be used to prove that the source attack nodes are not from OXC3 and OXC5. The eye diagram of SA1 can be seen to be affected because it is sent with the source attack Tx2 enters OXC1 together, an intra-channel crosstalk attack occurs, and SA2 has better eye quality because it is the source of the attack on Tx2 itself and is unaffected by a larger attack.

Summary and Outlook

By analyzing the characteristics of high-power attack signals and combining with the gray theory, this paper proposes a crosstalk attack location algorithm based on the gray theory. After the ONMS sends out the detection information, it can use fewer, known partial attack information pairs crosstalk attack source for accurate positioning, and VPI simulation platform experiments, the algorithm was verified. With the increase of the carrying capacity of optical network, its structure is more and more complicated. This algorithm has certain reference value for the location of crosstalk attack in the more complicated optical network in the future.

Acknowledgement

We gratefully acknowledge anonymous reviewers who read drafts and made many helpful suggestions. This work is supported by the National Science Foundation Project of P. R. China (No.61402529); the Natural Science Basic Research Plan in Shanxi Province of China (No.2015JQ6266); the Basic Research Foundation of Armed Police Engineering University (No.WJY201417, No.JLX201645).
References


