A crosstalk attack detection and location method based on distributed PCE in multi-domain optical networks

Qiwu Wu 1*, Fang Li 2, Lingzhi Jiang 2, Xueyue Liu 2 and Long Zhang 3

1 School of Equipment Management and Support, Engineering University of PAP, Xi’an, 710086, China
2 School of Information Engineering, Engineering University of PAP, Xi’an, 710086, China
3 School of Information and Electrical Engineering, Hebei University of Engineering, Handan, 056038, Hebei Province, China

*Corresponding author’s e-mail: wuqiwu700@163.com

Abstract. Aiming at the uncertainty problem of crosstalk attack detection and attack source localization in multi-domain optical networks, a new crosstalk attack detection and location method in multi-domain optical networks is proposed by using distributed PCE architecture and monitoring point placement strategy based on grey theory. Meanwhile, an example is given. The experimental results show that the proposed method is effective.

1. Introduction

At present, optical network undertakes the task of backbone transmission. Due to the transparent transmission of optical network, the crosstalk attack caused by the high-power signal injected by malicious users on the normal legitimate signal has a relatively large impact on the optical networks. In band crosstalk, out of band crosstalk and gain competition are three kinds of high-power crosstalk attacks in optical network, which seriously threaten the normal operation of optical network. Hence, how to detect and accurately locate cross-domain attacks in multi-domain optical networks in real time has become a major issue that needs to be resolved [1].

In terms of crosstalk attack detection in multi-domain optical networks, by using the method of parameter comparison and integrated monitor detection, a detection method of crosstalk attack and fiber breakage was proposed in reference [2]. However, the research on this method is not deep enough. Literature [3] proposed a new attack detection method in distributed network anomaly, but it is not suitable for the detection of cross-talk attacks in multi-domain optical networks. Literature [4] pointed out that monitoring equipment plays an important role in detecting and reporting the impact of attacks in optical networks, but considering the technical limitations, it costs more to equip monitoring equipment in each node. In reference [5], an attack detection method based on the combination of distributed BP neural network and genetic algorithm was proposed. However, this method needs to input small sample data into the detection model for detection, which has complex algorithm and low efficiency.

In the area of crosstalk attack location in multi-domain optical network, literature [6] proposed an effective monitoring routing strategy and developed a feasible routing algorithm. However, these strategies and algorithms are only applicable to networks with no more than one attack. Literature [7]
analyzed two attack location methods based on model and black box, and proposed an end-to-end optical channel attack location solution, but this solution is not suitable for the location of multipoint crosstalk attacks. Literature [8] proposed a fast location solution, which realizes the efficient location of multi-link faults in multi-domain optical networks, but it is also not applicable to the field of multipoint crosstalk attacks. Literature [9] proposed an in-band crosstalk attack location algorithm based on two-parameter comparison. The algorithm achieved the goal of more accurately locating the attack source by observing the two parameters of optical signal-to-noise ratio and power. But the algorithm does not consider the multi-domain characteristics of the network. In literature [10], a multi-crosstalk attack source identification algorithm was proposed to successfully identify the crosstalk attack sources existing in three different network type, but the algorithm needs to be further optimized in terms of comprehensive performance.

In the multi-domain optical network of distributed PCE, each domain has a PCE responsible for the topology of nodes in the domain and the path calculation within and between domains. Grey theory is an applied mathematics subject which studies the uncertainty phenomenon of some clear and some unclear information. In this paper, the grey theory is applied to detect and locate the uncertainty of crosstalk attack point. Hence, this paper will propose a new crosstalk attack detection and location method based on distributed PCE the multi domain optical network, by using the grey theory strategies.

2. Problem description

Definition 1: Define a multi-domain optical network topology as $G(V, E), V = \{V_1, \cdots, V_n\}$ is a collection of all the nodes in the network. The link between node $V_i$ and node $V_j$ is expressed as $e_{ij}$, $E = \{e_{ij} | 1 \leq i, j \leq n\}$ is a collection of links in the network. The set of monitoring points is $M$. At the same time, the number of nodes and links in the network is stable.

Definition 2: There are $q$ PCEs in $G$, which is $Q = \{PCE_1, PCE_2, \cdots, PCE_q\}$. A total of $p$ wavelengths is randomly distributed throughout the network. At the same time, it is assumed that each node has no wavelength conversion capability and the wavelengths on the same optical path are the same.

Definition 3: In order to achieve the purpose of real-time detection, the constant terms $a$ and $b$ in the original grey theoretical model are expanded into functions $a(t)$ and $b(t)$, and then formula (1) is obtained:

\[ X^{(i)}(t+1) = X^{(i)}(1) - \frac{b}{a} e^{-a} + \frac{b}{a} \] (1)

Formula (1) can be written as formula (2):

\[ X^{(i)}(t+1) = C_1 e^{(a)} + C_2 \] (2)

Use the sum of the linear regression equation and the exponential equation to fit and accumulate the formula (2) to obtain the formula (3). The parameter $C_1, C_2, C_3$ are constants.

\[ X^{(i)}(t) = C_1 e^{(a)} + C_2 t + C_3 \] (3)

Definition 4: In order to optimize the GMPS value of crosstalk attack detection, this paper defines the parameter $z$ in formula (3) as $(n-3) + (n-4) + \cdots + 2 + 1 = (n-2)(n-3)/2$. Take the average value $d$ of these $z$ as the estimated value $\hat{z}$ of $z$. That is formula (4):

\[ \hat{z} = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} z_{ij}(t)}{(n-2)(n-3)/2} \] (4)
3. Crosstalk attack detection and location method

3.1 Crosstalk attack detection

The crosstalk attack detection includes data collection module, data analysis module and monitoring-point placement strategy based on grey theory (referred to as GMPS) module.

3.1.1 Data collection

The data collection module submits the collected crosstalk attack data to the data analysis module for processing. Crosstalk attack data includes power, spectrum, waveform, and BER during information transmission. In this paper, the node where the monitoring device is placed is called the monitoring node, and the node without the monitoring device is called the non-monitoring node.

3.1.2 Data analysis module

The data analysis module classifies and sorts the data collected by the data collection module. Among them, the optical spectrum analyser OSA can achieve the purpose of detecting and locating crosstalk attacks by comprehensively analysing the spectrum diagram, waveform diagram and eye diagram of the monitoring signal. At the same time, a BER monitor can also be used. This paper uses two monitoring devices, optical power meter and OSA, to jointly monitor crosstalk attacks.

![Crosstalk attack monitoring model](image)

Figure 1. Crosstalk attack monitoring model

Figure 1 is a crosstalk attack monitoring model using the OXC node as an example. When two or more signals are exchanged through OXC, and then through the optical power combiner, they are finally sent to two monitoring devices, optical power meter and OSA, for signal detection. For the optical power meter, it is mainly used to detect the wavelength signal whose attack power exceeds 20dB. For OSA, it is mainly to use the eye pattern to determine the signal attack. The eye diagram can sample and monitor a single wavelength optical channel, and the eye diagram monitored in an ideal linear channel is symmetrical.

3.1.3 GMPS module

The GMPS module is based on the data collected by the data collection and data analysis modules. It takes advantage of the small amount of data required for grey modelling and uses time series data to monitor and detect the entire multi-domain optical network. In order to realize the function of the GMPS module based on the grey theory and achieve the purpose of using the least number of monitoring devices for crosstalk attack detection, the specific operation steps are as follows:

Step1: In a multi-domain optical network \( G(V, E) \), find the domain where the crosstalk attack source node \( s \) and destination node \( d \) are located, and apply Dijkstra algorithm to obtain the path set \( \Omega_s \subseteq \{s,d\} \).

Step2: For the \( n \) nodes in the path set \( \Omega_s \), after passing through the data collection and analysis module, attack feature extraction is performed, and the resulting sequence is as follows:

\[
\mathbf{x}^{(0)} = (x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(n))
\]

After iterating equation (5) once, we get:

\[
\mathbf{x}^{(1)} = (x^{(0)}(1), x^{(1)}(2), \ldots, x^{(0)}(n)), \quad x^{(0)}(k) = \sum_{i=1}^{k} x^{(0)}(i)
\]

Step3: After the attack signature sequence is obtained, the PCE of each domain counts the Traffic Engineering(TE) information in its domain, and summarizes the path set \( \Omega_s \) and wavelength and other information into the Traffic Engineering Database(TED).
Step 4: Statistics on the data in TED, combined with formula (3) and formula (4), get the characteristic power value of a node, and set the node as the monitoring node.

Step 5: Count the number of boundary nodes $|\mu|$ that interact frequently with neighbourhood information in TED, and combine Step 4 to obtain the minimum value of the monitoring points required by the multi-domain optical network as $\min |\mu| + |\mu|$.

3.2 Crosstalk attack location
Crosstalk attack location is based on the realization of real-time detection of multi-domain optical network crosstalk attacks, on the premise of collecting the alarm information of each channel, and using distributed location methods.

Assuming that a node in the network is the node that sends the alarm information, the alarm state parameter of the node is set to $A$. When $A = 1$, the node sends an alarm message; when $A = 0$, the node does not send an alarm message. At the same time, suppose the security state parameter of a node in the network is $B$. When $B = 1$, the node is subjected to crosstalk attack; when $B = 0$, the node is not subjected to crosstalk attack. Among them, the upstream node security state parameter of node $B$ is $B'$, and the upstream node security state parameter of node $B'$ is $B^*$. The specific location steps are as follows:

Step 1: When a crosstalk attack is detected, an alarm message is generated, and the PCE collects the alarm message through the control plane.

Step 2: If $A = 1$ is found, the upstream node $B$ that entered the node is detected; otherwise, the node does not issue an alarm message, and node $B$ does not need to be detected.

Step 3: In the process of detecting node $B$, if $B = 1$, the upstream node $B'$ of $B$ is detected, otherwise, node $B$ is not subject to crosstalk attacks.

Step 4: When $B' = 1$, if $B'$ has an upstream node, then the upstream node $B^*$ of $B'$ is detected, otherwise, node $B$ is the source attack node.

Step 5: When the security state parameter $B^* = 1$, then $B^*$ is the source attack node; otherwise, node $B'$ is the source attack node.

4. An example of the proposed method
This paper takes OXC as the main node of crosstalk attack, and fibre and gain amplifier as the secondary nodes of crosstalk attack. Determine that Tx1 ~ Tx7 are input user signals, OXC1 ~ OXC7 are the main attack nodes, F1 ~ F5 and EDFA1 are the secondary attack nodes, and SA1 ~ SA7 are the detection points, as shown in Figure 2. In this paper, high-power crosstalk attack signals are injected into A1 of signal input terminal Tx2 and A2 of signal input terminal Tx7. The specific crosstalk attack source location steps are as follows:

Figure 2. Crosstalk attack source location map
Step 1: When an alarm message is issued at SA3, the two optical paths entering OXC6 are detected.
Step2: It is found that there is a condition of crosstalk attack between the node EDFA₁ and the node OXC₇, and then the optical paths entering the node EDFA₁ and the node OXC₇ are detected.

Step3: It is found that the eye diagram at SA₇ is less affected, indicating that the source attack is not caused by Tx₆, and Tx₇ is the input end of a source attack.

Step4: Through the detection of SA₆, it is found that its eye diagram is relatively clear, indicating that the attack was not caused by Tx₅, and at the same time ruled out that the node OXC₅ is the source of the attack node.

Step5: Through the detection of SA₅, the suspicion that node OXC₃ is the source attack node can be excluded.

Step6: Through the detection of SA₁ and SA₂, it is found that SA₂ is more affected than SA₁, It means that Tx₂ is the input of another source attack.

Through the above analysis, it can be seen that the alarm information sent by SA₃, after monitoring and detection and distributed location methods, finally found that the input terminals of the crosstalk attack source are Tx₂ and Tx₇, which are consistent with the original settings of this article. Therefore, this method can achieve the goal of accurately locating the source of crosstalk attacks.

5. Simulation

5.1 Network structure and parameter settings
This paper uses VPI optical network simulation software to verify the effectiveness of crosstalk attack detection and location method. The simulation experiment uses the network structure as shown in Figure 3. The attacker uses a high-power signal with frequency $f_1$ to inject attack signals at @ 1 and @ 2 in the D1 and D3 domains. The injected attack signal propagates along optical fiber, EDFA, demultiplexer and OXC. Among them, in-band crosstalk is caused in OXC, out of band crosstalk is caused in optical fiber, and gain competition is caused in EDFA.

![Figure 3. Experimental simulation diagram](image)

5.2 Experiment analysis
According to the experimental setup, this paper focuses on the detection capabilities of d₁, d₂, d₄ and d₅ monitoring points.

(a) OSA diagram of d₁  
(b) eye diagram of d₁
From Figure 4, we can see that the crosstalk attacks with different power can be detected at d1, d2, d4 and d5 monitoring points. From the eye diagrams obtained from each monitoring point, we can see that the crosstalk attacks detected at d1 and d5 are more serious, because they are on the main path of the crosstalk attack source propagating in the multi-domain optical network. Compared with d1 and d5, the crosstalk attack detected at d4 is lighter, but more serious than d2, because it is affected by the accumulation of attack power of oxc8 and oxc14. The attack detected at d2 is relatively light.

6. Conclusions
In view of the uncertainty of detection and location of crosstalk attack sources in multi-domain optical networks, the distributed PCE architecture is adopted, and the real-time detection of crosstalk attack is realized by using data collection, data analysis and monitoring point placement strategy module based on grey theory. At the same time, based on the premise of crosstalk detection and distributed PCE collecting alarm information, combined with the idea of distributed location method, the location of crosstalk attack source is realized.
Acknowledgments
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.2020JM-361); the Young and Middle-aged Scientific Research Backbone Projects of Engineering University of PAP (No.KYGG201905); the Basic Research Foundation Project of Engineering University of PAP (No.WJY201920); the Natural Science Foundation of Hebei Province under Grant (NO.F2019402206); the Research Program for Top-notch Young Talents in Higher Education Institutions of Hebei Province, China under Grant (No.BJ2017037).

References
[1] Wen, W., Wu Q.W., Jiang, L.Z. (2017) Trust Model based on D-S Evidence and Game Theory in multi-domain optical network. Journal of Optoelectronics-Laser. 28:44-53.
[2] Li, W., Wang, F., Zhao, F. (2008) Detection and Location of Attacks in All-optical Networks. Modern Electronic Technology. 31:18-20.
[3] Wang, F.F. (2016) Simulation Analysis of Distributed Network Anomaly Attack Detection Model. Computer measurement and control. 24:61-63.
[4] Vosough, H., Tan, S.C. (2014) Performance Analysis of Integer Linear Programming Optical Monitor Placement for Crosstalk Attack Detection in Different Network Topologies. Optik-International Journal for Light and Electron Optics, 125:4722-4725.
[5] Xiao, S.Q.,Wang, S.B. (2017) Research on Automatic Detection of Typical Malicious Data in Optical Network. Laser magazine. 43:159-162.
[6] Wu, T. W. T., & Somani, A. K. (2003) Necessary and Sufficient Condition for k Crosstalk Attacks Localization in All-optical Networks. In: GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489), San Francisco, CA, pp. 2541-2546.
[7] Xie, D.H., Chen, G.J., Yang, J, et al. (2008) Research and Implementation of Optical Network Physical Layer Monitoring Switching System. Optical communication technology, 32:8-10.
[8] Yan, H., Wang, R.Y., Mao, Q.J., Wu, D.P. (2010) A Fast Multi-fault Localization Mechanism for Multi-domain All-optical networks. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, pp. 158-162.
[9] Ren, S., Zhang, Y.F., Peng, B.B., et al. (2014) Multi-point In-band Crosstalk Attack Localization Algorithm for Optical Networks based on Two-parameter Comparison. Semiconductor Optoelectronics. 35:507-511.
[10] Siew, H., W., Tan, S., & C., et al. (2017) Summation and Division of Status Algorithm for Multiple Crosstalk Attacks Source Identification. Journal for Light and Electronoptic. Optik-International Journal for Light and Electron Optics, 132:407-416.
[11] Li, F., Wu, Q.W., Chen, H., Zhou, Y. (2018) Crosstalk Attack Location Algorithm Based on Gray Theory. In: Proceedings of 2018 International Conference on Modelling, Simulation and Analysis (ICMSA 2018). Wuhan. pp. 169-174.
[12] F Li, F., Wu, Q.W., Chen, H., Zhou, Y. (2018) Study on the Effect of Crosstalk Attack in 40Gbs Optical Fiber Communication. In: The 3rd Annual International Conference on Information System and Artificial Intelligence. Suzhou. pp. 552-557.