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

Qiwu Wu 1*, Xueyue Liu 2, Lingzhi Jiang 2, Bo Gan 2

1 College of Equipment Management and Support, Engineering University of PAP, Xi’an, 710086, China
2 College of Information Engineering, Engineering University of PAP, Xi’an, 710086, China
*Corresponding author’s e-mail: cli@hunnu.edu.cn

Abstract. In order to solve the problem that crosstalk attack propagation leads to a large number of interference alarms in multi domain optical network and difficult positioning, the detection and screening mechanism based on attack optical path state discrimination and the improved MD-PLVM (multi domain parallel and limited vector Matching) algorithm for multi domain optical network are used in this paper, a new crosstalk attack detection and location scheme based on distributed PCE called DP-CADL (distributed PCE crosstalk attack detection and location) is proposed. The experimental results show that this scheme can not only eliminate the interference alarm and screen the original attack optical path accurately, but also realize the fast location of multiple crosstalk attack sources between domains and cross domain optical path, and has high location accuracy.

1. Introduction
How to accurately detect and quickly locate high-power crosstalk attacks in multi-domain optical networks is an important research content to ensure network security and improve the survivability of optical networks [1]. At present, there are not many researches on the detection and location of multi-point crosstalk attacks in multi-domain environments. The fault location method using minimum dominance set clustering proposed in [2] greatly shortens the fault location time, but does not consider multi-domain surroundings. The multi-domain and multi-fault location method proposed in [3] uses the PCE architecture and fuzzy set theory to solve the problem of inter-domain link fault location, but its location accuracy is not high enough and it is not suitable for crosstalk attacks. Literature [4] proposed a multi-link segmentation fault location scheme in a multi-domain environment, which realized the rapid location of the faulty link, but this scheme did not consider the propagation characteristics of high-power crosstalk attacks. Literature [5] proposes a detection and recovery mechanism for crosstalk attacks, but it requires a lot of detection equipment and costs too much. Literature [6] proposes a multi-link fault location mechanism that integrates active monitoring services. This mechanism combines active monitoring services with passive fault location algorithms to achieve precise location of concurrent multiple faults and is effective. It can be used for reference, but it is not suitable for multi-domain optical networks and high-power crosstalk attacks.

Therefore, this paper proposes a distributed PCE-based multi-domain optical network multi-point crosstalk attack detection and location scheme DP-CADL, which can eliminate a large number of interference alarms and realize rapid positioning under different attack situations.
2. Multi-point crosstalk attack detection and location scheme based on distributed PCE

2.1. The overall structure
This paper uses the BER detection and comparison of the attack optical path of the OXC port at the alarm to obtain its state information value, and then obtains an OALP set after the attack discrimination, to achieve the purpose of eliminating interference alarms. Finally, the MD-PLVM algorithm proposed in this paper, which is suitable for multi-domain optical network attack location, is used to locate multiple attack sources of OALP.

2.2. Attack detection
(1) OXC port optical path definition
When the multi-domain optical network is attacked by high-power crosstalk and generates a large number of alarms, the PCE of each domain collects the ID of the alarm optical path in the domain and finds the corresponding optical port ID of the OXC at the corresponding alarm. Figure 1 is an OXC optical path port definition diagram, define the input optical port set \( \{LP_{I1}, LP_{I2}, ..., LP_{Inm}\} \), output optical port set \( \{LP_{O1}, LP_{O2}, ..., LP_{Onm}\} \), define \( LP_n \) as the optical path set of all ports of the nth OXC, then there is \( LP_n = LP_{I1} \cup LP_{O1} \). [Diagram of OXC optical port]

(2) ALP status information calculation
Define the state information set of the port attack light path as \( \{S_{nk}\} \), where \( \{S_{nk}\} = \{0, 1, 2\} \). Define \( Br_{nk} \) as the actual BER detected by the optical path of the kth port of the nth OXC, \( Bb_{nk} \) and \( Bt_{nk} \) are the reference BER and threshold of the optical path of the port respectively, and \( dB_{nk} \) is the difference between \( Br_{nk} \) and \( Bb_{nk} \), namely:

\[
dB_{nk} = \left| Br_{nk} - Bb_{nk} \right| \quad (1)
\]

According to the different relationship between \( dB_{nk} \) and \( Bt_{nk} \), the state information value \( S_{nk} \) of the attack light path ALP is obtained, namely

\[
S_{nk} = \begin{cases} 
0, & 0 < dB_{nk} < Bt_{nk} \\
1, & Bt_{nk} \leq dB_{nk} < 2Bt_{nk} \\
2, & dB_{nk} \geq 2Bt_{nk}
\end{cases} \quad (2)
\]

(3) ALP attack discrimination classification
For all attack light paths of OXC at each alarm, we can calculate its status information and output a \( S_{nk} \) according to formula (2). According to the meaning of output \( S_{nk} \), the attack light path ALP is classified into attack discrimination, and the meaning of different status information value \( S_{nk} \) is shown in Table 1.

The ALP with \( S_{nk} = 0 \) is judged as DALP, the ALP with \( S_{nk} = 1 \) is judged as SALP, and the ALP with \( S_{nk} = 2 \) is judged as OALP. Through the sequential discrimination of the attack light path, the OALP set that is most likely to become the original attack light path is finally screened out.

\[\text{Table 1. Status Information Meaning} \]

| Status Information | Meaning |
|--------------------|---------|
| 0                  | DALP    |
| 1                  | SALP    |
| 2                  | OALP    |
2.3. Attack location

Since the traditional PLVM algorithm cannot locate multipoint crosstalk attacks in a multi-domain environment, this paper proposes an improved MD-PLVM algorithm, which uses distributed PCE based on the OALP set detected. First determine the crosstalk attack domain, and then locate the multipoint crosstalk attack between and within the domain.

Table 1. Definition of MD-PLVM algorithm parameter

| Parameter | Definition                                      | Parameter | Definition                                      |
|-----------|------------------------------------------------|-----------|------------------------------------------------|
| DN        | The destination node of each LP in OALP        | BN        | The boundary node of each LP in the OALP set    |
| Dl(m)     | Network diameter within the domain             | D(m)      | Link length between domains                     |
| v0(m/s)   | The propagation speed of the signal in the fiber| INTRADA   | Intra_Domain Alarm                              |
| INTERDA   | Inter_Domain Alarm                             | MS        | Monitor Signal                                  |
| GA        | Go Ahead                                       | ERQ       | Executive Route Queue                           |
| ER        | Executive Route                                | ES        | Executive Sink                                  |
| ALV       | Affected-Link Vector                           | LA        | Limited Area                                    |
| LV        | Link Vector                                    | BV        | Binary Vector                                   |
| PES       | Potential Executive Sink                       |           |                                                  |

(1) Determine the crosstalk attack domain

Step1: The DN included in the OALP set starts a timer with a duration of $2D_l / v_0$, and sends "INTRADA" to the PCE and all nodes in the domain.

Step2: The entry BN included in the OALP set starts a timer with a duration of $2d / v_0$, and sends "INTERDA" to the PCE and all nodes in the domain. After receiving the message, the PCE in the domain sends "INTERDA" to the upstream PCE and border node, and sends "MS" to the downstream BN and DN.

Step3: The exit BN included in the OALP set starts a timer with a duration of $2d / v_0$, and sends "INTERDA" to the PCE and all nodes in the domain. After receiving the message, the PCE in the domain sends "INTERDA" to the downstream PCE and border nodes, and also sends "MS" to the downstream BN and DN.

Step4: When a boundary node that does not belong to the BN set receives "INTERDA" in this ID field, it will send "GA" to its connected downstream boundary node.

Step5: If a border node receives "INTERDA" in different ID domains, the inter-domain link formed by the node and the signaling node will be judged as a crosstalk attack domain.

Step6: If there is only DN but no BN in a certain domain, the domain is regarded as a crosstalk attack domain.

Step7: If no egress boundary node in a certain domain receives "GA", and all DNIs and egress BNs have received the correct "MS", it is determined that there is no crosstalk attack in this domain. Otherwise, consider the domain as a crosstalk attack domain.

(2) Location of multi-point attacks between domains

Step1: If a border node that does not belong to the BN set receives "INTERDA" in different ID domains, it is determined that the inter-domain link formed by the node and the signaling node is subject to crosstalk attacks.

Step2: If a BN receives "INTERDA" from different ID domains, it will look for at least one of the pair of boundary nodes to receive the correct "MS" within $2d / v_0$'s time. If so, it is determined that the inter-domain link formed by the pair of border nodes is not subject to crosstalk attack, otherwise it is determined that it is subject to crosstalk attack.
To locate the crosstalk attack, the steps are as follows:

Step1: Define the DN in the domain as the potential execution node PES. Each PES sends "INTRADA" to all nodes in the domain. This "INTRADA" contains the ID of the PES and the length of the part of the OALP that reaches it.

Step2: When a PES receives "INTRADA", it extracts all the OALPs that point to it, and inserts them into a list in ascending order according to their length. If two OALPs have the same length, the OALP with the smaller source node ID is inserted first, and if the source nodes are the same, the node with the smaller ID connected to the OALP is inserted first.

Step3: Each PES compares the OALPs in the list one by one in order, and stores the two OALPs without common links into different ERQi (i=1,2,...,n). If there are common links between the first OALP and other OALPs, then the second OALP is compared with other OALPs in the table, and so on, until two OALPs without common links are found. If all the OALPs in the list cannot be found without a public link after the comparison, the attack is judged as a single-point crosstalk attack, and the LVM protocol can be used to locate the attack.

Step4: After finding two separate OALPs, continue to compare them with the remaining OALPs in the list. The specific steps are as follows:

Step4.1: If there is a common link between a certain remaining OALP and one of the two separated OALPs, add it to the ERQi corresponding to the OALP.

Step4.2: If there is a common link between a certain remaining OALP and two separate OALPs, it is determined that this OALP will not provide a useful reference for attack location, and it is ignored.

Step4.3: If there is no common link between a certain remaining OALP and two separate OALPs, add it to a new ERQi. This situation indicates that a new attack has been discovered, and then continue to compare this OALP with the OALP in the list.

Step4.4: Repeat the above steps until all the remaining light paths in the list have been compared.

Step5: At this time, all OALPs in the network have been stored in different ERQi according to the impact of different attacks. Next, each ERQi is located for a single point attack, and the positioning process can be performed at the same time. The specific steps for locating each ERQi attack are as follows:

Step5.1: Define the first OALP in ERQi as the execution path ER, because its link length is the shortest. At the same time, the PES of the OALP is determined as the execution node ES.

Step5.2: ES will generate a link vector ALV about ER affected by the attack, and at the same time determine a restricted area LA. The LA includes all nodes and links in the ER, as well as its neighboring nodes. Then ES broadcasts ALV to all nodes in LA.

Step5.3: When the node in LA receives the ALV, it will match the link vector LV of the optical path where it is located with the ALV, and the result is represented by a binary vector BV. For OALP, if there is a common link between LV and ALV, set the corresponding binary bit in BV to 1, otherwise set to 0, and set the OALP state to 0; for normal LP, if there is a common link between LV and ALV, then the corresponding binary bit in BV is set to 0, otherwise it is set to 1, and the LP state is set to 1.

Step6: If there is no common link between BV and ER, the corresponding destination node will not send the binary vector to ES. On the contrary, the corresponding destination node will send the BV to ES.

Step7: Each ES performs logical AND operation on all BVs received within the LA range. If the number of "1" in the result is 1, it means that the crosstalk attack has been accurately located, and the ES will transmit the attack link information to the PCE in this domain, and the PCE will broadcast an ATTACK_LOCATION message to all where it is. The PCE of the domain adjacent to the domain. Otherwise, the ES will expand the range of the LA, that is, add the neighboring nodes of the neighboring nodes of the ALV to the range of the LA, and perform positioning again.
The characteristic of cross-domain OALP is that when the OALP where the attack link in a certain domain passes through the domain and is transmitted to other domains, it will alarm the BN of the inter-domain link. In view of this situation, this article chooses to define the DN in the domain, the exit BN that did not receive the correct "MS" within time $2d / v_0$, and the exit boundary node that received "GA" as potential execution nodes PES, and then execute the steps in Step1~Step7 perform crosstalk attack positioning.

3. Simulation

3.1 Network structure and Parameter settings
This paper uses VPI simulation platform combined with MATLAB simulation software to verify the reliability and effectiveness of the DP-CADL program. Figure 2 shows the experimental simulation established in the VPI platform. The main parameter settings of the experiment are as follows: 1) Bit rate is 10Gbit/s; 2) Sampling rate is $8 \times 10^{10}$Hz; 3) Nonlinear refractive index is $2.6 \times 10^{-20}$m$^2$/W; 4) Time window is $1.024 \times 10^{-7}$s; 5) Dispersion coefficient is $2.0 \times 10^{-3}$ps/nm/km; 6) Fiber attenuation coefficient is 0.2dB/km.

The multi-domain optical network adopts the Dijkstra algorithm to dynamically select the service request optical path. Assume that the LP service requests in the network obey the Poisson distribution, and the destination nodes are evenly distributed in the network. Set the transmission speed $v_0$ of the signal in the optical fiber to $2.15 \times 10^8$ m/s, and the unit matching time $t_0$ of OALP to $2.1 \times 10^{-8}$s.

3.2 Experiment analysis
Set up different numbers of LP requests, observe the changes in the attack location accuracy of the DP-CADL solution, and analyze the changes in the maximum attack location delay and average attack location delay of the DP-CADL solution under different attack situations from A to G.

Figure 3(a) shows the accuracy of attack location under different numbers of LP requests. It can be seen from the figure that when the number of LP requests is small, the accuracy of attack location is lower, but when the number of LP requests continues to increase, the location accuracy rate of the system has improved rapidly and has grown significantly. Figure 3(b) shows the variation of the maximum attack location delay $T_m$ as the number of LP requests increases under different attack situations from A to G. Through the simulation experiment on the attack situation of A, it is obtained that the maximum attack location delay $T_m$ of A is $1.031 \times 10^{-8}$s, and the average attack location delay $T_A$ is $6.9782 \times 10^{-9}$s. Therefore, the DP-CADL solution can achieve the purpose of quickly locating multi-point attacks between domains. When the number of LP requests reaches 400, the attack
The location accuracy rate of the multi-domain optical network is close to 1, and the maximum attack location delay at this time is much less than the attack location time required by OSPF, which is 40 ms. Therefore, the DP-CADL solution can quickly locate the inter-domain and intra-domain multi-point crosstalk attacks of the multi-domain optical network, and has a high positioning accuracy.

![Figure 3. Experiment outcome](image)

4. Summary

In this paper, a new crosstalk attack detection and location scheme based on distributed PCE called DP-CADL is proposed. This scheme can not only eliminate the interference alarm and screen the original attack optical path accurately, but also realize the fast location of multiple crosstalk attack sources between domains and cross domain optical path, and has high location accuracy.

Acknowledgments

This work is supported by 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, No.WJY202019, No.WJY202144), the military theory research project of engineering university of PAP (No.JLY202085), the education and teaching fund project of Engineering University of PAP (No.WJ202039, No.WJX2021101), the research capacity improvement plan of engineering university of PAP (No.WKY202127), the PAP’s Military Scientific Research Mandatory Project (No.WJ2020A02048).

References

[1] Zhang B, Zhao Y, Rahman S, et al. (2020) Alarm classification prediction based on cross-layer artificial intelligence interaction in self-optimized optical networks (SOON)[J]. Optical Fiber Technology, 57:251-264.
[2] Hong Z.(2013) Research on Fault Location Mechanism Based on Restricted Area in Optical Network [D]. Chongqing University of Posts and Telecommunications, 2013.
[3] Jingran L. Research on multi-fault location mechanism and flexible network optimization mechanism in PCE-based multi-domain large-capacity optical transport network [D]. Beijing University of Posts and Telecommunications.
[4] Qijian M, Hong Y, Ruyan W, et al.(2010) Multi-domain all-optical network fast multi-link fault location mechanism [J]. Optical Communication Technology, 33(9):5-8.
[5] Furdek M. (2011) Physical-Layer Attacks in Optical WDM Networks and Attack-Aware Network Planning [J]. European Journal of Operational Research, 178(2):1160-1167.
[6] Chen M, Huixia D, Yongli Z, et al.(2013) Multi-link fault location algorithm based on active monitoring service in electric power optical transmission network [J]. Power System Technology, 37(11):3222-3225.