A multi-point crosstalk attack detection and localization scheme based on hierarchical PCE in multi-domain optical networks

Qiwu Wu 1*, Xueyue Liu 2, Lingzhi Jiang 2, Mingzhu Zheng 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: With the limited number of detection devices and the uncertainty of crosstalk attack source localization, how to propose an effective detection and localization scheme for multipoint crosstalk attack problem in multi-domain optical networks is an important problem that needs to be solved. A new multipoint crosstalk attack detection and location scheme HP-CADL (Hierarchical PCE-Crosstalk Attack Detection and Location) for multi-domain optical networks based on hierarchical PCE is proposed by using the monitoring point selection strategy of local immune algorithm and distributed localization considering continuous parametric analysis. VPI simulation results show that the scheme not only achieves low-cost monitoring and detection and accurate localization of multiple crosstalk attack sources, but also achieves higher accuracy and better performance than other similar schemes in the same multi-domain environment.

1. Introduction
Optical networks are gradually occupying an important position in daily communications, but their transmission transparency also gives challenges to the transmission security belt of various services. How to effectively detect and locate the service disruption attacks by illegal users is an important challenge that needs to be thought and studied at present.

There are already studies on crosstalk attack detection and localization. The crosstalk attack detection and localization method based on gray theory (GT-CADL for short) proposed in literature [1] can achieve real-time detection in a multi-domain environment, but the method only uses a spectrum analyzer to discriminate, and the accuracy rate is not satisfactory. The multi-link attack fast localization method proposed in the literature [2] discusses both intra-domain and inter-domain cases separately, but does not consider the propagation of crosstalk attacks. The literature [3] uses a parameter comparison and optical device monitoring method (referred to as PC-CADL) for attack detection, but this method affects the signal power and has low detection efficiency. The literature [4] proposes a distributed attack detection scheme that can improve the detection rate and achieve effective detection, but it is not suitable for multi-domain environments. The literature [5] proposes a binary tree-based fault location algorithm for optical networks, which improves the location accuracy, but is only applicable to single-domain and has high complexity. Most of the above methods are only for single-domain environment or single-point attacks, so this paper proposes a HP-CADL scheme for detection and localization for multi-domain optical network architecture with hierarchical PCE, which can effectively detect and locate multi-point...
crosstalk attacks in multi-domain environment.

2. Research Methodology

The idea of immunization strategy for complex networks is similar to the goal of monitoring and detecting crosstalk attacks in multi-domain optical networks. Therefore, this paper proposes a local immunization algorithm focusing on the comparison of node access and clustering coefficients, so that the set of nodes with high influence can be selected for the detection and localization of crosstalk attacks. The localization method of distributed control can locate the source of crosstalk attack by analyzing the information detected by a node and its upstream and downstream nodes, and has the feature of high timeliness, so it is widely used in the research of attack localization.

3. Crosstalk attack detection and localization scheme for multi-domain optical networks based on hierarchical PCE

The HP-CADL scheme designed in this paper combines the crosstalk attack propagation model to derive the set of monitoring nodes through a two-round selection mechanism, and selects nodes with high influence to place monitoring devices to achieve monitoring detection and accurate localization of the attack source with the least number of devices.

3.1 Attack Detection

3.1.1 Monitoring selection module

A local immunization algorithm with a two-round selection system is used as follows:

Step1: In a multi-domain optical network $G=(V,L,W)$, pPCE uses Dijkstra's algorithm to calculate the set of paths for attack propagation $U$, $U \subseteq (q,p), (i,j=1,2,\ldots,n)$. $V$ is the set of nodes, $L$ is the set of links, $W$ is the number of power accumulations between nodes, and $q$ and $p$ are the source and destination nodes for crosstalk.

Step2: The NAP values of the nodes in $U$ are calculated using the formula (1) and the iterative process, numbered from highest to lowest and stored in $Z_1$.

$$NAP(v) = \theta + \sum_{i=1}^{N} P^* NAP(v_i), v_i \in UNS(v) \quad (1)$$

$\theta$ denotes the probability that node $v$ is attacked by itself ($0 \leq \theta \leq 1$), $N$ is the number of upstream neighbors of $v$, and $P$ denotes the probability that $v$ is attacked by neighboring nodes.

Step3: In the first round of selection, the top $x$ proportion of nodes in $Z_1$ are extracted and deposited in $Z_2$, and the clustering coefficient of each node is calculated using $C_v = \frac{2E_v}{k_v(k_v-1)}$. $x$ is the density to be selected, $E_v$ is the total number of edges present, and $k_v$ is the degree of node $v$.

Step4: For the second round of selection, the $C_v$ values of $Z_2$ nodes are numbered from highest to lowest with reference to step 3 and stored in $Z_3$.

Step5: The nodes in the first $y$ proportions of $Z_3$ are extracted to obtain the set of monitoring nodes. $y$ is the monitoring density.

3.1.2 Detection and analysis module

Comparing each monitoring device, it can be seen that Eye and BER monitor have better detection capability, so Eye and BER monitor are used for joint monitoring.

3.2 Attack localization

Locate the source node of the attack using a distributed localization method considering continuous upstream node covariance analysis. Set the monitoring node M state including normal and alarm, denoted by $S = 0$ and 1; non-monitoring node N state including attacked and not attacked, denoted by $A = 1$ and 0; $A'$ and $A''$ are the upstream node $N'$ of $N$ and the attack covariates of the upstream node $N''$ of $N$. The specific steps are as follows:

Step1: The set of monitoring nodes is detected in real time, alerted when attacked and alarm messages
are generated.

Step2: Each cPCE is responsible for collecting alarm information in its domain, and the pPCE aggregates and processes the alarm information.

Step3: If $S=1$, upstream non-monitoring node $N$ needs to be detected; if $S=0$, no detection is required.

Step4: When detecting $N$, if $A=1$, need to detect $N'$; if $A=0$, no need to detect.

Step5: When detecting $N'$, if $A'=1$ and $N''$ exists, we need to detect $N''$; if $A'=0$ or there is no $N''$, we decide $N$ is the source node of the attack.

Step6: $S=1, A=1, A'=1$, if $A''=1$, determine $N''$ as the attack source node; if $A''=0$, determine $N'$ as the attack source node.

### 4. Simulation

In order to verify the effectiveness of the HP-CADL scheme, this paper uses the VPI platform to build the model shown in Figure 1 for simulation experiments, and compares the designed HP-CADL scheme with the GT-CADL scheme proposed in the literature[1] and the PC-CADL scheme proposed in the literature[3]. $\text{Tx}_1\text{OOK}$ is used for the transmit module; $\text{FiberNLS}$ is used for Fibers, $\text{SwitchDOS\_Y\_Two}$ and $\text{SwitchMatrix4\_4}$ for OXC, $\text{AmpSysOpt}$ for EDFA, $\text{WDM\_MUX\_2\_1}$/ $\text{WDM\_DEMUX\_1\_2}$ and $\text{WDM\_MUX\_4}$ for MUX/DMUX_1/WDM_DEMUX_1_4; crosstalk module injects attack signal with frequency $f_1$ to $\text{Tx}_1\text{OOK}$; detection module uses joint monitoring at $M_1, M_2, M_3, M_4$, $\text{CombinerPow\_N\_1}$ for combiner, $\text{SignalAnalyze}$ and $\text{Rx\_OOK\_BER}$ for monitor, $\text{Powermeter}$ monitors statistical optical power, connect the output of $\text{Rx\_OOK\_BER}$ and $\text{Powermeter}$ to $\text{NumericalAnalyzer2D}$.

![Experimental simulation diagram of HP-CADL scheme](image)

**Figure 1.** Experimental simulation diagram of HP-CADL scheme

#### 4.1 HP-CADL’s attack detection capabilities

The attacks in $D_1$ are monitored at $y=4$. As shown in Figures 2 and Figures 3, the attacks are detected at $\text{OXC}_1$-$\text{OXC}_4$ and $\text{OXC}_4$ is subjected to the largest attack. Therefore, to detect the attack source $@1$ in $D_1$, it is sufficient to set up a monitoring point at $M_1$ of $\text{OXC}_4$. Similarly, to detect the attack source $@2$ in $D_2$, it is only necessary to set up a monitoring point at $M_4$ of $\text{OXC}_5$. And for $D_3$, setting up monitoring points in $M_2$ and $M_3$ can monitor both the domain and the neighboring domains.
4.2 HP-CADL’s attack positioning capability
From Figure 4, it can be seen that OXC6 has the highest BER, indicating that it is the source node that causes the propagation of attacks within D2.
4.3 Accuracy analysis of HP-CADL

Figure 5 shows the trend of the accuracy rates of the three schemes over time. From the figure, it can be seen that the accuracy rate of GT-CADL is slightly higher than that of HP-CADL in the early stage, but in the middle and late stage, HP-CADL has the highest accuracy rate and obvious advantage.

5. Summary

In this paper, a new hierarchical PCE-based multi-domain optical network multi-point crosstalk attack detection and location scheme (HP-CADL) is proposed. This scheme can not only achieve low-cost monitoring and detection, but also can accurately locate multiple sources of crosstalk attacks.

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.JLY2020085), the education and teaching fund project of Engineering University of PAP (No.WJJ202039, No.WJX2021101), the research capacity improvement.
plan of engineering university of PAP (No.WKY202127), the PAP’s Military Scientific Research Mandatory Project (No.WJ2020A020048).

References
[1] Li,F.(2018)Research on crosstalk attack detection and intrusion tolerance technology for multi-domain optical networks. M.D. Thesis, Armed Police Engineering University, Xian.
[2] Yan,H., Wang R Y., Mao Q J., et al.(2010) A fast multi-fault localization mechanism for multi-domain all-optical networks. In: 2010 3th International Conference on Advanced Computer Theory and Engineering, pp.158-162.
[3] Li,W., Wang,F., Zhao,F.(2008)Detection and localization of attacks in all-optical networks. Modern Electronic Technology, 31(15):18-20.
[4] Wang,F.(2016)Simulation analysis of distributed network anomaly attack detection model. Computer measurement and control, 24(10):61-63.
[5] Wang,Q., Ao,F.(2008) Research on optical network fault location algorithm based on binary tree. Journal of Guilin University of Electronic Science and Technology, 28(4):273-276.