CHALMERS
UNIVERSITY OF TECHNOLOGY

Eavesdropping Detection and Localization in WDM Optical System

Eavesdropping Detection and Localization in WDM Optical System

Haokun Song[1,2]
[1]Electrical Engineering Department
Chalmers University of Technology
[2]School of Electronic Engineering
Beijing University of Posts and Telecommunications
Gothenburg, Sweden
haokun@ chalmers.se

Rui Lin
Electrical Engineering Department
Chalmers University of Technology
Gothenburg, Sweden
ruilin@chalmers.se

Lena Wosinska
Electrical Engineering Department
Chalmers University of Technology
Gothenburg, Sweden
wosinska@chalmers.se

Paolo Monti
Electrical Engineering Department
Chalmers University of Technology
Gothenburg, Sweden
paolo@chalmers.se

Yajie Li
School of Electronic Engineering
Beijing University of Posts and Telecommunications
Beijing, China
yajieli@bupt.edu.cn

Jie Zhang
School of Electronic Engineering
Beijing University of Posts and Telecommunications
Beijing, China
jie.zhang@bupt.edu.cn

***Abstract*—Leveraging our initial work on detecting eavesdropping events in WDM optical systems [1], we propose a mechanism that utilizes bisecting k-means on dynamic optical performance monitoring (OPM) data to initialize the detection. We develop a method to detect and localize single and multiple eavesdropping events in WDM optical systems. Very small losses caused by eavesdropping can be detected using OPM data collected at the receiver, while the in-line OPM data enables localizing single and multiple eavesdropping events.**

Keywords—eavesdropping, power, machine learning

I. INTRODUCTION

Security in optical networks is becoming very critical due to the increasing amount of data and critical services utilizing fiber network infrastructures. [2]. Physical-layer-based monitoring systems and various detection methods need to be employed to enhance security.. The most commonly used detection methods are based on time domain reflection [3,5] and Rayleigh scattering [4]. However, such methods are costly and complex [5]. Moreover, monitoring link impairments and other channel conditions may lead to the negative impact on transmission.

The development of machine learning applied in optical communications offers a promising solution to ensure transmission quality while conducting failure localization [6]. Various data sources, including transceiver parameters at multiple nodes, can be utilized to localize soft faults in optical networks (device insertion loss exceeds twice the maximum normal value, amplifier gain less than half of the minimum normal value, *etc.*) [7]. In [8], interpretable artificial intelligence is used to localize 11 dB additional attenuation in 3 spans of fiber link with a single monitor at the receiver or multiple monitors along the lightpath. Nevertheless, detection and localization of events that do not significantly degrade transmission performance, such as eavesdropping, remain challenging.

In this paper we leverage on our prior work [1] on detecting individual instances of eavesdropping in a WDM system, and we study scenarios where multiple eavesdroppers may be present. The primary contribution of this paper is: i) the proposal of a clustering-based approach for identifying and localizing multiple eavesdropping events, ii) subdivision and discussion of different eavesdropping cases at the transmitter end for WDM systems, iii) application of clustering algorithms to dynamic data for more flexible eavesdropping detection, making the approach more general as well as fitting to the real scenarios involving WDM systems. We validate our proposal by simulations conducted on a two-channel WDM system spanning four fibre spans. An attenuator inducing power loss of 0.8dB [9] is used as the emulator of a fibre-bending-based eavesdropping event. OPM data at the receiver and in-line link are collected for eavesdropping detection and localization purposes. With the data for the normal case (*i.e.*, without eavesdropping), the agent can decide when to start detecting. Based on the variation of average sum of squared errors (SSE), an eavesdropping event can be detected. The detection results demonstrate that fiber-bending eavesdropping with 0.8dB power loss all achieve a 100% label matching rate with receiver OPM data. Besides, 100% label matching rate localization can be achieved by leveraging in-line OPM data including of transmitter, receiver, and spans data. In addition， we define D representing the distance between the central points of clustering, which can be used to get an estimate of how many possible eavesdropping points are in the spans.

This work is supported by the EUREKA cluster CELTIC-NEXT project AI-NET PROTECT funded by VINNOVA, the Swedish Innovation Agency.

II. Flow Chart for Detecting Multiple Eavesdroppers

In a WDM system, eavesdropping can occur at different places, including the transmitter before the signal booster, within the path, and at the receiver end. Among those options, eavesdropping after the receiver booster is easiest to detect due to obvious power loss. In this context, we classify the system's conditions into three distinct types. The absence of eavesdropping is characterized as the *normal scenario*. When eavesdropping occurs at the transmitter, its impact is confined to a specific channel within the WDM signal, while others remain unaffected. We refer to this as "*selective eavesdropping*", which can be discerned through the disparities in the OPM data across the different channels. Conversely, when eavesdropping occurs within the in-line fiber link, it affects all WDM channels equally. We term this as "*uniform eavesdropping*". Eavesdropping before the booster and in fiber spans both belong to this category. For eavesdropping detection, OPM data about the receiver and other in-line links in *normal scenarios* must be collected as a benchmark. As the system operates, fresh OPM data is continuously collected. This new set of OPM data is called "*pending data*" representing "*pending event*".

The proposed eavesdropping detection method consists of three steps shown in Fig. 1. Step 1 starts with categorizing the *pending events* as either *normal scenario* or *eavesdropped*, which involves the OPM data available at the receiver end in both the *pending event* and the *normal scenario*. Eavesdropping can be detected using the dynamic data clustering method described in Section IV. The results of the detection are the basis for the next two steps. Step 2 determines if there is *selective eavesdropping* (only eavesdropping at partial channel transmitters). OPM data from different channels is attempted to be categorized into two groups. Successful categorization indicates the presence of transmitter eavesdropping on the worst channels. Subsequently, the data associated with the better channel conditions are selected for localization in STEP 3. This step requires OPM data from both the receiver and the in-line link. These two sets of OPM data are separately employed to carry out binary classification of the pending and the normal data. In the event of a successful classification, it confirms that an eavesdropping point exists either preceding the booster or within the spans. The approach is applicable to known transmission lines. Detection and localization of the entire topological network is not involved. There is a particular case worth noting. If the *pending event* is identified as being eavesdropped in STEP 1, however, determined to be free of selective transmitter eavesdropping [STEP 2] and the presence of transmitter eavesdropping [STEP 3] at the same time, it signifies that all channels' transmitters are subject to eavesdropping.

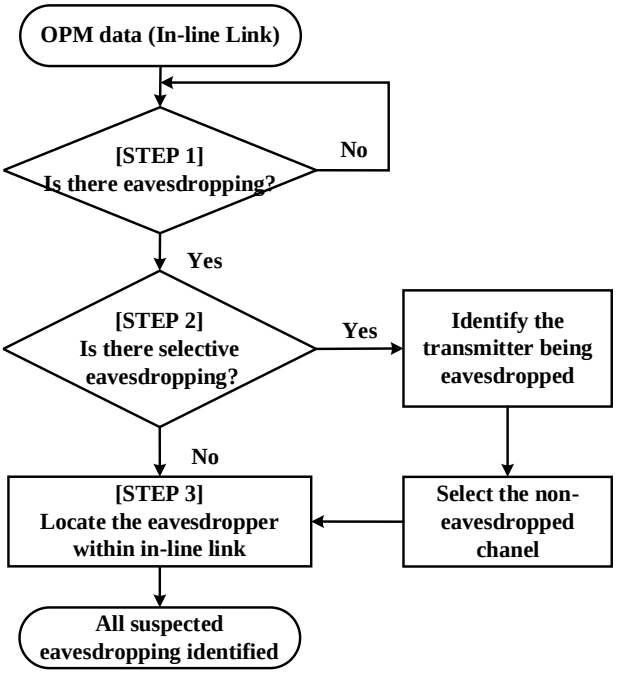

Fig. 1. Flow-chart for multi-eavesdropping detection procedure.

III. Eavesdropping Simulation System

A. Simulation Setup

The low-loss eavesdropping simulation system in Fig. 2 is based on the previous work in [1]. Compared than before, the transmitter cases are subdivided into *normal scenario, selective eavesdropping* and *uniform eavesdropping*. As well as the eavesdropping is extended from a single point to multiple points. So both detection and localization are more complicated. We have a 112Gbps dual-polarization quadrature phase shift keying (DP-QPSK) WDM system with two channels (1550.12 nm and 1550.92 nm) and four fiber spans, which can be divided into four parts: two transmitters, link (with four spans), two receivers, and multiple monitors (see Fig. 2). All parameters at the transmitters are held constant to keep the output power at 0 dBm. The attenuator is used to simulate different power loss events. The booster gain is adjusted so that the power into the in-line fiber remains at 0 dBm. The in-line amplifiers compensate for all the attenuation in the current span so that the power into the next fiber span can be consistent.

B. OPM Data Collection

The sample data obtained from each run includes the following nine optional parameters: optical signal noise ratio (OSNR), bit error rate (BER), power at the receiver (P_{rx}), power at the transmitter (P_{tx}), power before the booster (P_{link}), and power of each span ($P_{spani,\ i=1,\ 2,\ 3,\ 4}$). Power can be obtained from the optical power meter. OSNR is available from the WDM analyzer. The BER is calculated by the BER test set located at the transmitter part, which compares the transmitted and received sequences and counts the different bits for BER calculation. These parameters can be obtained directly from the monitoring components. In real- deployed systems, OSNR, BER, and P_{rx} can be acquired directly at the receiver. At the same time, the remaining parameters need to be communicated to the receiver end, *e.g.*, via the control/management plane.

In the simulation, an attenuator emulates the eavesdropping device. The power loss induced by a typical clip-on coupler-based eavesdropping device [9] is measured as a benchmark to establish the scope of the power range under investigation. Measured by OTDR, a power loss of 0.8dB on the link can be observed. Attenuators are used to emulate eavesdropping at six possible locations indicated as dashed arrows in Fig.2 (two cases before the booster and four cases in spans). There are four

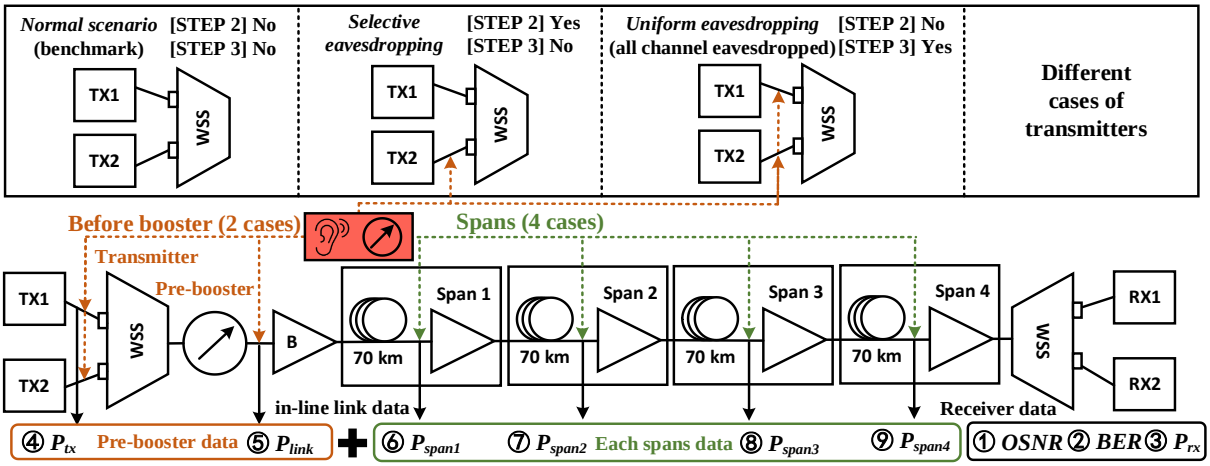

Fig. 2. Flow chart of power-loss eavesdropping simulation system.

combinations of two-point eavesdropping: transmitter & pre-booster, transmitter & spans, pre-booster & spans, and two-points in spans. In addition, we can distinguish between two cases involving transmitter eavesdropping. Since the data with better channel conditions, *i.e.*, no transmitter eavesdropping, are selected after the [STEP 2] of the judgment, there are no cases in which the results of both [STEP 2] and [STEP 3] are YES. For each case, 200 data samples are collected, where each data sample includes nine parameters. The simulation system collects 1400 data samples for multi-eavesdropping detection and localization.

IV. Dynamic Data Bisecting K-means Clustering

K-means clustering is a method that aims to partition n observations into k clusters by minimizing within-cluster variations. The detailed process and the reason it is selected can be found in [1]. Differently from [1], the dynamic data clustering method detects the eavesdropping by constantly changing the amount of data, setting the value of K, and observing the results for SSE. The performance indicators considered in this work are label matching rate and SSE (calculation formula is also in [1]). A small SSE represents a better clustering result. Since the amount of data constantly changes, we consider SSE/data volume instead of SSE, implying the average Euclidean distance of the data points involved in the clustering to their centers, hereafter referred to as SSEDV.. It is necessary to clarify that when clustering methods are utilized to solve the detection problem, only the K=1 or K=2 clustering is involved. In the *normal scenario*, the SSEDV should not vary much (whether K=1 or K=2) between the clustering of the receiver data collected and the known normal data. The pending and known normal data are mixed for clustering whenever eavesdropping is taking place. If K=1 is set, SSEDV will increase with the number of outliers. So when it is found that the SSEDV for K=1 is increasing, we check the results for K=2. If SSEDV for K=2 is more stable and smaller than for K=1, it can be concluded that the observed event is an eavesdropping.

V. Results and Discussion

The results are discussed following the three main steps presented in Fig.1. The collected OPM data is standardized before implementation of the clustering algorithm. It is transformed into pure dimensionless values in order to make it comparable and for weighting data of different units or magnitudes. This allows for the calculation of D, i.e., the distances between the centroids of the different clusters. Higher D means that the data of this two clusters are more distinct.

A. Eavesdropping Detection by Dynamic Data Clustering

The eavesdropping detection results based on the dynamic data bisecting k-means clustering are shown in Fig. 3. The system continuously collects new OPM data and classifies it with the existing *normal scenario* data. The x-axis represents the increasing amount of *pending data* and the y-axis represents SSEDV. If the *pending event* is *normal scenario*, the resulting SSEDV is relatively stable no matter K=1 or K=2. However, the presence of eavesdropping data does cause the SSEDV to increase for all classification results, indicating that the results are getting worse. As the eavesdropping data keeps increasing, the SSEDV for K=2 is very similar to the results in the classification with only *normal scenario* and K=1, indicating that the classification results are once again stabilizing. Thus, the *pending data* does include extra-normal scenarios data, *i.e.*, eavesdropping.

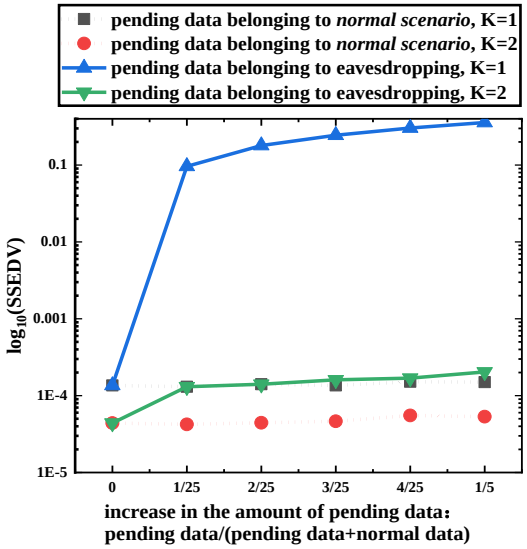

Fig. 3. Differences in SSEDV changes with different pending data increasing.

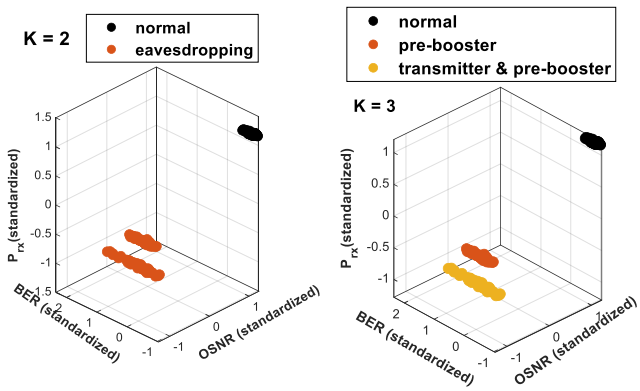

Fig. 4. Detection results for the selective transmitter eavesdropping case.

B. *Selective Eavesdropping*

Fig. 4 shows the results of STEP 2, selective transmitter eavesdropping detection. The case of K = 2 shows that different channel states are classified together as eavesdropping, indicating that selective eavesdropping does not affect the eavesdropping detection results. The clustering result for K=3 with the same data shows that the receiver OPM data can be used to distinguish between different channel states. Following the eavesdropping detection procedure, *pending data* that is closer to the *normal scenario* (*i.e.*, the better channel state) should be selected for the next step.

C. *Localizing the Eavesdropping in the In-line Link*

Localizing the suspected eavesdropping points requires in-line OPM data of both the *normal scenario* and the *pending event*. The suspected points are determined independently by dividing the link into two sections: before the booster and within the spans. The location of the pre-booster section requires two parameters, P_{tx} and P_{link}, while the spans section requires the $P_{spani,\ i=1,\ 2,\ 3,\ 4}$. Different parameters compose different dimensions of the data. If the chosen parameters can differentiate the data, there will be a variation in the data within this dimension, indicating a potential eavesdropping point. Fig. 5 illustrates several possible categorization outcomes.

In Fig. 5, the (a), (b), and (c) diagrams show three possible clustering results for the pre-booster, each illustrated with different data examples: (a) indistinguishable data (divided into two groups with random initial center points), (b) data distinguishable in one dimension, and (c) data distinguishable in two dimensions. Likewise, in the within-spans section, (d), (e), and (f) diagrams correspond to the three possible outcomes: (d) indistinguishable data, (e) data distinguishable in one dimension, and (f) data distinguishable in two dimensions. However, it's worth noting that (e) and (f) can be challenging to differentiate based on the clustering results obtained from the selected mapping parameters. This situation raises the issue of potentially multiple eavesdropping points within the spans. To address this problem, the parameter D is introduced, *i.e.*, the distance between the central points of clustering. The more eavesdropping points in spans, the more significant the gap between the two groups of data, and the distance between the clustering centers is farther away. The method allows for an estimation of the number of eavesdropping points. Notably, the clustering results exhibit a label-matching rate of 100% across all scenarios except for (a) and (d).

VI. Conclusion

A three-step cluster-based method for eavesdropping detection in a WDM optical system is proposed and validated. It requires only OPM data and achieves a 100% label-matching rate for an eavesdropping caused 0.8 dB power loss. In addition, bisecting K-means clustering algorithms are applied to detect eavesdropping. Validation of this method in an experimental system and using semi-supervised learning for automatic detection are envisioned for future work.

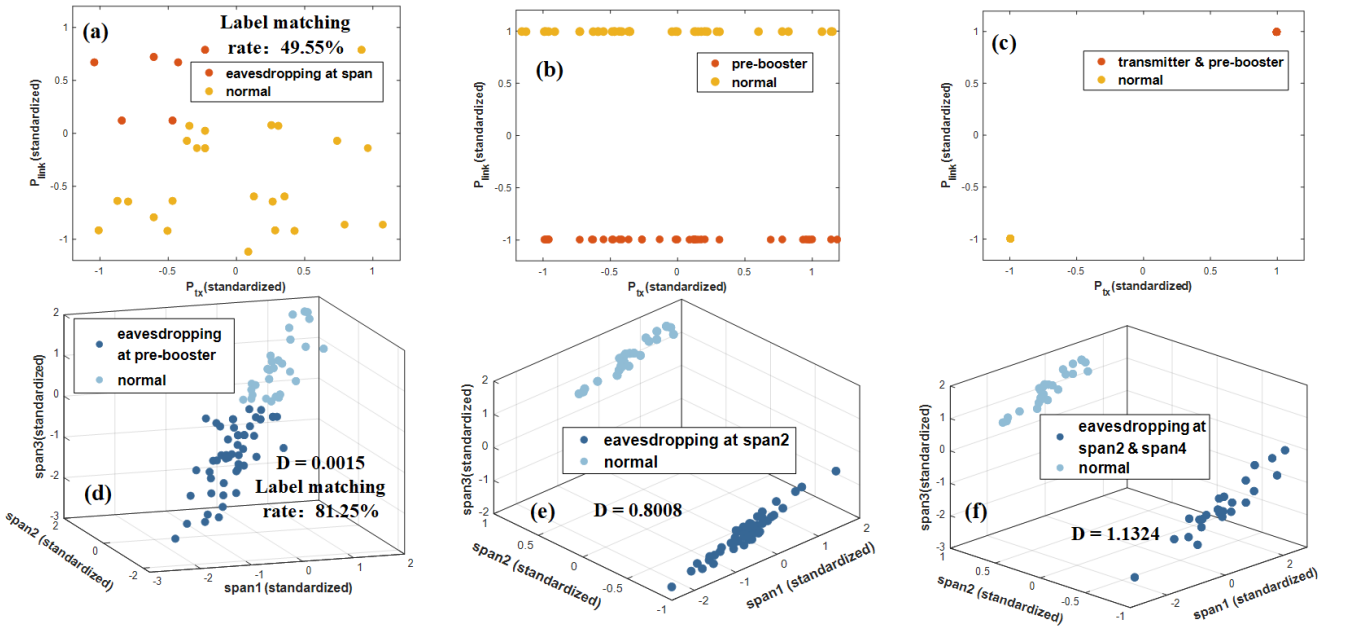

Fig. 5. Clustering results for the before booster and spans. (a) before booster section: indistinguishable (b) before booster section: distinguishable in one dimension (c) distinguishable in two dimensions (d) spans section: indistinguishable (e) spans section: in one dimension (f) spans section: in two dimensions

REFERENCES

[1] H. Song, R. Lin, A. Sgambelluri, F. Cugini, Y. Li, J. Zhang, and P. Monti, "Cluster-based method for eavesdropping identification and localization in optical links (invited presentation)," arXiv submit: 5134247, 2023.

[2] M. Ruzicka, L. Jabloncik, P. Dejdar, A. Tomasov, V. Spurny, P. Munster, "Classification of Events Violating the Safety of Physical Layers in Fiber-Optic Network Infrastructures," Sensors, vol. 22, 2022, pp. 1-17.

[3] M. Fernández, L. Bulus Rossini, L. Morbidel and P. Caso, "PON monitoring technologies based on OTDR techniques: state of the art and trends," IEEE Biennial Congress of Argentina (ARGENCON), San Miguel de Tucuman, Argentina, 2018, pp. 1-7.

[4] X. Bao, Y. Wang, "Recent advancements in Rayleigh scattering-based distributed fiber sensors," Advanced devices & instrumentation, 2021.

[5] A. Usman, N. Zulkifli, M. R. Salim, K. Khairi, A. I. Azmi, "Optical link monitoring in fibre-to-the-x passive optical network (FTTx PON): A comprehensive survey," Optical Switching and Networking, vol. 39, 2020, pp. 100-107.

[6] X. Pan, X. Wang, B. Tian, C. Wang, H. Zhang and M. Guizani, "Machine-learning-aided optical fiber communication system," IEEE Network, vol. 35, 2021, pp. 136-142.

[7] C. Zeng, J. Zhang, R. Wang, B. Zhang, and Y. Ji, "Multiple attention mechanisms-driven component fault location in optical networks with network-wide monitoring data," J. Opt. Commun. Netw., vol. 15, 2023, pp. C9-C19.

[8] O. Karandin, O. Ayoub, F. Musumeci, Y. Hirota, Y. Awaji and M. Tornatore, "If not here, there. explaining machine learning models for fault localization in optical networks," presented at Optical Network Design and Modeling (ONDM), Warsaw, Poland, 2022, pp. 1-3.

[9] H. Song, R. Lin, Y. Li, Q. Lei, Y. Zhao, L. Wosinska, P. Monti, and J. Zhang, "Machine-learning-based method for fiber-bending eavesdropping detection," Opt. Lett., vol.48, 2023, pp. 3183-3186