Detection of abnormal activities on a SM or MM fiber

Stefan Karlsson[1], Mikael Andersson[2], Rui Lin[3], Lena Wosinska[3], Paolo Monti[3]
[1] *Swedish Defense Material Administration, Linköping, Sweden*
[2] *Micropol Fiberoptics, Åled, Sweden*
[3] *Electrical Engineering, Chalmers University of Technology, Göteborg, Sweden*

stefan.karlsson@fmv.se

Abstract: We demonstrate eavesdrop detection based on polarization signatures by analyzing polarization state changes at the receiver. We identify changes related to the normal operation and the ones caused by eavesdropping.

1. INTRODUCTION

Fiber optical based infrastructures are today carrying high traffic volumes using both multimode and singe mode fibers. The threat from sabotage leading to disruption of the transmitted data may seriously affect the information society of today. The threat from eavesdropping or changing critical and secure information is also existing and well known. In our recent work [1] we showed that optical fiber can be easily eavesdropped without detection based on of monitoring the optical power level at the receiver. Dependent on technology of taping out light from the fiber a successful eavesdrop can be made along the fiber at up to a certain distance from the transmitter. This leads to a serious security threat to fiber optical installations. Therefore, it's important to detect abnormal activities exposed to a fiber optical installation.

Consider Bob and Alice who are connected over an optical fiber and Eve who is eavesdropping the transmitted information. Eve can make the eavesdrop by peeling off the protective layers of the optical cable and couple out the light by for example bending the fiber in a certain angle and bending radius, as in Fig. 1(a).

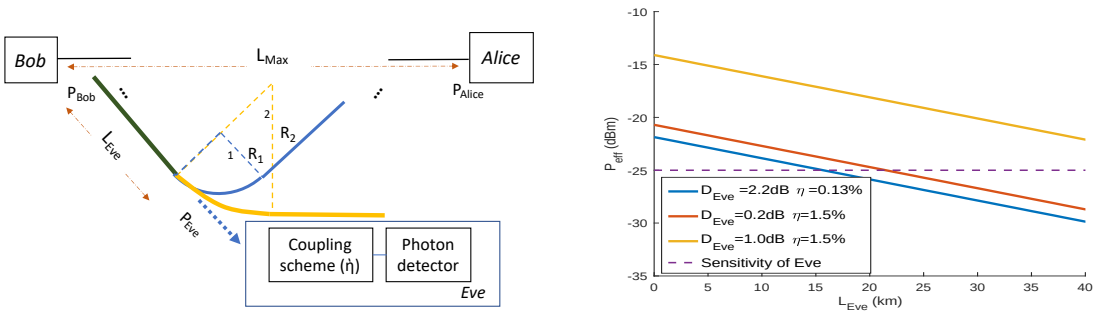


Fig. 1. (a) tapping bending the fiber (b) introduced attenuation and efficiency of, e.g., 1.5%

Figure 1(b) is showing the eavesdropped optical power at the photon detector in figure 1(b) measured in dBm. The sensitivity limit for Eve is -25 dBm, including an optical amplification factor of 11 dB, as described in resent work [1]. On the X-axes is shown the distance from the optical transmitter. Eve are able to eavesdrop at a distance from the transmitter where the eavesdropped optical power are higher than the sensitivity limit. Eve must invent technology for the fiber bending and detection of the out coupled light. This process will results in an efficiency of tapping the transmitted signal. For example, the 1.5% efficiency can lead to e.g., 0.2 dB attenuation, but if the skills of the Eve are low it can also can lead to 1.0 dB attenuation (see Fig. 1 (b)). Consider a transmission example of 40 km as described in paper [1]. Eve can eavesdrop at a distance up to 20 km from the transmitter with introduced attenuation below the resolution from an OTDR as shown in Fig. 1(b) (red line).

Interconnects inside data centers are often based on multimode OM3 or bend insensitive G.657 fibers. Fiber installations over long distances are normally based on single mode G.652 or G.657 fibers. This demonstration will focus on detection of abnormal activities performed on both multimode and single mode fibers.

2. OVERVIEW OF DEMONSTRATION

This demonstration shows a proof of concept to recognize abnormal activities along the fiber that can be originating from tapping out light from an optical fiber. The demonstration begins with a theoretical background on detecting abnormal activities on multimode (MM) and single mode (SM) fibers. In order to detect and prevent possible sabotage or eavesdropping, abnormal signatures caused by tapping attempts or activities threatening the optical fiber shall cause an alarm alerting the system owner. Example of signatures from abnormal activities will be shown and compared to normal signatures along the fiber. The normal signatures must not generate any false alarms in order to avoid unnecessary preventive actions.

3. INNOVATION

By monitoring the polarization state and making a frequency transform for analyzing the signature with respect to time, many signatures can be classified. Normal changes in the polarization state can be analyzed and compared to abnormal activities such as eavesdropping of information. This comparison will form a base for anomaly detection and for rising an alarm, leading to, e.g., interruption of the transmission. In this way the eavesdropping of sensitive information can be avoided. Figure 2 shows example of a normal signature and an abnormal signature

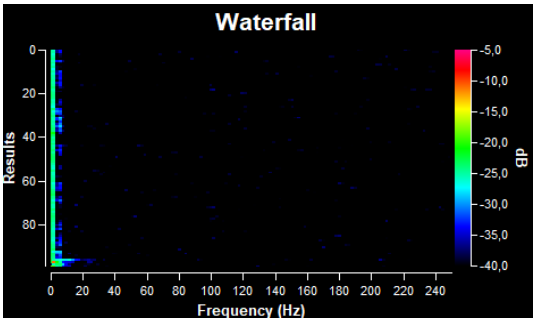
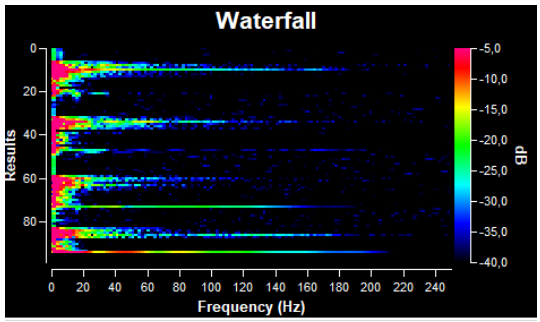


Fig.2 (a) signature from relaxed fiber



(b) lifting the fiber four times with a 60 degree bend angle

Figure 2 shows the frequency analyze with respect to time on the Y-axes and signal strength from -5 dB to -40 dB.

4. DEMO CONTENT & IMPLEMENTATION SECTION

The demonstration will include the following parts.

A. Architecture

The demonstration is based on a proof of concept to detect changes in the Poincare sphere that generates signatures related to specific activities along the fiber.
One activity that generates a specific signature is an attempt to couple out light from the fiber.
Given: a certain efficiency of coupling out light and at the same time not causing a significant decrease in received optical power. The decrease in optical power should be within the resolution of an OTDR. This will then not be detectable by monitoring the power level.
The demonstration will show a signature based on polarization state to identify an attempt of coupling out light, which is significantly different from polarization changes caused by other activities.

B. Experimental set up

The demonstration will show how a clip on device can couple out enough optical power to detect a 10 Gbps information signal.
The experiment will use a laptop computer connected to an experimental set up installed in a transportable box. The box will be connected to a fiber cable with G.657 fiber and also a bare G657 fiber lying on a table.
The fiber cable and bare G657 fiber will lifted and bent to couple out optical power. At the same time the signatures will be presented on the screen of the laptop. A clip-on device will be put directly on the bare G.657 fiber and the generated signature will be presented.
Normal signatures appearing in a real life installation will be introduced by a specific vibrations on the fiber and separated from signatures from the clip on device.
Attendees of the demonstration will have the possibility to handle the fiber cable and bare fiber to explore the different signatures.

5. OFC RELEVANCE

This demonstration will be the first to showcase a proof-of-concept for eavesdrop detection based on changes in the fiber polarization signature. The broad security topic and this specific study focusing on the fiber infrastructure, are very relevant to an OFC's audience, both from academia and the industry. The attendees will have first-hand experience handling fibers and see their action's effects on the polarization in real-time. This highly interactive setup was thought to foster discussions and possibly trigger new ideas and develop this concept even further.

Acknowledgements:
This work has been supported by CELTIC-NEXT AI-NET-PROTECT, Swedish Defence Material Administration and Micropol Fiberoptics

References

[1] S.Karlsson, R.Lin, L.Wosinska, P.Monti “Eavesdropping G.652 vs. G.657 fibres: a performance comparison”, ONDM2022.