Long-term Perimeter Protection System Monitoring Using State of a Polarization Analyzer

1st Adrian Tomasov  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
tomasov@vutbr.cz

2nd Petr Dejdar  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
Petr.Dejdar@vut.cz

3rd Pavel Záviška  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
Pavel.Zaviska@vut.cz

4th Vladimir Spurny  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
xspurn07@vutbr.cz

5th Petr Munster  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
munster@vut.cz

6th Tomas Horvath  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
horvath@vut.cz

7th Ondrej Klicnik  
Dept. of Telecommunications  
Brno University of Technology  
Brno, Czech Republic  
xklicn02@vutbr.cz

Abstract—The paper proposes the deployment of a perimeter and data protection system with long-term data storage in an InfluxDB time-series database enhanced by a graphical interface based on a Grafana dashboard. The perimeter is protected using a fiber optic cable, and the transmitted light is analyzed by a state of polarization analyzer detecting mechanical vibrations. Using a simple spectrum comparison method and a threshold, it can detect a perimeter breach and generate an alert.

Index Terms—information security, optical polarization, perimeter protection, vibration detection

I. INTRODUCTION

Fiber optics technology gathers many advances year by year and indeed becoming the sole communication solution for wide area networks (WAN) or local area networks (LAN), and distribution networks (e.g., passive optical networks), mainly due to their transmission throughput and achievable distance. The considerable benefit of the fiber optic networks is allowing updating the optical transceivers for the new faster ones, while the optical paths remain the same. Thanks to a dense wavelength division multiplexing (DWDM) [1] or flexi-grid in elastic optical networks (EON) [2], many optical transceivers can utilize a single optical path and achieve aggregated throughput up to tens of Terabits per second [3].

The fiber itself has more usage than just a transmission medium. There are many point and distributed sensory systems based on the analysis of transmitted light, which may change its physical attributes, such as frequency, phase, or polarization. The current use cases for optical sensors are mechanical or acoustic vibration analysis using Distributed Acoustic Sensing (DAS) [4], temperature sensing with the help of Brillouin Optical Time Domain Reflectometry (BOTDR) [5], or temperature sensing in biomedical applications using state of the art Fiber Bragg gratings (FBG) [6]–[8]. At the same time, there is testing of sensing systems for a large range of applications from perimeter security [9], [10], pipeline industry [11], nuclear facilities [12], biomedical [13] and many other industries.

However, the fiber-optic paths are not resistant to eavesdropping attacks. There are various ways to wiretap transmitted communication, such as V-groove, fiber bending, splitter insertion, FBG, and others [14], [15]. Another possibility is to eavesdrop on human speech near fiber cable by analyzing phase variations of the back-reflected light [16].

There are already various proposed solutions for eavesdropping and abnormal event detection. The quality of the communication channel between optical transceivers can be expressed using an eye diagram, which includes parameters such as jitter, signal-to-noise ratio, or distortion. The abnormal behavior of these parameters may indicate a potential attack on the optical path. Thus, the eye diagram is analyzed by a convolutional neural network and detects possible eavesdropping attempts [17]. Another option is to analyze the network using Optical Time Domain Reflectometer (OTDR) and analyze its output using convolution or recurrent neural networks [18], [19].

The paper proposes a long-term perimeter and data protection monitoring system on a fiber optic path. The optical sensor is based on our ongoing research of the fast state of polarization change analyzer and experimental anomaly detection methods [20], [21]. The sensor can detect mechanical and loud acoustic vibrations based on the polarization change of the transmitted light caused by fiber manipulation by an attacker or an unauthorized person entering a protected perimeter [22]. This output is captured and analyzed using Raspberry Pi (RPi), and the results are sent into a database running in a cloud environment. The deployment also contains a graphical user interface for data visualization, allowing an
anomaly threshold modification and set email alerts if the perimeter is breached or data security is potentially violated.

II. MONITORING SYSTEM PROPOSAL

The proposed system consists of an optical sensory system with data acquisition and software processing parts, running in an optional environment such as a cloud, bare metal server, or sensor controller.

The hardware part of the perimeter protection system is based on a cost-effective solution analyzing a state of polarization change of transmitted light through the protected fiber path. It can detect mechanical vibrations, including walking on a protected perimeter, fiber manipulation, and others [20]. All vibrations cause tiny differences in the fiber structure and consequently change the transmitted light polarization due to birefringence [23]. The analyzer diagram is shown in Figure 2, where the main components are a polarization beam splitter, and a Koheron LPD 100 balanced photo-detector [24] with a built-in 1550 nm laser. The analyzed fiber segment consists of a common patch cord with G.652D single-mode fiber.

The output is sampled using a Raspberry Pi with an audio card, and the processed data are stored in a time-series database, as shown in Figure 1. All of these components are further described in the following subsections.

A. Signal processing

The analog signal is sampled by a USB audio card connected to RPi [25]. It uses a sampling rate of 8000 samples per second, which is high enough to detect requisite frequencies within the range of 20 to 250 Hz. The incoming signal is divided into overlapping segments of length 4096 samples and a stride\(^1\) of 2048 samples. The individual segments are multiplied with a Hamming window of the corresponding length, and converted into a frequency domain using a single-sided real-valued Discrete Fourier Transform. The spectrum is normalized by subtracting its mean value and then analyzed by comparing means of the bottom and the upper portions of the spectrum, which reduces the signal strength by noise. The whole operation is shown in Eq. (1):

\[
\text{DIFF}(x, p) = \frac{1}{L} \sum_{i=1}^{L} x_i - \frac{1}{N-L} \sum_{i=L}^{N} x_i,
\]

where \(x \in \mathbb{R}^N\) is a magnitude spectrum vector, \(p\) is a number within the range 0 to 1 defining a portion of the lower spectrum part, \(N\) is the number of samples in a single window, and it holds that \(L = N \cdot p\). The output of this function is compared against the threshold to detect potential perimeter breaches. The higher the output, the more intensive is the intensity of vibrations.

Both portion and threshold parameters are considered as hyper-parameters of the function. The optimal values are evaluated using a grid-search algorithm optimizing the highest accuracy in the anomaly detection occurrences. Furthermore,

\(^1\)The stride parameter represents the number of samples by which the window shifts.
the threshold parameter should be fine-tuned for each specific deployment based on location. The optimal values can be found in a testing measurement, where the threshold is set to a maximal achievable value by Eq. (1) or a $99^{th}$ quantile of the equation output.

B. Long-term monitoring

The output of the signal processing function is sent into a long-term monitoring system consisting of InfluxDB [26] time series database and Grafana [27] system for graphical representation of stored data. InfluxDB is optimized for time series data from many sources by allowing storing data in several separate tables. Furthermore, it allows distinguishing data in the same tables using tags. Our proposed system uses these to differentiate between various deployed perimeter protection systems.

Another key attribute of InfluxDB is the possibility to aggregate/interpolate requested data using mathematical functions (e.g., mean) to reduce data request size, which is very useful, particularly in requests with very long time ranges (e.g., months, years).

All data stored in the database are graphically shown in charts using the Grafana platform. Grafana is an open-source, user-friendly project for real-time charts and similar system monitoring tools. It has a native integration with many data sources, including InfluxDB. Many different charts in Grafana allow the creation of many advanced system monitoring dashboards. This proposal uses a simple time-series chart enhanced with a threshold to decide whether the signal is nominal or abnormal. Furthermore, if the threshold is exceeded, it generates an email alert to a responsible person.

InfluxDB and Grafana are standalone services that can run in a cloud environment or any possible Linux based system. The only requirement is network visibility because they use a representational state transfer application interface (RestAPI) for communication. However, the cloud deployment option is preferred because it can utilize and store data for more sensory systems in one place.

The whole deployment proposal is shown in Figure 1, where ADC stands for analog-digital converter, DSP is digital signal processing, ETH is ethernet, Rest API stands for representational state transfer application interface, and HTTPS abbreviation means hypertext transfer protocol secure.

### III. Implemented Results

The core program responsible for sampling, data processing, and writing to the database in RPi is written in python3 with third-party opensource libraries, such as numpy for signal processing, influxdb-client for database communication, and last but not least, soundcard for simple data sampling from the audio card. It automatically starts on system start-up using a SystemD service and runs in an infinite loop.

InfluxDB and Grafana are installed into a virtual machine with an assigned public IP address secured by a firewall. Furthermore, both services use certbot [28] program to request a valid certificate inside the public key infrastructure (PKI), which allows using trusted connections between them and users. It creates a trustworthy channel for the following password authentication.

The hardware part of the proposed system is deployed in a test laboratory with fiber optics cable installed in ceilings. It should detect anyone opening the door and entering the room. Figure 4 shows the fiber path and the laboratory itself. Figure 3 shows a time-series chart from the Grafana dashboard containing the difference of spectrum means, as is defined in Equation (1), represented by a green line and threshold line drawn by a red color with the abnormal red highlighted region. There are three visible abnormal events, the first is door closure, and the second is fiber manipulation. All these events generated alerts and sent them to a desired e-mail address.

Furthermore, a specific tag is added to a database write request to distinguish the data from this specific instance.

### IV. Conclusion

The paper describes deploying a cost-effective perimeter and fiber protection system with all required monitoring software.
in a real-life scenario. The hardware part is based on the state of the polarization analyzer and a Raspberry Pi with an audio card for analog data sampling and processing. The potential security breach in the protected perimeter is detected using our ongoing research’s simple spectrum comparison method. The results are stored in the InfluxDB time-series database for long-term monitoring. These data are displayed by line charts using the Grafana web application, which compares the data against a defined threshold. Additionally, the application can send an e-mail alert if the output, if comparison, exceeds the defined threshold.

Future work will focus on adapting this deployment proposal to classification problems based on neural networks. They require more computational power to run a neural network model; thus, the RPi is unsuitable. Also, their output is more complex, which is a vector of probabilities for each classification class. Another critical part is the graphical representation of these vectors together with class counters and similar.

ACKNOWLEDGMENT

Research described in this paper was supported by the Ministry of the Interior of the Czech Republic, program IMPAKT1, under grant VJ01010035, project “Security risks of photonic communication networks”.

REFERENCES


