Implementing and testing a fiber-optic polarization-based intrusion detection system

Rasha El Hajj
Gregory MacDonald
Pramode Verma
Robert Huck

Implementing and testing a fiber-optic polarization-based intrusion detection system

Rasha El Hajj, Gregory MacDonald, Pramode Verma,* and Robert Huck
University of Oklahoma-Tulsa, School of Electrical and Computer Engineering, Telecommunications Engineering Program, 4502 East 41st Street, Tulsa, Oklahoma 74135, United States

Abstract. We describe a layer-1-based intrusion detection system for fiber-optic–based networks. Layer-1-based intrusion detection represents a significant elevation in security as it prohibits an adversary from obtaining information in the first place (no cryptanalysis is possible). We describe the experimental setup of the intrusion detection system, which is based on monitoring the behavior of certain attributes of light both in unperturbed and perturbed optical fiber links. The system was tested with optical fiber links of various lengths and types, under different environmental conditions, and under changes in fiber geometry similar to what is experienced during tapping activity. Comparison of the results for perturbed and unperturbed links has shown that the state of polarization is more sensitive to intrusion activity than the degree of polarization or power of the received light. The testing was conducted in a simulated telecommunication network environment that included both underground and aerial links. The links were monitored for intrusion activity. Attempts to tap the link were easily detected with no apparent degradation in the visual quality of the real-time surveillance video. [DOI: 10.1117/1.OE.54.9.096107]

1 Introduction

The world is transitioning to an information-based society. Information represents a "wealth" component of such a society. As such, it is important to protect this wealth from unauthorized accesses and unauthorized entities. This is equally important for data at rest and for data in transit.

Fiber-based optical networks are the primary mode of transmitting data. While information leakage can be prevented through the use of encryption, all contemporary forms of encryption are only computationally secure. Given enough computational power, a cryptanalyst can recover the original information. The detection and prevention of eavesdropping/tapping activity in fiber-based optical networks represents an elevation in security, as it prevents the adversary from obtaining information in the first place.

Intrusion is not limited to criminal intent. One well-publicized intrusion occurred in October 2013. Leaked documents indicating that the U.S. National Security Agency (NSA) infiltrated Yahoo and Google data centers captured the attention of the public. The NSA and its British counterpart tapped optical fiber cables connecting Google's and Yahoo's worldwide data centers.[1]

The system described in this paper is a countermeasure to fiber-optic tapping activity. The state of polarization is extremely sensitive to changes in fiber geometry. Tapping activity necessarily involves changes to fiber geometry.

Previous research includes fiber-based sensor networks for perimeter protection using Mach–Zehnder Sagnac interferometers,[2] fiber Bragg grating sensors,[3] and polarization optical time domain reflectometry (POTDR) sensing devices.[4] Perimeter protection may involve fiber-optic meshes on fences

for protection of sensitive areas, mats in museums, and the protection of railway assets. POTDR devices depend on polarization variations but do not measure the state of polarization directly. Instead, it converts polarization variations into power fluctuations that can be detected on POTDR traces.

This paper is organized as follows. In Sec. 2, the polarization properties of light (as they relate to this paper) are briefly described. In Sec. 3, fiber-optic tapping methods are reviewed. The theory behind the intrusion detection system, the experimental setup, and the results are addressed in Sec. 4. The application of the polarization-based intrusion detection system to a simulated telecommunications network is presented in Sec. 5. In Sec. 6, possible future work is discussed. Section 7 concludes the paper.

2 Polarization Properties of Light

This section describes the polarization properties of light as they relate to this paper. By convention, the direction of the electric field is used to define the polarization of the light. The electric field can be represented as

$$
\begin{aligned}
\vec{E}(\vec{r}, t) = {} & E_{0x} \cos(\vec{k} \cdot \vec{r} - \omega t + \varnothing_x)\hat{x} \\
& + E_{0y} \cos(\vec{k} \cdot \vec{r} - \omega t + \varnothing_y)\hat{y},
\end{aligned}
\tag{1}
$$

where $\hat{x}$ and $\hat{y}$ are the directions of the two orthogonal components of the electric field, $\vec{k}$ is the wave vector, $\varnothing$ is the phase angle, ω is the angular frequency, E_{0x} and E_{0y} are the amplitudes of the orthogonal components of the electric field.[5]

An alternate way of describing the state of polarization is in terms of the Stokes parameters (S_1, S_2, and S_3) and their mapping onto the Poincare sphere.[6] Each point on the

*Address all correspondence to: Pramode Verma, E-mail: pverma@ou.edu

Table 1 Stokes vector of common states of polarization.

LHP	LVP	RCP	LCP	Unpolarized
$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Poincare sphere represents a unique state of polarization.[7] The points on the surface of the sphere represent fully polarized light, while the points interior to the sphere represent partially polarized light.

The four Stokes parameters are defined in terms of the electric field components:[8]

$$S_0 = E_{0x}^2 + E_{0y}^2,$$

$$S_1 = E_{0x}^2 - E_{0y}^2,$$

$$S_2 = 2E_{0x}E_{0y} \cos \delta, \quad \text{where } \delta = \varnothing_y - \varnothing_x,$$

$$S_3 = 2E_{0x}E_{0y} \sin \delta,$$

$$S_0^2 = S_1^2 + S_2^2 + S_3^2,$$

where S_0 is the total intensity of light, S_1 is the amount of linear horizontal or vertical polarization, S_2 is the amount of linear +45 deg or −45 deg polarization, and S_3 is the amount of right or left circular polarization.[9] The Stokes parameters are real quantities and can be experimentally measured. Examples of various states of polarization and their representation in Stokes space (S_0, S_1, S_2, and S_3) are shown in Table 1.

3 Fiber-Optic Tapping Methods

This section lists the fiber-optic tapping methods and the current countermeasures. It should be noted that all these tapping methods require access to the fiber and removal of the outer jacket. This activity necessarily involves perturbations of the fiber cable.

Tapping methods can be divided into three categories:[10]

- Fiber bending: light is coupled out of the core when the bend radius reaches a critical angle. At this angle, some portion of the light is emitted from the core and is detected by an optical detector.
- Splitter or coupler: the original path is cut and a splitter or coupler is inserted. Cutting the original path can be easily detected because it interrupts the data flow.
- Scattering: a fiber Bragg grating is etched to the core and part of the light is scattered outside the core and then detected by an optical detector.

Whatever the reason behind tapping optical fiber cables (criminal or otherwise), certain measures should be taken to secure sensitive networks.[11] One countermeasure is to encase the fiber cable in cement, which prevents unauthorized access to the optical fiber cable. A second countermeasure is to install the fiber cable in a pressurized conduit, which generates alerts when pressure fluctuations occur. A third countermeasure is the continuous surveillance of the entire optical fiber link, which detects any unauthorized access to the fiber.

4 Intrusion Detection System

While Sec. 3 described the current countermeasures to fiber-optic tapping, this section presents a countermeasure based on monitoring the state of polarization. Polarization is extremely sensitive to any physical change in the fiber. Fiber geometry is necessarily altered during the placement of optical taps, and this affects the stability of polarization in the fiber. The theory behind this countermeasure, the experimental setup, and the results of the tests performed are addressed in detail in the following subsections.

4.1 Theory

In Ref. 12, the author investigated the properties of light as a means of insuring the integrity and security of the physical layer of a fiber-optic–based communication link. Specifically, the author focused on the behavior of polarization in a single-mode fiber, as it is shown to be especially sensitive to fiber geometry and to changing environmental conditions. Accordingly, we posit that the state of polarization (as represented in Stokes space) is more sensitive to environmental conditions than either the degree of polarization or the received power (S_0).

Recall that the degree of polarization is represented as $\text{DOP} = (\sqrt{S_1^2 + S_2^2 + S_3^2}/S_0)$. Given negligible changes in DOP and S_0, a change in one Stokes parameter necessitates a change in at least one other Stokes parameter (unless there is a sign change in a single parameter). From a practical standpoint, this last case is observed only under controlled conditions. What is usually observed are the changes in S_1, S_2, and S_3. Furthermore, "small" changes over time are usually due to changing environmental conditions, while "large" changes are due to fiber perturbations.

Here, we regard polarization measurements as sampled points from a continuous function. In time series analysis, a common preprocessing step is to remove any trend in the data by taking the first-differences of the sampled points. The resulting time series of first-differences can often be regarded as a stationary process. The presence of "large" first-differences in the time series of first-differences is interpreted as being generated by a mechanism that is somehow different from the generating mechanism behind "small" first-differences. We interpret the former as arising from fiber perturbations and the latter as arising from changing environmental conditions. We approach the problem of detecting fiber perturbations as a time-series anomaly-detection problem.

Many techniques exist for detecting anomalous events. A few include (1) from ordinary statistics, the kurtosis of the distribution of first-differences, (2) from spatial statistics, the Hopkins metric for identifying cluster formation,[13] and (3) from machine learning, one-class support vector machines. In this paper, we employ the use of extreme value theory (EVT) for detecting anomalous events.

EVT has the advantage of being able to adapt to changing environmental conditions and encapsulating varying notions of "unusualness" (degrees of anomalous behavior). Essentially, we use EVT to characterize the first-difference

behavior of unperturbed fiber, so that the first-differences produced by perturbations can be identified probabilistically.

EVT employs two main approaches:[14] peak over threshold model and block maxima model. Block maxima model, used in this work, uses the maximum occurring data value from each block (a contiguous set of first-differences) without regard to preset thresholds. EVT essentially addresses the following question: What is the probability of observing some quantity that is more extreme than any quantity so far observed? We do not explain EVT here but later make references to "sensitivity threshold." This phrase refers to the magnitude of first-differences that are likely to be observed only under rare circumstances (fiber perturbations) as determined by the EVT block maximum method. (EVT-suggested threshold in terms of normalized Stokes parameters was 0.05.)

4.2 Experimental Setup

Section 4.1 presented the fundamental components of the intrusion detection system. This section describes the implementation of the system. The system was tested in the Quantum Optics Lab at OU-Tulsa, where the surrounding temperature is around 65°F. In the conducted experiment, depicted in Fig. 1, the following hardware and software were used:

- Polarization analyzer: Agilent 8509C lightwave polarization analyzer offers high-speed, calibrated polarization measurements of optical signals and components. For the purpose of the experiment, it was used to measure the state of polarization, represented by the Stokes parameters, the degree of polarization, and the power.

- Optical fiber: Single-mode optical fiber with FC connectors on both ends was used in the experiment. The system was also tested with multimode optical fiber with FC connectors. The operating wavelength was 1550 nm.

- LabVIEW controller: LabVIEW 10.0.1 was used to build the implementation procedure and driver program. LabVIEW communicated with the Agilent 8509C lightwave polarization analyzer. It also saved the collected measurements in a text file for further processing.

The degree of polarization, power, and state of polarization of the received light were measured. The LabVIEW controller and driver generated a text file that included the following (Fig. 2):

SeqNumber, Timestamp, LinkStatus, Power, S_1, S_2, S_3, DegreeOfPolarization, HeartbeatInterval, FutureUse1, FutureUse2

- Sequence number: helps to identify missing measurements.

- Timestamp: the time and date at which the measurement is made. The time is in the 24-h format.

- Link status: OK, Intrusion, and Suspicious: link status depends on the first-differences of the Stokes parameters. If the first-differences of S_1, S_2, and S_3 are below the sensitivity threshold, link status is OK. If they are all above the threshold, it is intrusion. In the other cases, the link status is suspicious.

- Measured raw data: power of the received signal, the state of polarization in terms of the Stokes parameters (S_1, S_2, and S_3), and the degree of polarization.
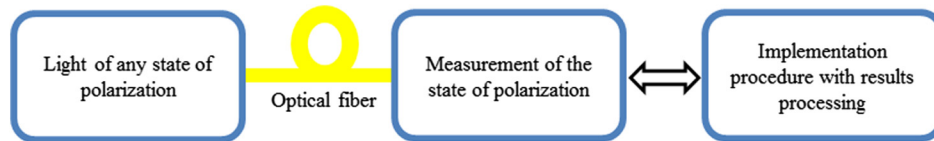

Fig. 1 Schematic diagram of polarization-based intrusion detection system consists of: Agilent 8509C lightwave polarization analyzer which measures the state of polarization, the degree of polarization, and the power, LabVIEW 10.0.1 that controls the experiment and collects the measured data, and optical fiber with FC connectors on both ends.

```
20,10:00:47 9/15/2014,OK,4.312181E-05mW,-.9642598,.1602537,-.1817518,.9942394,5s,futureuse1,futureuse2
21,10:00:49 9/15/2014,OK,4.312107E-05mW,-.9640558,.1594267,-.1821155,.9939751,5s,futureuse1,futureuse2
22,10:00:52 9/15/2014,OK,4.310184E-05mW,-.9638325,.1606475,-.181856,.9939076,5s,futureuse1,futureuse2
23,10:00:54 9/15/2014,OK,4.309892E-05mW,-.9639255,.1611923,-.1805002,.9938387,5s,futureuse1,futureuse2
24,10:00:56 9/15/2014,OK,4.312029E-05mW,-.9640692,.1605127,-.1813008,.994014,5s,futureuse1,futureuse2
25,10:00:58 9/15/2014,OK,4.313569E-05mW,-.9647786,.1584617,-.1806245,.99425,5s,futureuse1,futureuse2
26,10:01:01 9/15/2014,OK,4.310966E-05mW,-.9643043,.1600006,-.1807907,.9940665,5s,futureuse1,futureuse2
27,10:01:03 9/15/2014,OK,4.312015E-05mW,-.9645903,.1601306,-.1810278,.9944081,5s,futureuse1,futureuse2
28,10:01:05 9/15/2014,OK,4.311911E-05mW,-.9635097,.1608307,-.1811701,.9934989,5s,futureuse1,futureuse2
29,10:01:08 9/15/2014,OK,4.312312E-05mW,-.9643953,.1608168,-.1803,.9941974,5s,futureuse1,futureuse2
30,10:01:10 9/15/2014,OK,4.311878E-05mW,-.9637945,.1611042,-.1802603,.993654,5s,futureuse1,futureuse2
31,10:01:12 9/15/2014,OK,4.3143E-05mW,-.9640971,.1594487,-.181045,.9938232,5s,futureuse1,futureuse2
32,10:01:15 9/15/2014,OK,4.31442E-05mW,-.9645333,.1588815,-.1819154,.9943144,5s,futureuse1,futureuse2
33,10:01:17 9/15/2014,OK,4.313379E-05mW,-.963989,.1606798,-.1809573,.9939006,5s,futureuse1,futureuse2
34,10:01:19 9/15/2014,OK,4.314482E-05mW,-.9642271,.1593157,-.1807891,.9938813,5s,futureuse1,futureuse2
35,10:01:22 9/15/2014,OK,4.313351E-05mW,-.9639977,.1599554,-.1809125,.993784,5s,futureuse1,futureuse2
36,10:01:24 9/15/2014,OK,4.314826E-05mW,-.964191,.1592727,-.1808593,.9938522,5s,futureuse1,futureuse2
37,10:01:26 9/15/2014,OK,4.312597E-05mW,-.9645693,.1600896,-.1808089,.9943413,5s,futureuse1,futureuse2
38,10:01:28 9/15/2014,OK,4.312447E-05mW,-.9642321,.1597496,-.1805179,.9939066,5s,futureuse1,futureuse2
39,10:01:31 9/15/2014,OK,4.314412E-05mW,-.9638712,.1599187,-.1802871,.9935417,5s,futureuse1,futureuse2
40,10:01:33 9/15/2014,OK,4.312131E-05mW,-.9652541,.158798,-.179218,.9945105,5s,futureuse1,futureuse2
41,10:01:35 9/15/2014,OK,4.314331E-05mW,-.9640119,.1600732,-.1792498,.9935154,5s,futureuse1,futureuse2
42,10:01:38 9/15/2014,OK,4.315595E-05mW,-.9641436,.1595142,-.1800317,.9936947,5s,futureuse1,futureuse2
43,10:01:40 9/15/2014,OK,4.311647E-05mW,-.9645304,.1588167,-.1794175,.9938473,5s,futureuse1,futureuse2
44,10:01:42 9/15/2014,OK,4.311786E-05mW,-.9642872,.1599119,-.1796924,.9938364,5s,futureuse1,futureuse2
45,10:01:45 9/15/2014,OK,4.312738E-05mW,-.964204,.1589892,-.1815305,.9939418,5s,futureuse1,futureuse2
```

Fig. 2 Sample text file of collected measurements.

- Heartbeat interval: the time interval after which the file is updated (in seconds).

Two extra fields were reserved for any possible future use.

4.3 *Results*

The intrusion detection system was tested under a variety of scenarios. The results of those tests are presented in this section. The system was tested with a 10-km unperturbed single-mode fiber. For the unperturbed fiber, Stokes parameters, degree of polarization, and power were relatively stable. The first-differences of the Stokes parameters were relatively stable as well and did not exceed the EVT suggested sensitivity threshold. For this same unperturbed fiber, the input polarization state was modified using the Agilent 8169A polarization controller. As expected, the change in the input polarization state resulted in a significant change in the received state of polarization but with negligible differences in the degree of polarization and power values. Furthermore, the time-evolving Stokes parameters and their first-differences were relatively stable and did not exceed the sensitivity threshold.

Simulation of changing environmental conditions (specifically, minor vibrational fluctuations and temperature variations) led to gradual changes in the values of the Stokes parameters. The resulting trajectory on the Poincare sphere traced out by the changing Stokes parameters tended to be more organized. However, first-differences of the Stokes parameters were relatively stable and did not exceed the sensitivity threshold. This suggests that the intrusion system is robust against changing environmental conditions, namely occasional vibration and temperature. (Vibrational stimuli were applied by affixing the fiber cable to cell phone set on vibrate mode. The vibration stimuli had a frequency of 180 Hz and $[-0.08, +0.08]$ g. Temperature fluctuations were induced using a heating element in close proximity to the fiber cable. The applied external heat was in the range of 1500 to 1800 W, which resulted in a temperature of $[70, 130]°$F.)

The system was tested with single-mode fiber for 24 h with occasional variations in temperature, vibration, and perturbation. The resulting measurements were plotted and are shown in Fig. 3. The system was tested with the following alterations:

- At interval 3141 to 3378, external heat was applied to the fiber. This resulted in a change in the values of S_1, S_2, and S_3. However, the first-differences were stable below the sensitivity threshold.
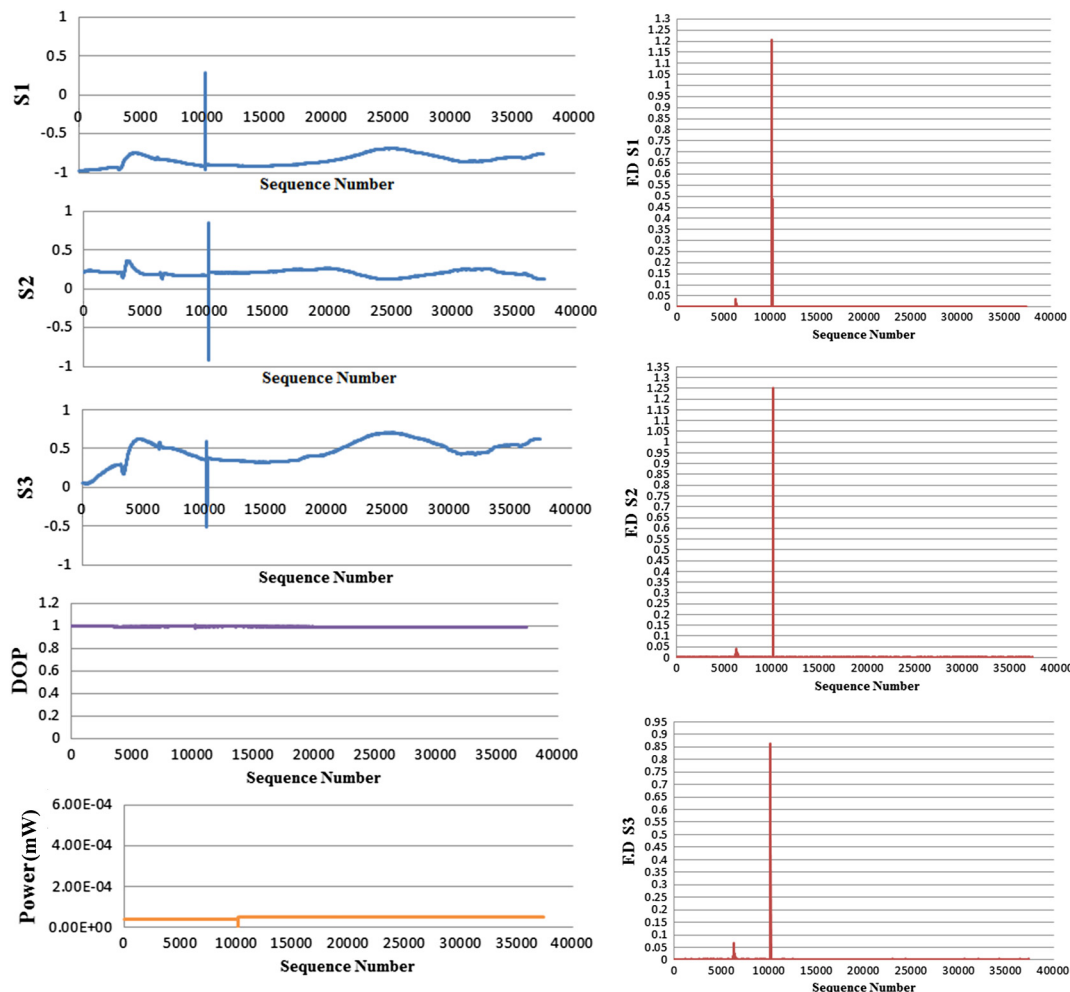

Fig. 3 Results of single-mode fiber with occasional alterations.

- At interval 6235 to 6490, the fiber was subjected to external vibration. There was a smooth change in the values of the Stokes parameters and only the first-difference of S_3 exceeded the threshold. In both intervals, the power and the degree of polarization were stable and did not reflect the external alterations.
- At interval 10178 to 10203, the fiber was bent. This event can be clearly seen in the values of S_1, S_2, and S_3 that showed an abrupt change. Also, the magnitude of the first-differences for all Stokes parameters far exceeded the sensitivity threshold, suggesting a different generating process. Only negligible changes in the degree of polarization and power were observed.

For a 5-m single-mode fiber, the system was tested with the following alterations:

- At interval 130 to 157, vibration was applied.
- At interval 262 to 310, external heat was applied.
- At interval 391 to 416, the fiber was bent.

The results of the 5-m single-mode fiber, displayed in Fig. 4, were consistent with the results obtained in the previous case. The intrusion system was robust against changing environmental conditions. The Stokes parameters experienced an abrupt change when the fiber was bent. The magnitude of the first-differences for all Stokes parameters far exceeded the sensitivity threshold. Again, only negligible changes in the degree of polarization and power were observed.

The same procedure that was applied for the single-mode fiber was repeated for a 5-m multimode fiber (Fig. 5). The system was tested with the following alterations:

- At interval 130 to 155, external vibration was applied to the fiber. S_1, S_2, and S_3 slightly changed and their first-differences remained below the threshold. Degree of polarization and power experienced negligible change.
- At interval 260 to 285, the fiber was subjected to applied heat. This resulted in a change in the values of S_1, S_2, and S_3. Although the first-differences of some measurements in this interval exceeded the sensitivity threshold, not all three first-differences exceeded the sensitivity threshold simultaneously. These two events suggest that the intrusion system is robust against environmental conditions when using multimode fiber.
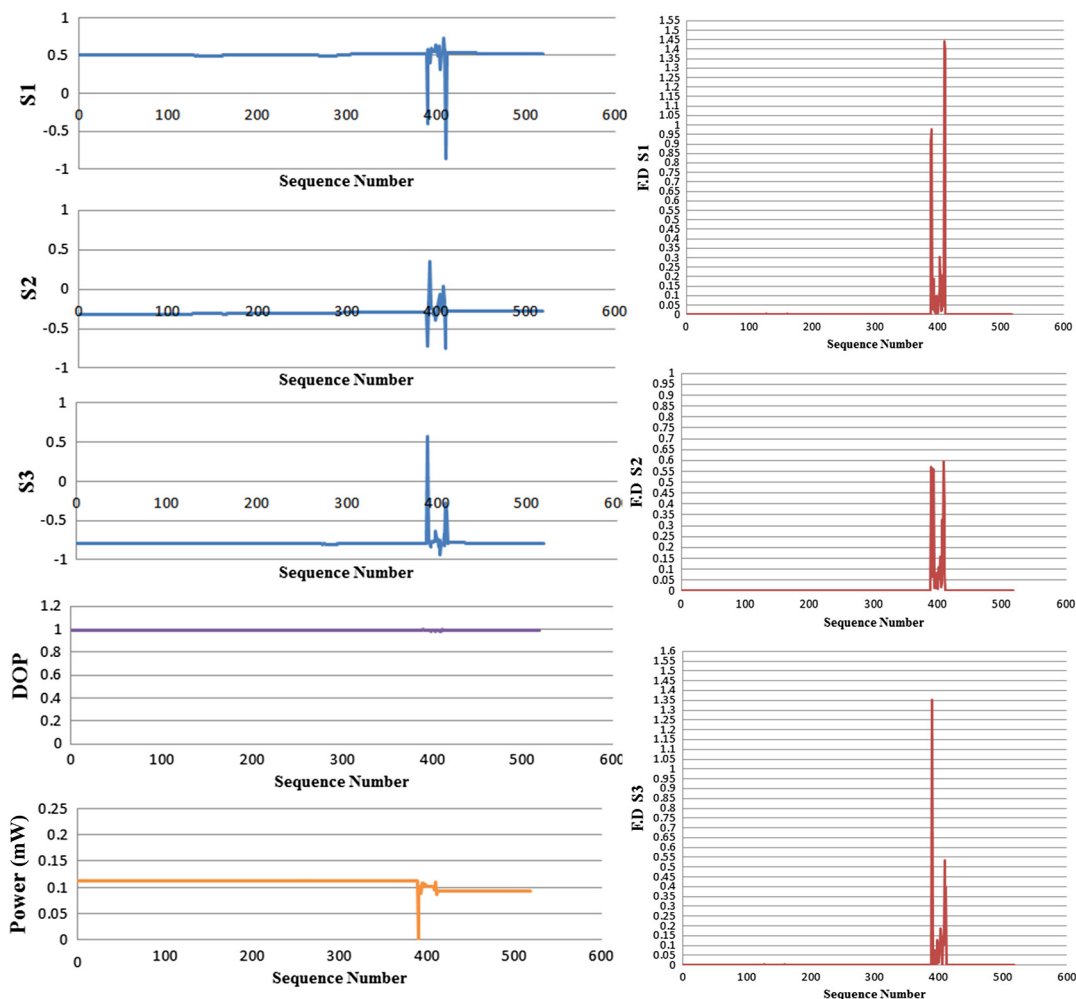

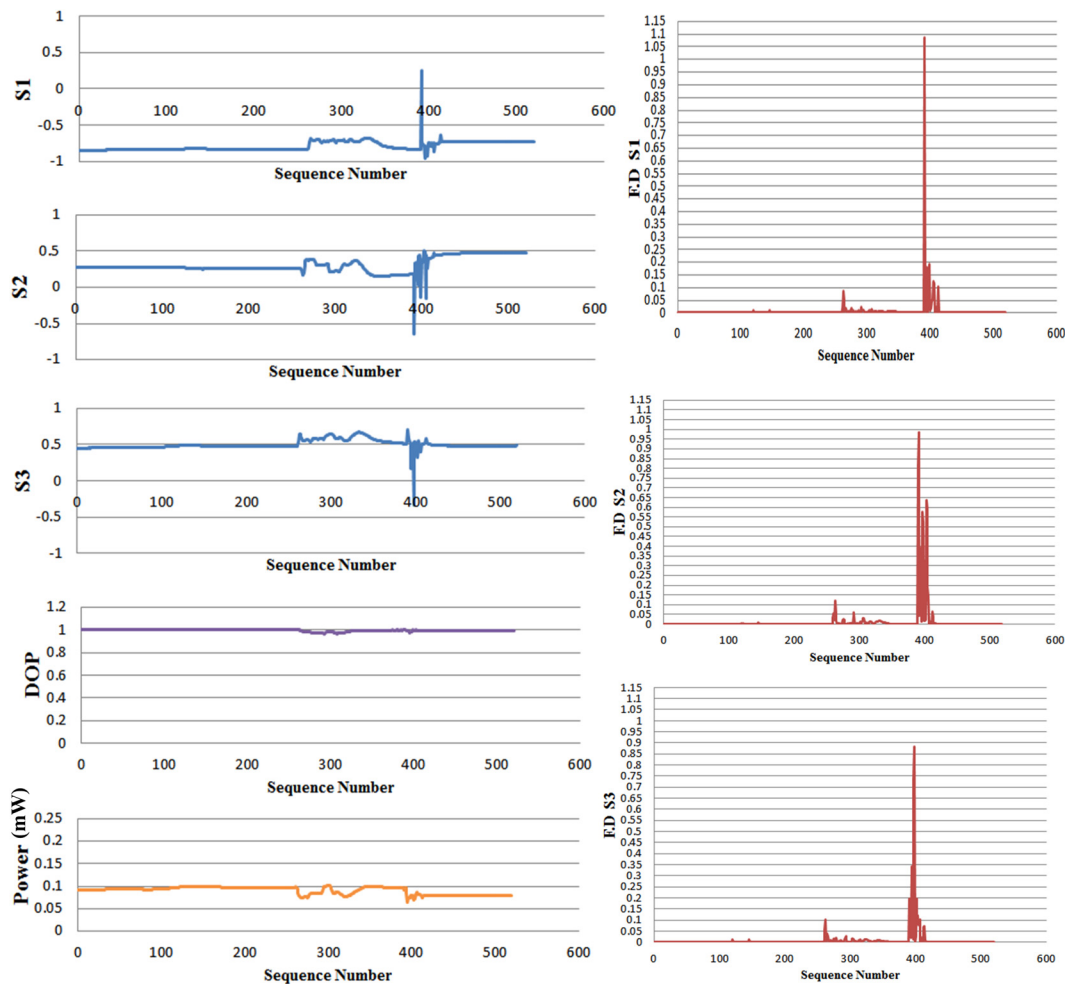**Fig. 4** Results of perturbed single-mode fiber.

Fig. 5 Results of perturbed multimode fiber.

- At interval 390 to 415, the fiber was bent. All three Stokes parameters experienced an abrupt change. The magnitude of the first-differences of the Stokes parameters far exceeded the sensitivity threshold, suggesting a different generating process. Similar to the case of a single-mode fiber, only negligible changes in the degree of polarization and power were observed.

5 Real-Life Application of Intrusion Detection System

The polarization-based intrusion detection system was implemented as shown in Fig. 6. A schematic diagram of the system is depicted in Fig. 7. An IP camera was used to transmit real-time video. The output of the IP camera was connected to a Cisco SGE2010P switch #1 [Fig. 6(a)]. The intrusion detection system [Fig. 6(b)] was applied on the link that connects switch #1 to Cisco SGE2010P switch #2. The corresponding port of switch #2 was connected to a computer for live viewing of the real-time video streamed by the IP camera [Fig. 6(d)]. The information between the two switches was routed through an optical fiber link similar to the one deployed in current networks [Fig. 6(c)]. The passage of information through this optical fiber link was monitored using the intrusion detection system.

Information corresponding to the real-time video was sent through port 13 of the Fiber Patch Panel at the input of the armored cable. The information passed through a Splice Case to either the aerial cable or to the cable in a conduit depending on the port number used at the input panel. (Ports 1 to 12 in the input panel connect the information to the conduit cable panel. Ports 13 to 24 in the input panel connect the information to the aerial cable panel.) The corresponding output port in the aerial cable panel was connected to the polarization analyzer of the intrusion detection system using a single-mode fiber.

The results of the intrusion detection system as applied in the aforementioned network were consistent with previously described findings. When perturbations were applied to the optical fiber link, the system issued an intrusion alert to indicate that an intruder was trying to tap the link. The transmitted video captured by the IP camera showed no apparent difference for unperturbed and perturbed fiber links. This application of the intrusion detection system in this configuration showed that the system is able to detect intrusion activity on the optical fiber link even when no hint of such activity is apparent to an observer of the video output.

6 Future Work

The system described above seems well suited for single-link networks. Future work includes an analysis of networks
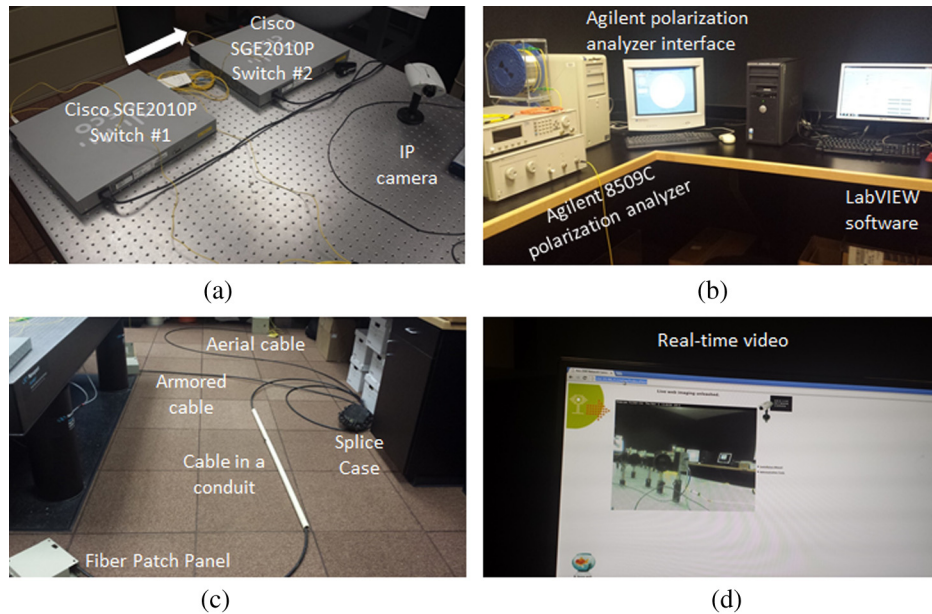
Fig. 6 Real-life application of intrusion detection system: (a) switches and IP camera layout; (b) intrusion detection system; (c) optical fiber link layout; and (d) real-time video.
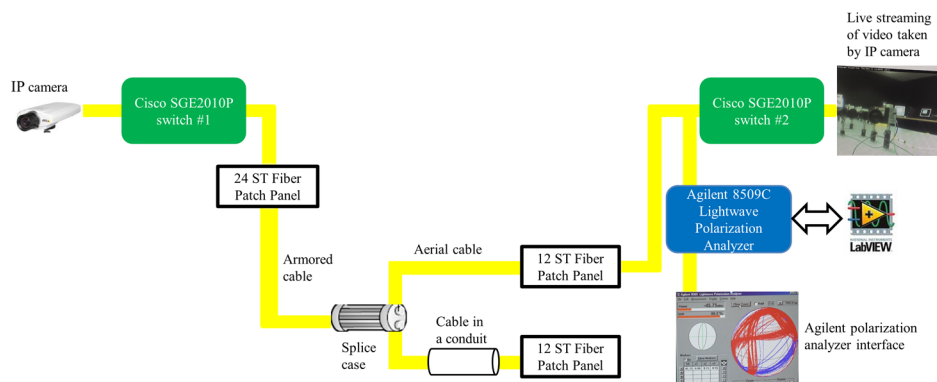

Fig. 7 Schematic diagram of real-life application of intrusion detection system.

employing optical amplifiers. Optical amplifiers change the input state of polarization. Since the state of polarization is the mechanism by which intrusion is detected, the behavior of any optical amplifier on a fiber span should be modeled in order to estimate the relationship between the output polarization state and the input polarization state. Such a model is required to enable intrusion detection on an end-to-end basis rather than a link-to-link basis.

Sensitivity of the system can be improved by adjusting sensitivity thresholds dynamically. Just as EVT can be used to estimate the probability of observing values more extreme (larger) than what has been previously observed, it can also be used to estimate the probability of observing values smaller than that has been previously observed. In the case of intrusion detection, variations smaller than those previously observed are indicative of periods of greater ambient stability. This information can be used to update the sensitivity threshold, presumably to one that is lower than the current sensitivity threshold.

At the hardware level, the Agilent polarization analyzer used is a multipurpose device. Replacing this device with a single function polarization analyzer that only measures

the state of polarization brings this system closer to being productized.

7 Conclusions

The intrusion detection system implemented and analyzed in this paper prevents data theft in optical fibers. The behavior of certain attributes of light has been examined both in unperturbed and perturbed optical fiber links of various lengths and types and under different environmental conditions and changes in fiber geometry. The system has also been tested in a real-life scenario to monitor the link through which a real-time video was being sent. The tests have proven that the state of polarization of light, represented by the Stokes parameters, is a better indicator of intrusion than the power and the degree of polarization and that the first-differences of the Stokes parameters indicate the presence of an intruder when their values exceed a sensitivity threshold. In the case of intrusion detection, the system will issue an alert to stop the communication due to the possibility of data theft. Since optical fibers are a primary means of transmitting information, efforts will continue to be exerted in this field in order to protect transmitted data from unauthorized access.

References

1. B. Gellman and A. Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post* (30 October 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (19 March 2015).
2. X. Li et al., "Hybrid TDM/WDM-based fiber-optic sensor network for perimeter intrusion detection," *J. Lightwave Technol.* **30**, 1113–1120 (2012).
3. A. Catalano et al., "Intrusion detection system for the protection of railway assets by using fiber Bragg grating sensors: a case study," in *2014 Third Mediterranean Photonics Conf.*, pp. 1–3 (2014).
4. N. Linze, P. Megret, and M. Wuilpart, "Development of an intrusion sensor based on a polarization-OTDR system," *IEEE Sens. J.* **12**, 3005–3009 (2012).
5. A. M. Bork, "Maxwell and the electromagnetic wave equation," *Am. J. Phys.* **35**, 844 (1967).
6. D. Goldstein, "Stokes polarization parameters," in *Polarized Light*, C. Roychoudhuri et al. Eds., pp. 59–91, CRC Press, New York (2010).
7. A. Kumar and A. Ghatak, "The Stokes parameters representation," in *Polarization of Light with Application in Optical Fibers*, pp. 97–119, SPIE Press, Washington (2011).
8. E. Collett, "The observables of polarized light," in *Field Guide to Polarization*, pp. 12–27, SPIE Press, Washington (2005).
9. D. Goldstein, "The Stokes polarization parameters," in *Polarized Light, Revised and Expanded*, pp. 31–59, CRC Press, New York (2003).
10. K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention," in *IEEE MILCOM Military Communications Conf.*, pp. 711–716 (2004).
11. M. Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: methods and precautions," in *8th Int. Conf. High-Capacity Optical Networks and Emerging Technologies*, pp. 164–168 (2011).
12. G. MacDonald, "*Detecting eavesdropping activity in fiber optic networks*," PhD Dissertation, The University of Oklahoma, Oklahoma (2012).
13. B. Hopkins and J. Skellam, "A New method for determining the type of distribution of plant individuals," *Ann. Bot.* **18**(2), 213–227 (1954).
14. J. Galambos, "Extreme value theory for applications," in *Extreme Value Theory and Applications*, J. Galambos, J. Lechner, and E. Simiu, Eds., pp. 1–14, Springer, Gaithersburg, Maryland (1994).

Rasha El Hajj holds a master's degree in telecommunications engineering from the University of Oklahoma. Her research interests are in the field of quantum cryptography and data encryption. In April 2014, she led the university's team to winning the first prize at a telecommunications-related business case competition held by Information and Telecommunications Education and Research Association in Louisville, Kentucky, USA.

Gregory MacDonald is a lead data scientist for the Strategic Analytics Group at HP. He is also an adjunct lecturer of electrical and computer engineering at the University of Oklahoma. His research interests include the application of machine learning methods and predictive analytics to various aspects of data center operations.

Pramode Verma is a professor and director of the Telecommunications Engineering Program in the School of Electrical and Computer Engineering of the University of Oklahoma-Tulsa. He also holds the Williams Chair in Telecommunications Networking. Prior to joining the University of Oklahoma in 1999 as the founder-director of a graduate program in Telecommunications Engineering, he held a variety of professional, managerial, and leadership positions in the telecommunications industry at AT&T Bell Laboratories and Lucent Technologies.

Robert Huck is the director of Applied Research and Unmanned Systems in the College of Engineering of the University of Oklahoma. He is also an adjunct lecturer of electrical and computer engineering. Prior to joining the University of Oklahoma in 1997, he served 20 years in the United States Air Force. He served as a manager of the Telecommunications Interoperability Lab of the University of Oklahoma-Tulsa and a manager of the Intelligent Transportation Systems Lab in Norman, Oklahoma.