OPTICA QUANTUM

Eavesdropper localization for quantum and classical channels via nonlinear scattering

Alexandra Popp,[1,2,3] **Florian Sedlmeir,**[1,2,4] **Birgit Stiller,**[1,2,3,*] 🔵 **and Christoph Marquardt**[1,2,3]

[1]*Max Planck Institute for the Science of Light, Staudtstr. 2, 91058 Erlangen, Germany*
[2]*Department of Physics, Friedrich-Alexander-Universität Erlangen-Nürnberg, Staudtstr. 7, 91058 Erlangen, Germany*
[3]*SAOT, Graduate School in Advanced Optical Technologies, Paul-Gordan-Str. 6, 91052 Erlangen, Germany*
[4]*Department of Physics, University of Otago, Dunedin, 3016, New Zealand*
*birgit.stiller@mpl.mpg.de

Optical fiber networks are part of the important critical infrastructure and known to be prone to eavesdropping attacks. Hence, cryptographic methods have to be used to protect communication. Quantum key distribution (QKD), at its core, offers information theoretical security based on the laws of physics. In deployments, one has to take into account practical security and resilience. The latter includes the localization of a possible eavesdropper after an anomaly has been detected by the QKD system to avoid denial-of-service. Here, we present an approach to eavesdropper location that can be employed in quantum as well as classical channels using stimulated Brillouin scattering. The tight localization of the acoustic wave inside the fiber channel using correlated pump and probe waves allows discovery of the coordinates of a potential threat within centimeters. We demonstrate that our approach outperforms conventional optical time-domain reflectometry (OTDR) in the task of localizing an evanescent outcoupling of 1 % with centimeter precision inside standard optical fibers. The system is furthermore able to clearly distinguish commercially available standard SMF28 from different manufacturers, paving the way for fingerprinted fibers in high-security environments.

1. INTRODUCTION

Communication in optical fibers plays a crucial role in modern information society, allowing for real-time communication over large distances. However, in most cases in communication, security is of equal importance as bandwidth and distance. Therefore, for decades, researchers have devoted their time and energy to secure encryption concepts and algorithms to block eavesdroppers from their secret communication using encryption keys on messages [1–3].

While established state-of-the-art encryption techniques rely on mathematical problems to generate and distribute encryption keys, quantum key distribution (QKD) [4,5] offers a secure key exchange concept based on the laws of quantum mechanics. By monitoring the relevant parameters (quantum bit error rate in the case of discrete variable-QKD [6] and excess noise in the case of continuous variable-QKD [7]), the QKD system can bound the information gain of a possible eavesdropper and initiate appropriate counter measures with privacy amplification [8] to ensure security depending on the amount of channel distortion. This can also mean that key generation stops when a possible information gain is too high.

QKD thus offers the unique possibility to detect possible eavesdropping based on fundamental physics principles.

However, practical security aspects and resilience have to be taken into account. In deployments, one wants to avoid a denial-of-service (DoS) scenario where an attack has been detected, but the key generation is rendered impossible because one is not able to locate and remove the attack, and this has been explicitly highlighted in a comment by the NSA [9]. To avoid DoS, it is necessary to localize and remove the eavesdropper from the channel after the detection of its presence. While this might be easier for a free-space QKD [10] system, where the communication channel is often over large distances openly visible to everyone, it can be especially challenging for fiber systems [11,12], which usually come with barely accessible underground cables or many nodes which need to be kept under control and managed. This challenge exists also in purely classical communication systems.

Research has targeted this problem developing intra-fiber monitoring techniques for several decades. Today, most distributed fiber sensors are based on Rayleigh, Raman, or Brillouin scattering [13]. While all three of these offer well-established sensing schemes based on the corresponding backscattering effect, Brillouin scattering, as the nonlinear effect with the highest gain coefficient in solid materials [14], is particularly suited for high sensitivity measurements with large

signal-to-noise requirements. Furthermore, due to the inelastic scattering nature, a distortion of an ambient parameter such as temperature, pressure, or strain will manifest in a change of the phonon resonance frequency, which offers an additional layer of sensitivity.

Most in-fiber sensing focuses on time-domain methods [15,16], where the sensor position is encoded in the backscattering time of short pulses. While this offers a strong advantage in sensing time and reduced complexity, this approach needs large gradients for clear distinction of features. In the case of fiber eavesdropping, this means that such systems can easily detect end facets or broken fibers [11] but reach limits when it comes to spliced connections or evanescent outcoupling [17]. The correlation-based approach [18,19], which we are pursuing in this work, offers the unique advantage that it is probing the nonlinear intensity as well as spectrum with high precision and sensitivity, allowing to identify and locate an eavesdropper in a quantum or classical channel.

In this work, we present a Brillouin optical correlation-domain analysis (BOCDA) system relying on centimeter-precision localized acoustic waves applied to a fiber channel that can be used for quantum or classical communication. We test the capability of the sensor to identify typical eavesdropping approaches on the channel. Mimicking a typical eavesdropping approach, we use evanescent outcoupling by fiber bending with different strengths between 1 % and 10 % of transmission loss. We show that we can localize evanescent tapping with an outcoupling intensity as low as 1 % of the total channel transmission with centimeter precision due to its influence on the acousto-optic interaction amplitude. Additionally, we are able to localize the position of evanescent outcoupling via a commercially available in-fiber tap-coupler for as low as only 1 % of coupling strength due to its sharp influence on the acoustic resonance frequency. Furthermore, we show that standard, commercially available SMF28 single-mode fibers from three different manufacturers exhibit a distinct acousto-optic fingerprint signal. We test them when connected either as patchcord or directly spliced into the channel, allowing us to clearly identify and differentiate an attacker fiber from the channel fiber even without patchcord signature. In a final step, we realize similar measurements with a commercially available Rayleigh optical time-domain reflectometer, showing that it can not reproduce our findings.

2. CONCEPT

When a secret key is exchanged by two parties Alice (A) and Bob (B) using QKD, it is possible that both parties detect the presence of an eavesdropper (E). When noticing this, the eavesdropper should be removed from the channel before pursuing the key exchange and thus the channel cannot be used until E is localized (Fig. 1, top). We apply the well-established technique of direct frequency-modulated BOCDA with high spatial resolution [18,19] to localize the eavesdropper.

BOCDA uses stimulated Brillouin scattering (SBS) [20], a third-order nonlinear interaction between light and acoustic phonons in a medium underlying energy and momentum conservation. The Brillouin resonance frequency Ω_B is dependent on temperature and pressure of the host medium via the effective refractive index and acoustic velocity:

$$\frac{\Omega_B}{2\pi} = \frac{2}{\lambda} \cdot n_{eff}(p, T) \cdot v_{ac}(p, T). \quad \textbf{(1)}$$

In a standard configuration, the acoustic phonons are excited by a strong optical pump of frequency ω_{Pump} together with a counterpropagating weak optical probe detuned by the Brillouin resonance Ω_B resulting in a backscattered, red-shifted Stokes interaction at $\omega_{Stokes} = \omega_{Pump} - \Omega_B$.

In the case of directly frequency-modulated BOCDA, the counterpropagating pump and probe fields are both sinusoidally frequency modulated with a modulation frequency f_m and bandwidth Δf, as shown in Fig. 2. This results in a position z and time t-dependent beating with frequency

$$\Delta\Omega = 2\pi\Delta f \sin(2\pi f_m t) \cdot \sin(2\pi f_m z/v_g), \quad \textbf{(2)}$$

with the group velocity of the light in the medium v_g. Resulting from this beating, SBS is only possible at the correlation points $z_m = nv_g/(2f_m)$, $n \in \mathbb{N}$ with a spatial extent of

$$\Delta z = \frac{\Delta\nu_B v_g}{2\pi f_m \Delta f}, \quad \textbf{(3)}$$

due to the necessary overlap of the probe frequency with the Brillouin resonance, where $\Delta\nu_B$ is the Brillouin gain bandwidth. At all other positions, only spontaneous scattering can be observed due to the rapid change in pump–probe frequency difference according to Eq. (2). Using standard single-mode fibers
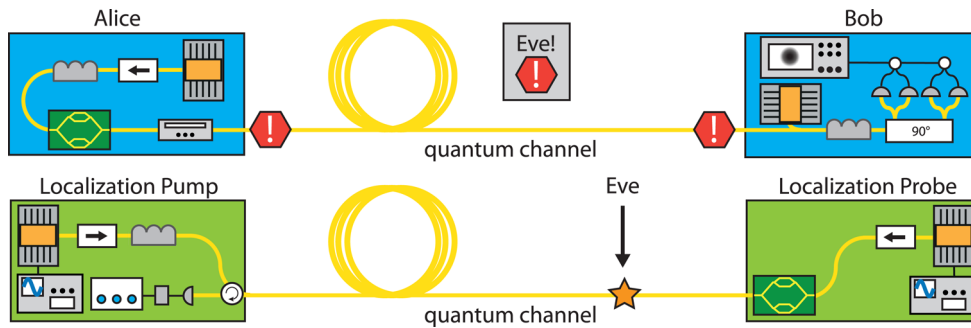

Fig. 1. Schematic of eavesdropper localization in a quantum channel. A secret key is exchanged between the two communication parties Alice (A) and Bob (B) using a quantum key distribution (QKD) system (blue). One or both of the party members notice the presence of an eavesdropper (E) by a variation of crucial QKD parameters quantum bit error rate (QBER, DV-QKD) or excess noise (CV-QKD). If a threshold is reached, where a secure key exchange is no longer feasible, the quantum state exchange is stopped between the two parties and the channel is classified insecure. The eavesdropper localization system (green) is brought into the quantum channel. Pump and Probe are connected from A and B's access points mapping out the location of E with centimeter precision, allowing to remove E and regain the channel. QKD can be resumed.
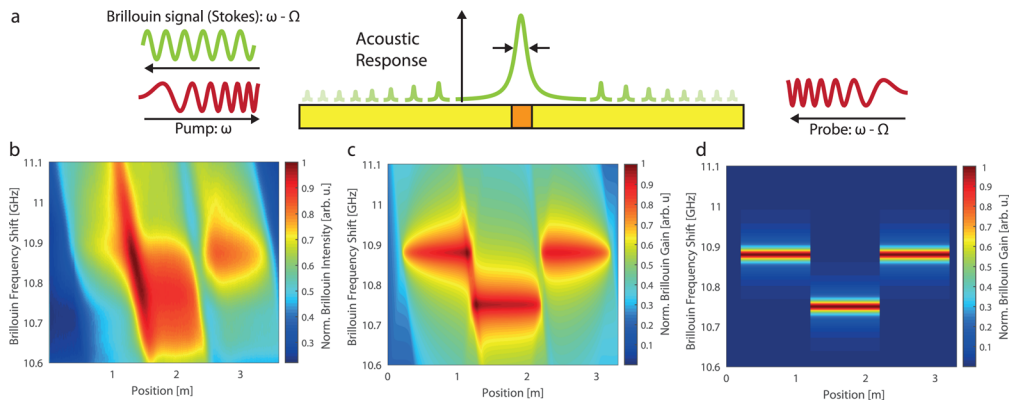
Fig. 2. (a) Scheme of directly frequency-modulated Brillouin optical correlation-domain analysis (BOCDA) in an optical waveguide. A frequency modulated pump beam (red) of optical frequency ω with modulation frequency f_m is launched into the waveguide counterpropagating to an optical probe beam (red) of optical frequency $\omega - \Omega$ is modulated by the same frequency and shifted by the waveguide acoustic resonance Ω. Due to frequency correlations, a stimulated acoustic response is only created at the specific correlation position $z_m(f_m)$ with a resolution $\Delta z(f_m, \Delta f)$, with the modulation bandwidth Δf. A frequency red-shifted Stokes signal is backscattered in counterpropagating direction of the pump, with environmental information encoded in its frequency and intensity. (b) Typical BOCDA measurement of a 980A optical fiber (position 1.1–2.1 m) embedded inside two SMF28 (positions 0.1–1.1 m and 2.1–3.1 m) fibers. Brillouin frequency shift (BFS) is shown over measurement position (arbitrary offset in m) with the normalized Brillouin intensity in color code. (c) Full frequency-domain simulation of BOCDA measurement presented in panel (b). (d) Retrieved gain spectrum without background resulting from frequency correlations.
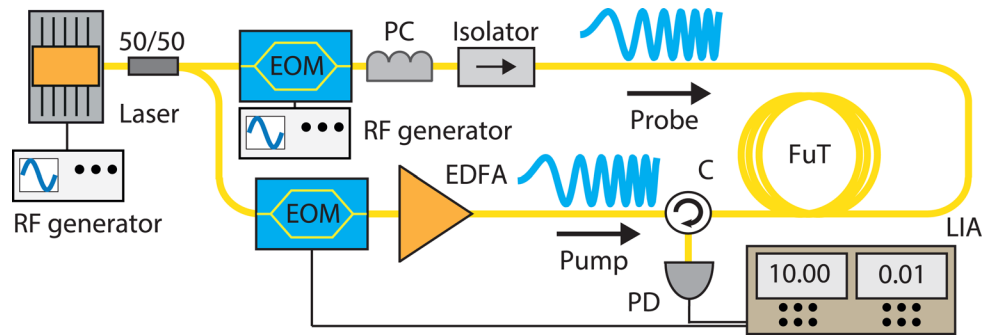

Fig. 3. Typical setup for BOCDA adapted from Ref. [18]. RF, generator radio frequency generator; 50/50, 50:50 beam splitter; EOM, electro optical modulator; PC, polarization controller; isolator, optical isolator; EDFA; erbium-doped fiber amplifier; C, optical circulator; FuT, fiber under test; PD, photodiode; LIA, lock-in amplifier.

with a Brillouin gain bandwidth of $\Delta \nu_B = 27$ MHz, a modulation bandwidth of $\Delta f = 47$ GHz and a modulation frequency $f_m = 699$ kHz, we achieve a maximum between two different correlation points $\Delta z_m = 146$ m and a resolution of $\Delta z = 3.0$ cm. The correlation point distance can easily be extended to several kilometers by decreasing the modulation frequency. The position inside the sensing target can be moved by adjusting the modulation frequency, which allows for delayline-free measurements, which is a strong benefit for communication channels which can be of the order of several kilometers.

For a complete measurement as shown in Fig. 2(b), the full Brillouin resonance is acquired for each position of the channel. For this, the probe frequency is swept over the Brillouin resonance and data acquisition is handled by a fast ADC ensuring Hz-speed measurement rates. The experimental setup is shown in Fig. 3. It uses a narrow linewidth laser that is directly modulated by a radio frequency generator. The frequency-modulated light is split into a pump and probe arm. The pump is modulated by a low-frequency sinusoidal signal to be able to lock it to the lock-in amplifier. The pump is afterwards amplified by an erbium-doped amplifier to achieve efficient coupling between

optical and acoustic waves. The probe passes through an electro-optic modulator which sweeps the frequency difference between pump and probe from approximately 10.6 GHz to 11.1 GHz to image the full Brillouin spectrum. The probe is then detected after passing through the fiber under test and a circulator at the photodiode.

We can employ frequency-domain simulations following Refs. [21,22] for full understanding of the spectrum [Fig. 2(c)]. Furthermore, we use it for retrieval of the underlying gain spectra without the influence of the frequency correlation [Fig. 2(d)] causing the asymmetric tilt of the spectra observed in Figs. 2(b) and 2(c). Most of the time, it is however sufficient to extract information directly from the raw data, especially for a channel with a smooth underlying gain profile, which is usually the case for long fibers. With this type of measurement, it is now possible to gain spatially resolved information about the spectral profile of the Brillouin response as well as the intensity of all spectral components. As shown in Fig. 2, this allows the straightforward distinction of fibers with slightly different refractive index. For illustration, we embed 1 m of commercially available 980A fiber patchcord (position 1.1–2.1 m within two SMF28

(positions 0.1–1.1 m and 2.1–3.1 m). While both fibers support 1550-nm light, the 980A is clearly localized by the measurements due to the shift in Brillouin resonance by approximately 150 MHz. Another advantage of this technique is the agility of resolution and sensing distance, which can be accessed by simple variation of the frequency modulation allowing to reach resolutions from few centimeters to several 10s of meters along with a delayline-free sensing range of several kilometers [23].

3. APPLICATION

A simple, but conventionally very hard-to-detect, eavesdropping approach is evanescent coupling [12]. Using fibers, evanescent outcoupling can easily be realized by bending the fiber either using appropriate devices or just brute-force. Already bending the fiber slightly will result in several percent of transmission loss for the channel which is accessible for E. Since this kind of bending does not produce a sharp edge, it is difficult to detect it with conventional optical time-domain reflectometry (OTDR) [17].

Full spectral measurements of a 1-m SMF28 which is bent to achieve evanescent outcoupling are shown in Fig. 4. A reference measurement of the undisturbed fiber is provided in Fig. 4(a). The measurement scheme is as explained in Section 2 and shown in Fig. 2(b), the white dots in each measurement denote the location of maximum BFS. The fiber is bent around the location 1.5 m over a length of approximately 10 cm, inducing transmission losses of 1 % [Fig. 4(b)], 5 % [Fig. 4(c)], and 10 % [Fig. 4(d)].

For all three cases, the Brillouin intensity is locally influenced by the bendloss, showing a narrowing of the high-frequency

signal around the bend position due to the decreased opto-acoustic interaction amplitude. This asymmetric decrease is caused by the asymmetric shape of the BOCDA background explained in Section 2, which also causes the peak around position 2.2 m that is visible in all measurements including the reference. As expected, the amount of intensity loss is continuously increasing proportional to bendloss. No significant change in maximum BFS is visible, confirming that the bending is not influencing the longitudinal acoustic phonons but only the opto-acoustic interaction amplitude. This means that this change is not visible by most techniques monitoring only refractive index changes, but localizable explicitly due to the large nonlinear Brillouin gain. Furthermore, it can be seen that the intensity decrease is highly localized around the bending position and, especially in the 1 % case, only a small fraction of the total intensity. Thus, the centimeter resolution offers a considerable advantage not only in localization sensitivity, but also in precision. In the presented data, no additional algorithm or threshold-dependent decision scheme has been used. The changes are visible by the bare eye. Observing such changes directly in the data shows the feasibility of our method, which can be strongly improved by a formal algorithm. One could for example use the root mean square (rms) difference between the reference and current trace to quantify the deviations or track the curve width involving a fitting model to boost the sensitivity beyond 1 % of evanescent outcoupling. Also, a machine learning based algorithm could be employed for further sensitivity increase.

In a practical application of our method to a QKD system, we would propose a initial fingerprint of the system. That can be done when taking the system into operation or at given regular times such as a maintenance routine on the channel which keeps
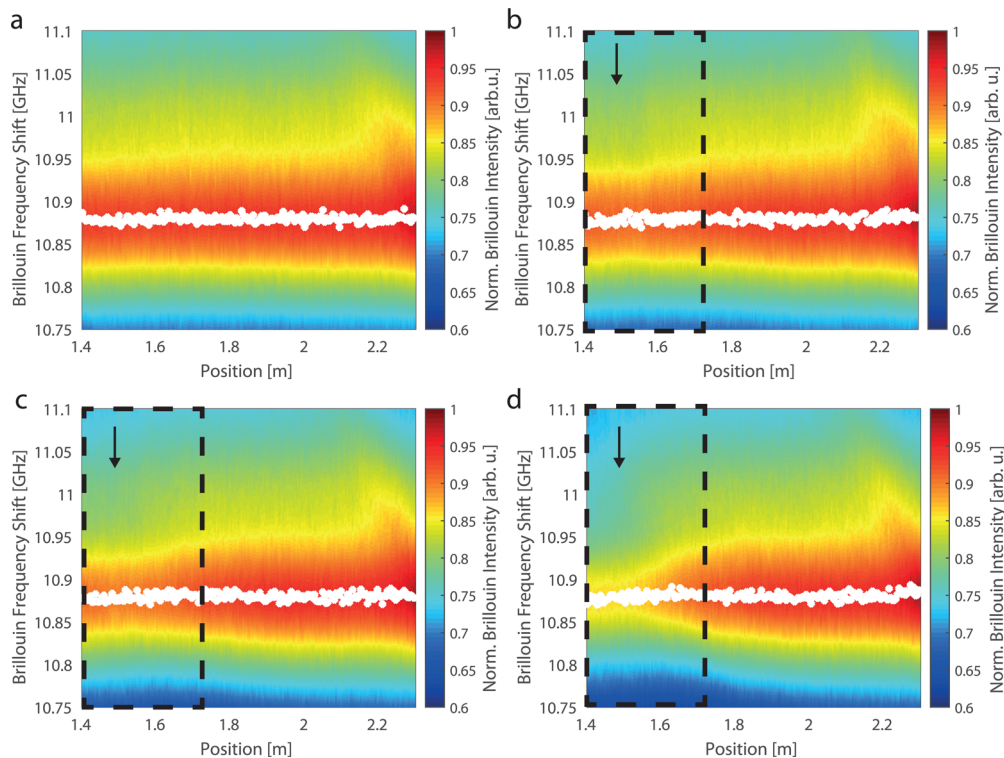

Fig. 4. (a) Full spectrum reference measurement of 1 m SMF28, BFS over position, normalized Brillouin intensity color coded. White dots denote location of maximum BFS. Steady BFS is observed with nearly constant spectral features. Spectral distortion at position 2.15 m results from patchcord for coupling at position 2.35 m (not shown). (b) Same fiber as in Fig. 3(a) with a bending at position 1.5 m resulting in an evanescent coupling loss of 1 % (location marked by black box). Clear change of spectral features visible, marking the bending position. (c) and (d) Similar measurement as Fig. 3(b) for a bendloss of (c) 5 % and (d) 10 % resulting in strongly enhanced spectral features.
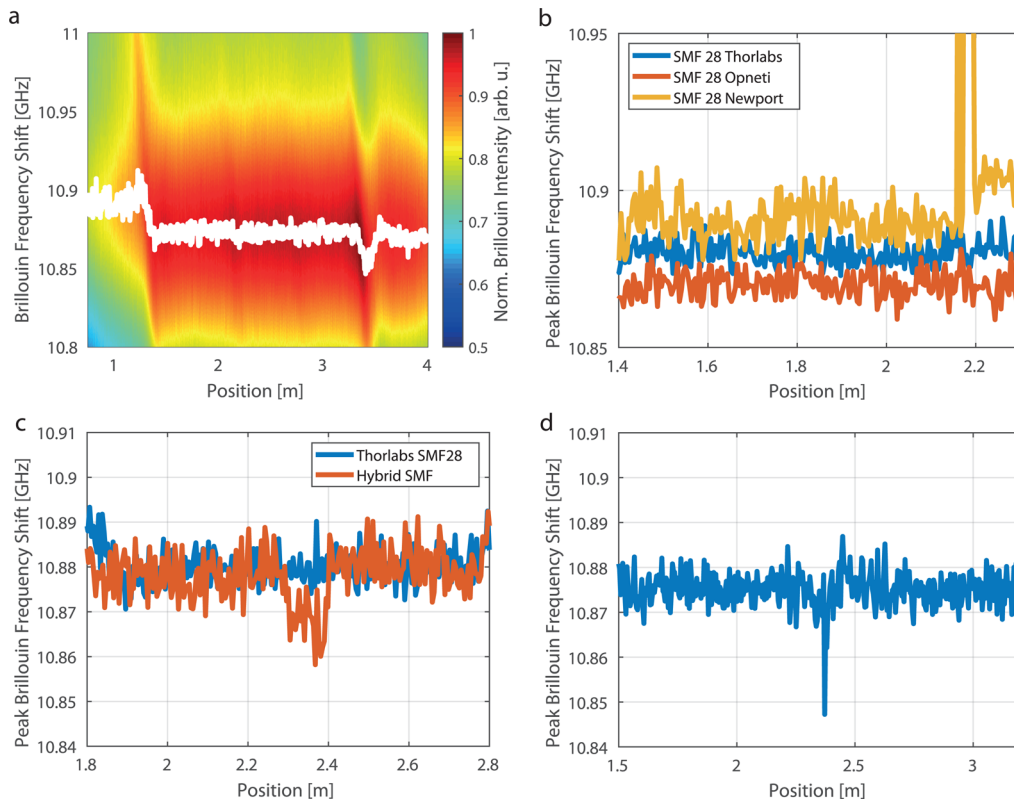
Fig. 5. (a) Full spectrum of Opneti SMF28 (position 1.4–3.4 m, BFS over position, norm. Brillouin intensity color coded, white dots denote location of maximum BFS) in between Thorlabs SMF28 (position 0.8–1.4 m) and Opneti SMF28 (position 3.4–4.0 m) all connected with FC/AP connectors. Clear localization of FC/APC connector positions (connectors C1 at 1.4 m and C2 at 3.4 m) through full spectral features as well as maximum BFS only. Clear distinction of maximum BFS frequency for fibers from different manufacturers. (b) Peak BFS over position for commercially available SMF28 fibers from three manufacturers, Thorlabs (blue), Opneti (red), and Newport (yellow), showing clear distinction of mean maximum BFS of several MHz. (c) Comparison of maximum BFS of standard Thorlabs SMF28 patchcord (blue) with hybrid spliced patchcord (red, 6-cm Opneti SMF28 spliced into 1.0-m Thorlabs SMF28), section of Opneti fiber clearly visible by mean BFS shift. (d) Maximum BFS over position of commercially available Thorlabs 99-1 in-fiber beam splitter clearly locating the 1 % splitting position.

track of all changes that are made to the channel. The initial fingerprint will contain certain features of the quantum channel but will depend on the overall absolute temperature and fixed strain. However, we want to mention that the QKD system will detect a possible eavesdropper due the implemented security proofs and therefore, both systems QKD and BOCDA will work together to ensure security and reliability at the same time.

Next, we replace the previously used SMF28 by an SMF28 patchcord from a different manufacturer. All fibers used in this case are commercially available standard SMF28 with FC/APC connection from the manufacturers Thorlabs, Opneti, and Newport. We measure the Brillouin response of each of the fibers separately in between two standard SMF28 fibers, where the fiber at low position is a Thorlabs SMF28 and the fiber at high position is an Opneti SMF28 [Fig. 5(a)]. Here, the following constellation is used: Thorlabs SMF28 (0.8–1.4 m)–Opneti SMF28 (1.4–3.4 m)–Opneti SMF28 (3.4–4.0 m). The FC/APC connectors are clearly visible in the Brillouin intensity as well as in the maximum BFS. Furthermore, we see that the maximum BFS of the Opneti SMF28 is clearly distinct from the Thorlabs SMF28. Thus, we can monitor only the maximum BFS and find significant distinction among the three manufacturers [Fig. 5(b)] by several MHz. Therefore, we can assign a fingerprint BFS to seemingly undifferentiable commercially

available fibers directly using our measurements without significant postprocessing. Furthermore, we create a hybrid SMF28 splicing 6 cm of Opneti SMF28 into a Thorlabs SMF28 patchcord [Fig. 5(c)] to exclude a bias from the connection facets. Figure 5(c) shows that we can clearly identify the spliced piece by just monitoring the maximum BFS, which shows a difference of approximately 10 MHz from the rest of the hybrid fiber. Thus, we have confirmed that even though these fibers should be nearly identical and have very similar light guiding properties, their respective refractive index or acoustic velocity [resulting from Eq. (1)] varies enough to identify and distinguish each of them clearly.

This result has severe implications on the possibility to secure fiber networks. Showing that the difference in standard SMF28 composition is enough for clear identification of the fiber type paves the way for complete fingerprint measurements of deployed fiber channels, where parts that are added after a maintenance or offline period of the network can be clearly mapped and identified, ensuring no third party tampering with the channel. An additional layer of security could be achieved by only using fibers with a special composition, unknown to the public, when deploying new fiber networks in the future. As there are currently many future quantum fiber networks planned and deployed in Europe and around the world [24,25], our findings
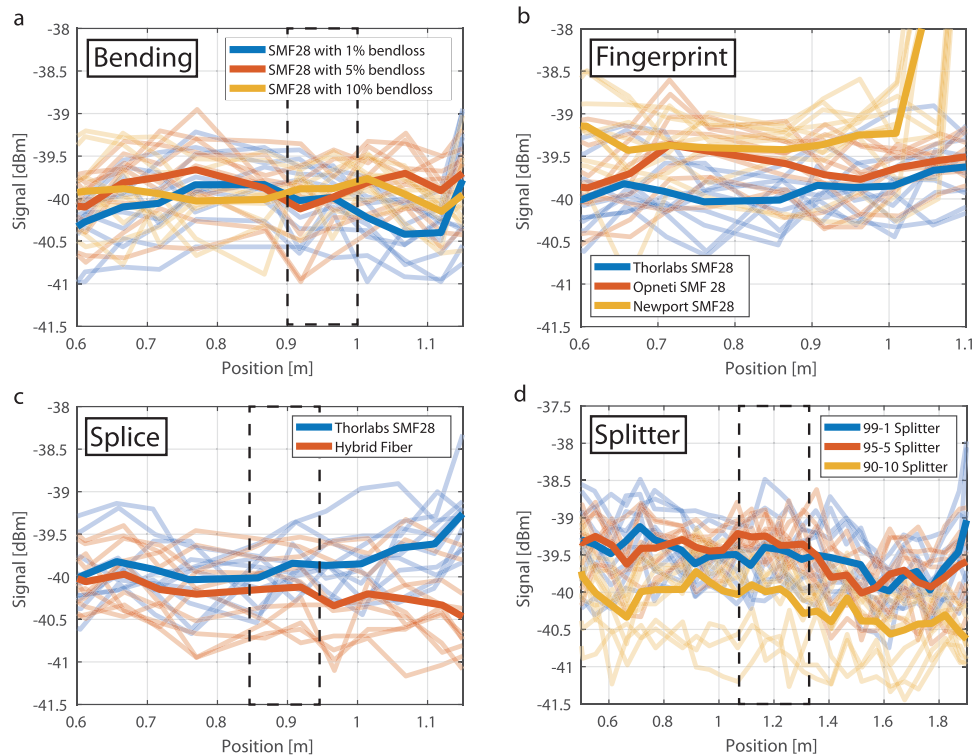
Fig. 6.   OTDR measurements using commercially available LOR-200 high-resolution optical time-domain reflectometer with 2-ns pulses and 2.5-cm sampling resolution. Saturated, solid curves of all plots mark the mean of 10 consecutive measurements, weakly saturated curves mark results of all 10 individual measurements. (a) SMF28 fibers of Thorlabs (blue), Opneti (red), and Newport (yellow) as shown with BOCDA in Fig. 4(b). No clear distinction of fiber composition possible, significant scattering of individual measurements (weakly saturated curves). (b) SMF28 with 1 % (blue), 5 % (red), and 10 % (yellow) transmission loss introduced by evanescent outcoupling similar to Fig. 3. Marked area denotes bending position. No point of introduced loss is visible for any of the induced transmission losses. (c) Thorlabs SMF28 (blue) and hybrid fiber with 6-cm Opneti SMF28 spliced in between Thorlabs SMF28 at marked position. No clear identification of spliced section, large variance of individual measurement sets (weakly saturated curves). (d) In-fiber 99-1 (blue), 95-5 (red), and 90-10 (yellow) splitters. Splitting at marked position, no clear identification of splitting location or induced loss possible.

could be used in dedicated deployments in the near future. Furthermore, due to the high resolution of only $\Delta z = 3.00\,\mathrm{cm}$ together with the above features, our system can also be used to detect tampering inside complex fiber or waveguide based devices. This can create an additional layer of security for end-users, removing the necessity of blind trust in black boxes supplied by manufacturers. Also the length of the method can be increased substantially as several recent publications have proven experimentally [26–28].

Another tapping method is the simple optical tap-coupler [12], which can split optical powers of different fractions as small as 1 % of transmission. This small fraction of tapping loss might easily be overlooked, especially in a classical system. Here, we show [Fig. 5(d)] that it is possible to localize the interruption point as a very distinct feature in the maximum BFS.

In a final step, we compare the performance of our system to a commercially available Rayleigh optical time-domain reflectometer. We use a LOR-200 high-resolution optical time-domain reflectometer with 2-ns pulses and 2.5-cm sampling resolution, and repeat the measurements shown in Figs. 4 and 5. Results are shown in Fig. 6, where an average of 10 consecutive measurements (solid curves) as well as the results of all 10 individual measurements (weakly saturated curves) are given. The difference in absolute position is caused by the measurement method, where we define the absolute 0 of the BOCDA measurement at

the start of the seed isolator, while we define the absolute zero of the OTDR measurement at the beginning of the respective test fiber. During our measurements, we do not find any signature of the loss induced by the fiber bending up to a transmission decrease of 10 %. This is a significantly worse performance than considering the results in Fig. 4, where a clear signature is already visible for 1 % loss. Comparing with Fig. 5(b), we find that first of all, no clear distinction of the individual fiber manufacturers is possible, since the scatter of the individual measurements is large. Furthermore, the mean does not reproduce our previous findings, producing partly overlapping curves as shown in Fig. 6(b). In agreement with Fig. 6(b), it was also not possible to resolve the hybrid spliced fiber as shown in Fig. 6(c) in contrast to Fig. 5(c). There were also no significant features caused by the splicing facets. Lastly, no significant signature of the optical splitters was observed, while splitters with ratios up to 10 % splitting were investigated [Fig. 6(d)]. Note that recent research on OTDR [29] has shown the sensitive detection of fiber connections via APC connectors [17] do not usually specialize in gradual changes of the refractive index.

4. CONCLUSION

In this work, we have shown a novel method for eavesdropper localization that can be applied to quantum as well as classical

channels. We use localized acoustic waves created via Brillouin optical correlation-domain analysis (BOCDA) to monitor standard optical fibers with centimeter spatial resolution, observing the complete Brillouin spectrum. This allows us to monitor the BFS caused by the longitudinal acoustic phonons as well as the intensity of the nonlinear scattering. We clearly identify and localize an eavesdropping approach using evanescent outcoupling via fiber bending with a transmission loss down to 1 %. Furthermore, we show that we can clearly distinguish commercially available standard SMF28 fibers from three different manufacturers, finding that each of them has a clear fingerprint BFS distinct from the others. In addition, this can be applied inside a hybrid spliced fiber, showing that this distinction is possible over a length of 6 cm of spliced SMF28. Also, we are able to identify splitting by commercially available tap-couplers, clearly locating the tap-position of a 1 % splitter. In a final step, we show that it was not possible to recreate any of these findings with a commercially available optical time-domain reflectometer.

Acknowledging the importance of physical layer security for optical communication networks, we believe that our monitoring approach, which can be used for classical as well as quantum channels, will allow more than one additional layer of eavesdropper security for all communication systems. Note that due to the practical restrictions on loss budget, today, most fiber-based QKD systems are still limited to possibly a few 100 km in range as well as weakly complex optical topology. The restrictions of QKD furthermore limit the application of optical components strictly to linear optical building blocks. While systems might get more complex in the future, our work shows that we can already address each of those components individually.

The possibility to detect evanescent eavesdropping via acoustic waves is a great advance compared with conventional OTDR as it excels in the detection of gradual changes of the refractive index as usually found in eavesdropping techniques. Furthermore, our novel finding of distinct Brillouin fingerprints for commercially available SMF28 opens up the possibility for dedicated fiber composition designs for high-security application, allowing us to precisely characterize future networks, and prevent fiber additions and other tampering. While the setup can be used as a stand-alone device, it can also be implemented into QKD systems, operating for example in a switching mode. This can pave the way to consistent monitoring about the installed networks in real-time. Finally, it has to be stressed that the physical limits of the detection sensitivity and resolution are yet to be explored and can be pushed further, for example, by applying machine-learning techniques to detect even smaller deviations.

REFERENCES

1. S. Singh, *The Code Book*, Vol. 7 (Doubleday New York, 1999).
2. C. E. Shannon, "A mathematical theory of communication," The Bell system technical journal **27**(3), 379–423 (1948).
3. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**, 120–126 (1978).
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
6. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Steering Committee, 1984).
7. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**(1), 010303 (1999).
8. C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995).
9. "NSA on quantum key distribution (QKD) and quantum cryptography (QC)," https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-//Cryptography-QC/. Accessed: 2023-06-23.
10. W. Buttler, R. J. Hughes, P. G. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**(15), 3283–3286 (1998).
11. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans.Inform.Forensic Secur. **6**(3), 725–736 (2011).
12. K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention,", in *IEEE MILCOM 2004. Military Communications Conference, 2004.*, Vol. 2 (IEEE, 2004), pp. 711–716.
13. P. Lu, N. Lalam, M. Badar, B. Liu, B. T. Chorpening, M. P. Buric, and P. R. Ohodnicki, "Distributed optical fiber sensing: review and perspective," Appl. Phys. Rev. **6**(4), 041302 (2019).
14. F. Yang, F. Gyger, and L. Thévenaz, "Intense Brillouin amplification in gas using hollow-core waveguides," Nat. Photonics **14**(11), 700–708 (2020).
15. Y. Rao, Z. Wang, H. Wu, Z. Ran, and B. Han, "Recent advances in phase-sensitive optical time domain reflectometry (OTDR)," Photonic Sens. **11**(1), 1–30 (2021).
16. Q. Bai, Q. Wang, D. Wang, Y. Wang, Y. Gao, H. Zhang, M. Zhang, and B. Jin, "Recent advances in Brillouin optical time domain reflectometry," Sensors **19**(8), 1862 (2019).
17. M. Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: methods and precautions", in *8th International Conference on High-Capacity Optical Networks and Emerging Technologies* (IEEE, 2011), pp. 164–168.
18. K. Hotate and T. Hasegawa, "Measurement of Brillouin gain spectrum distribution along an optical fiber using a correlation-based technique–proposal, experiment and simulation–," IEICE transactions on electronics **83**, 405–412 (2000).
19. A. Zarifi, B. Stiller, M. Merklein, Y. Liu, B. Morrison, A. Casas-Bedoya, G. Ren, T. G. Nguyen, K. Vu, D.-Y. Choi, A. Mitchell, S. J. Madden, and B. J. Eggleton, "On-chip correlation-based Brillouin sensing: design, experiment, and simulation," J. Opt. Soc. Am. B **36**(1), 146–152 (2019).
20. C. Wolff, M. Smith, B. Stiller, and C. Poulton, "Brillouin scattering-theory and experiment: tutorial," J. Opt. Soc. Am. B **38**(4), 1243–1269 (2021).
21. T. Yamauchi and K. Hotate, "Performance evaluation of Brillouin optical correlation domain analysis for fiber optic distributed strain sensing by numerical simulation", in *Fiber Optic Sensor Technology and Applications III*, Vol. 5589 (SPIE, 2004), pp. 164–174.
22. K. Y. Song and J. H. Choi, "Measurement error induced by the power-frequency delay of the light source in optical correlation-domain distributed Brillouin sensors," Opt. Lett. **43**(20), 5078–5081 (2018).

23. Y. Wang and M. Zhang, "Recent progress in long-range Brillouin optical correlation domain analysis," Sensors **22**(16), 6062 (2022).

24. "European consortium OpenQKD," https://openqkd.eu/. Accessed: 2023-01-24.

25. Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, "Quantum information research in China," Quantum Sci. Technol. **4**(4), 040503 (2019).

26. K. Hotate, H. Arai, and K. Y. Song, "Range-enlargement of simplified Brillouin optical correlation domain analysis based on a temporal gating scheme," SICE Journal of Control, Measurement, and System Integration **1**(4), 271–274 (2008).

27. D. Elooz, Y. Antman, N. Levanon, and A. Zadok, "High-resolution long-reach distributed Brillouin sensing based on combined time-domain and correlation-domain analysis," Opt. Express **22**(6), 6453–6463 (2014).

28. Y. Zhou, L. Yan, Z. Li, H. He, J. Ye, W. Pan, and B. Luo, "Long-range high-spatial-resolution distributed Brillouin sensing enabled by correlation-domain encoding," Opt. Lett. **48**(12), 3143–3146 (2023).

29. F. Azendorf, A. Sandmann, M. Eiselt, and B. Schmauss, "Distributed sensing of single mode fibers with correlation techniques," in *Photonic Networks; 23th ITG-Symposium* (VDE, 2022), pp. 1–4.