CHALMERS
UNIVERSITY OF TECHNOLOGY

Eavesdropping G.652 vs. G.657 fibres: a performance comparison

Citation for the original published paper (version of record):

Kalsson, S., Lin, R., Wosinska, L. et al (2022). Eavesdropping G.652 vs. G.657 fibres: a performance comparison. 2022 International Conference on Optical Network Design and Modeling, ONDM 2022. http://dx.doi.org/10.23919/ONDM54585.2022.9782849

Eavesdropping G.652 vs. G.657 fibres: a performance comparison

Stefan Karlsson
FMV VO LedM
Swedish Defence Material Administration
Linköping, Sweden
stefan.karlsson@fmv.se

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

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

Paolo Monti
Electrical Engineering
Chalmers University of Technology
Göteborg, Sweden
mpaolo@chalmers.se

***Abstract*— With increasing dependence on secure access to digital services and the ultra-high traffic volumes running on the optical fibre communication infrastructure, the protection of this infrastructure from eavesdropping is extremely important, especially in defense and military applications. The G.657 fibre is recommended to be deployed in in-building installations for its improved bending performance compared to the G.652 fibre. However, the easiness to be eavesdropped, which reflects the security level of those two types of fibres has not yet been investigated. In this paper, we study the eavesdropping of fibre from a system perspective and compare the bending property of G.652 and G.657 fibres. The measurement results show that G.657 can be bent sharper than G.652 without causing any additional power attenuation at the receiver. This indicates that the so-called bending-insensitive G.657 fibre can potentially be eavesdropped more easily than their G.652 counterparts.**

Keywords—eavesdropping, bend radius, bend angle, G.657

I. INTRODUCTION

Optical fibres form the physical infrastructure of today's communication networks, carrying from Gbps to Tbps of information. Therefore, protecting this infrastructure from illegal eavesdropping and/or sabotage is of increasing importance. Fig. 1 shows the eavesdropping concept from a system perspective. Eve is eavesdropping the optical signal between Bob and Alice at the distance L_{Eve} from Bob. The eavesdropping can be implemented by several methods, e.g., beam splitting, decoupling, V-groove, and fibre bending [1]. Among those methods, fibre bending is the cheapest for tapping the optical signal. However, bending the fibre to tap the light out introduces an attenuation that Alice can observe if high enough.

Two types of single mode fibre (SMF), i.e., G.652 and G.657, are considered in this study. G.652 is bending sensitive and is widely deployed in outside plants. However, it cannot be used in installations where much bending is unavoidable, e.g., in-building applications. It is advisable to use G.657 fibres in such cases thanks to their better bending performance (i.e., they introduce less attenuation). The bending properties of the two fibre types have been studied extensively [2], [3]. However, their security performance in terms of eavesdropping properties has not been investigated yet. More specifically, it is crucial to understand the security level of these two fibre types when a malicious party tries to eavesdrop them.

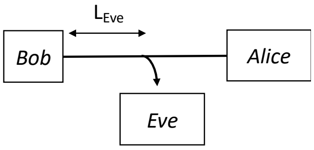

Figure 1. Example of eavesdropping between Alice and Bob. Eve tries to eavesdrop the information at a certain distance from Bob.

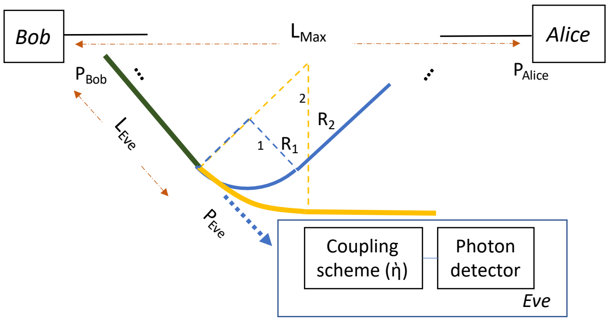

Figure 2. The principle of out-coupling light due to fibre bending at different radiuses and angles.

In this paper, we model, experimentally evaluate and compare the bending and eavesdropping characteristics of G.652 and G.657 single-mode fibres.

II. PRINCIPLE OF EAVESDROPPING AN OPTICAL FIBRE

The simplest method for eavesdropping is bending a fibre and detecting the outcoupled light. Fig. 2 shows this principle. The amount of light that can be coupled out of a fibre depends on the bend radius R and the bend angle θ. When the bend radius is small and the bend angle is large, more optical power can be coupled out from the fibre, leading to a higher attenuation detected by the receiver at Alice's side. Fig.2 shows examples of bending with R_1, θ_1, and R_2, θ_2. The light coupled out from the fibre with a bend angle θ_1 and radius R_1 is higher than an angle θ_2 and a radius R_2 are used. To eavesdrop, Eve needs a coupling scheme with efficiency $\dot{\eta}$ to focus the outcoupled light onto the active area of the photon detector. When the fibre is bent, the outcoupled light forms a light cone. A sharper bend angle can be beneficial for the light cone to be focused on the detector more efficiently. As a result, a sharper bent in fibre may produce more efficient eavesdropping without causing any additional power loss at the destination (i.e., consequently, fewer chances of detection). Note that details on how Eve can implement a high-efficient detection scheme are out of the scope of this study and are not discussed in the paper.

The value of the power level coupled out of the fibre by Eve can be expressed as:

$$P_{Eve} = P_{Bob}\, \alpha^{L_{Eve}} \left(1 - 10^{-D_{Eve}/10}\right), \quad (1)$$

where P_{Bob} is the optical power level at Bob, α stands for fibre attenuation (i.e., including the connectors along the link), L_{Eve} is the distance between Bob and Eve, and D_{Eve} is the attenuation introduced by Eve's eavesdropping attempt. Given Eve's efficiency to detect the out coupled light $\grave{\eta}$, the power level at which Eve can detect the signal is:

$$P_{eff} = P_{Eve}\, \grave{\eta}\,. \qquad (2)$$

After Eves' eavesdropping attempt, the power level received by Alice can be expressed as:

$$P_{Alice} = P_{Bob}\, \alpha^{L_{max}}\, 10^{-D_{Eve}/10}\,, \qquad (3)$$

where L_{max} is the distance between Bob and Alice.

A system operator can install an alarm triggered when the received power at Alice falls below a certain level to detect eavesdropping. On the other hand, due to additional power losses along the transmission link (e.g., fibre flaws, installation losses, couplers, connectors), operators need to set a margin when computing the power budget for the transmission between Bob and Alice. However, if the power attenuation induced by an eavesdropper falls within this margin, the eavesdropping attempt will not be detected. So, for example, if a system sets a margin of 3 dB, there is a high chance that it will miss all the eavesdropping attempts that cause less than 3 dB of attenuation at Alice’s side.

Let's now consider, as an example, a 40 km long fibre link within the Swedish defence network running at 10 Gbps. The parameters describing this transmission system are shown in Table I. Alice is equipped with a detector (e.g., small form-factor pluggable (SFP)) with a sensitivity of -25 dBm [4]. Eve is equipped with the same photodetector and an optical amplifier providing an 11 dB gain [5]. A commercial clip-on eavesdropping device [6] is used as a reference. This commercial clip-on introduces an attenuation of 2.2 dB (i.e., when used at a wavelength of 1310 nm) while its detection efficiency is 0.13%. It is also essential to consider the possibility that Eve might use more efficient, non-commercial eavesdropping devices able to introduce lower losses than the commercial ones. For this reason, we look at two additional cases, i.e., one where a clip-on device with 1 dB loss and a 1.5% coupling efficiency is used, and another one with 0.2 dB loss and the same (i.e., 1.5%) coupling efficiency. Figure 3 shows the input power at Eve's SFP detector [4] (i.e., P_{eff}) when the eavesdropping occurs at different places along the fibre link. The blue line represents the case where the commercial clip-on device is deployed for eavesdropping, and the purple dotted line indicates the sensitivity of the detector at Eve's side. It can be observed that, when the commercial clip-on device is used, Eve can successfully tap data as long as Eve’s location is within 15 km from Bob. When moving further away (i.e., more than 15 km from Bob), the power of the outcoupled light power becomes too low for Eve's photodetector. When equipped with a more advanced eavesdropping device (e.g., with coupling efficiency as high as 1.5% and with 0.2 dB of attenuation (red line in Fig. 3)), Eve can successfully tap data up to 21 km from Bob. If an attenuation of 1dB can be obtained with the same coupling efficiency (i.e., 1.5%), Eve can then tap the information along the entire 40 km link.

The analysis presented above indicates that eavesdropping detection based on power measurement at the system receiver might not always be practical. For example, if the power threshold for an alarm is set higher than the system margin, there is a high probability that an eavesdropping attempt goes undetected. On the other hand, putting the power threshold for an intrusion alarm lower than the system margin might lead to frequent false alarms.

Table I. Notation and values

Notation	P_{Bob}	α	L_{max}
Value (unit)	1 mW	0.955 (km^{-1})	40 km

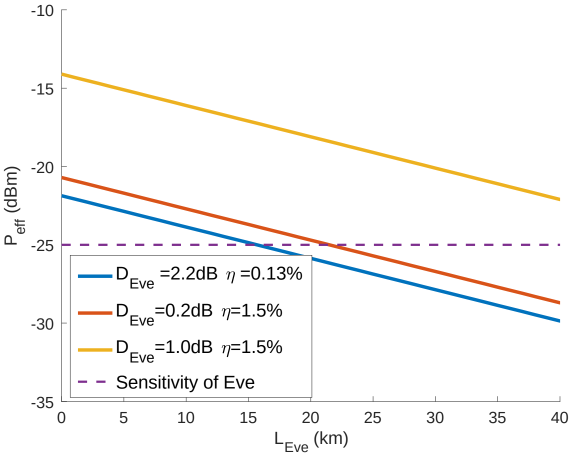

Figure 3. Input power at the Eve’s detector (P_{eff}) when using eavesdropping devices with different attenuation (D_{Eve}) and coupling efficiency ($\grave{\eta}$).

III. Measurement and discussion

To investigate the practical difficulty of coupling out the light from a G.652 and a G.657 fibre, we experimentally characterize the value of the power of the outcoupled light bending the fibres with different radii and angles. Two telecommunication wavelengths, i.e., 1550 nm and 1310 nm, are tested. The same commercial clip-on eavesdropping device described in Sec II [6] is used as a reference where the considered bend radius is 3.1 mm, while the bend angle is 36 degrees. The measured attenuation and efficiency at wavelengths 1310 nm and 1550 nm of the clip-on device are shown in Table II. To characterize the G.652 and G.657 fibres, we set the bend angles to 10, 20, 30, 40, 50, and 60 degrees with a bend radius of 2 and 10 mm, respectively. A 3D-printed test rig is used to bend the fibres to the desired values of the radius and angle. A power meter (mPm-100 Notice Korea) with a resolution of 0.01 dB and an accuracy of ± 5% is used for the measurement [7].

Table II. Attenuation and coupling efficiency of clip-on eavesdropping device [6]

Wavelength / Fibre type	1310 nm		1550 nm	
	attenuation	$\grave{\eta}$ (%)	attenuation	$\grave{\eta}$ (%)
G.652	2.2 dB	0.13	5.2 dB	1.05
G.657	0.3 dB	0.0001	1.5 dB	0.001

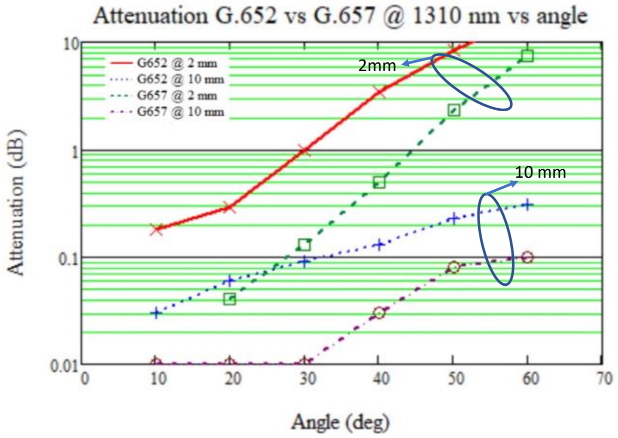

Figure 4. Attenuation caused by fibre bends on G.652 and G.657 fibre at 1310nm.

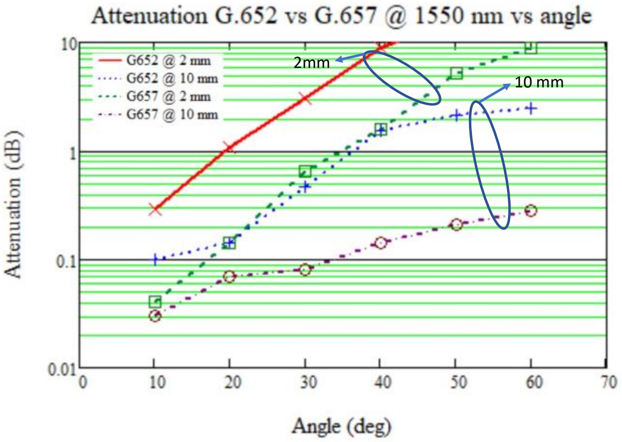

Figure 5. Attenuation caused by fibre bends on G.652 and G.657 fibre at 1550 nm.

Figure 4 shows the attenuation caused by fibre bends on G.652 and G.657 fibre at 1310 nm. To reach 1 dB attenuation at the wavelength of 1310 nm, a G.652 fibre needs to be bent at an angle of 30 degrees when the bend radius is 2 mm. With the same bend radius value (i.e., 2 mm), a G.657 fibre needs to be bent at 45 degrees to reach the same attenuation. With a bend radius of 10 mm, a G.652 fibre needs to be bent at 45 degrees to introduce 0.2 dB of attenuation, while a G.657 fibre needs to be bent at an angle larger than 60 degrees.

The attenuation measurement of the two fibre types using the 1550 nm wavelength is shown in Fig. 5. When using a bend radius of 2 mm, the G.652 fibre needs to be bent at an angle of 20 degrees, while the G.657 fibre needs 35 degrees bending to introduce 1 dB attenuation. To introduce 0.2 dB attenuation with a bend radius of 10 mm, a bend angle of 23 degrees is needed with a G.652 fibre and 50 degrees with a G.657 fibre.

The value of the attenuation due to the bending radius and bending angle shown in the figures is somehow fluctuating. This is caused by mode interference through back reflections in the passage through the cladding and the 250 µm coating [3]. We notice that a G.657 fibre needs to be bent to a sharper angle with both wavelength values to introduce the same attenuation as in a G.652 fibre. A sharper bend angle would facilitate the design of a more efficient coupling scheme that focuses the outcoupled light on Eve's photodetector. With a higher $\grave{\eta}$, Eve can collect more power at the same attenuation that Alice experiences. In this sense, eavesdropping over a G.657 fibre is more effortless than over a G.657 fibre, even if the induced power attenuation remains the same.

IV. CONCLUSIONS

Every attempt to eavesdrop an optical fibre will cause increased attenuation at the receiver side of the transmission system. Therefore, the eavesdropper needs to introduce low attenuation (below the threshold) not to be detected.

In this paper, we analyse the conditions of eavesdropping through fibre bending. Characterization of fibre bend induced attenuation with different bend radii and bend angles over G.652 and G.657 fibres is carried out. The results show that it is feasible to couple out optical power from single mode fibres G.652 and G.657 and detect the signal transmitted at 10 Gbit/s over 40 km.

The introduced attenuation can be as low as 0.2 dB at the system receiver, provided that the efficiency to detect the eavesdropped optical power can be above 1.5 %. The G.657 fibres need to be bent at a sharper angle than G.652 fibres. This implies a more efficient detection of the out coupled light. Consequently, it is easier to eavesdrop G.657 than G.652 seamlessly. This leads to the recommendation for a higher level of security to reduce the risk for eavesdropping when G.652 fibres are used.

This paper also shows that the power level measurement at the system receiver is not sufficient for efficient eavesdrop detection. Thus, there is a need for other techniques which would be more effective in detecting a signature of the eavesdropping.

ACKNOWLEDGMENT

Thanks to VINNOVA, CELTIC-Plus AI-NEXT PROTECT, and FMV for supporting this work. Special thanks to Micropol Fiberoptics AB, who provided the mechanical arrangements for bending the fibres.

REFERENCES

[1] M. Zafar Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," *8th Int. Conf. High-Capacity Opt. Networks Emerg. Technol. HONET 2011*, pp. 164–168, 2011.

[2] D. Marcuse, "Curvature loss formula for optical fibers," *J. Opt. Soc. Am.*, vol. 66, no. 3, pp. 216–220, Mar. 1976.

[3] A. Harris and P. Castle, "Bend loss measurements on high numerical aperture single-mode fibers as a function of wavelength and bend radius," *J. Light. Technol.*, vol. 4, no. 1, pp. 34–40, 1986.

[4] Cisco SFP-10G-ZR100FM, available online: https://www.fiber-mart.com/datasheet/SFP-10G-ZR100FM.pdf

[5] Optilab, EDFA-25P-C-M, available online: https://www.oequest.com/getDatasheet/id/10747-10747.pdf

[6] FOD, Clip-On Coupler FOD 5503, available online: fods.com/optic_clip_on_coupler.html

[7] Noticekorea, mini power meter: MPM-100, available online: http://www.noticekorea.com/?p=2336&ckattempt=1