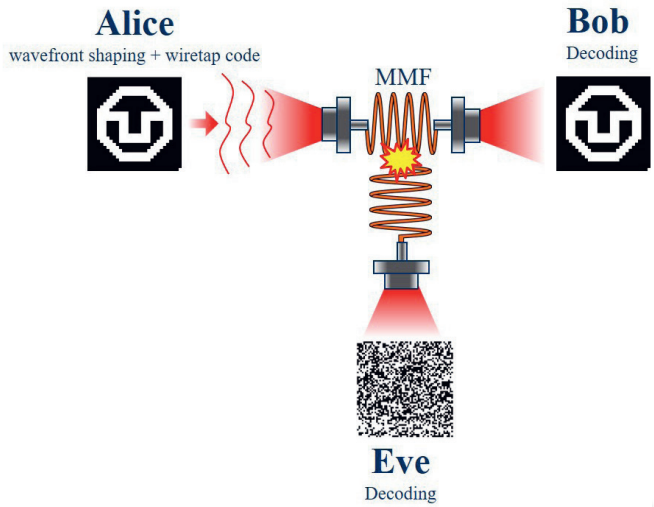
Dresdner Berichte zur Messsystemtechnik

Herausgeber: Prof. Dr.-Ing. habil. Jürgen Czarske

20

Stefan Rothe

Harnessing Disorder of Multimode Fibres to Achieve Information Security on the Physical Layer



SHAKER VERLAG

MST
Professur für
Mess- und Sensorsystemtechnik

Technische Universität Dresden

Harnessing Disorder of Multimode Fibres to Achieve Information Security on the Physical Layer

Dipl.-Ing.
Stefan Rothe
Geboren am 21.12.1992 in Mainz

der Fakultät Elektrotechnik und Informationstechnik der Technischen Universität Dresden

zur Erlangung des akademischen Grades
Doktoringenieur
(Dr.-Ing.)

genehmigte Dissertation

Vorsitzender:	Prof. Dr.-Ing. Dr. h.c. Frank H. P. Fitzek	Tag der Einreichung	01.11.2022
Gutachter:	Prof. Dr.-Ing. habil. Jürgen W. Czarske	Tag der Verteidigung	23.02.2023
	Prof. Dr. Tomáš Čižmár		
	Prof. Dr.-Ing. Eduard A. Jorswieck		

Dresdner Berichte zur Messsystemtechnik

Band 20

Stefan Rothe

Harnessing Disorder of Multimode Fibres to Achieve Information Security on the Physical Layer

Shaker Verlag
Düren 2023

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Dresden, Techn. Univ., Diss., 2023

Printed in Germany.

ISBN 978-3-8440-9123-6
ISSN 1866-5519

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren
Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9
Internet: www.shaker.de • e-mail: info@shaker.de

I ain't here to break it,

just see how far it will bend.

— Joshua Homme

A great songwriter and presumably a fibre enthusiast.

Kurzfassung

Digitale Kommunikationstechniken haben das Leben innerhalb kürzester Zeit maßgeblich verändert und beeinflussen es in allen Bereichen. Dadurch steigt die Gefahr neuartiger Cyberangriffe rapide an und erfordert neue Methoden digitale Sicherheit zu gewährleisten. Als Rückgrat der globalen Digital-Infrastruktur stellen optische Kommunikationsnetze eine besonders sensible Umgebung dar. Die Multimodefaser repräsentiert hierbei einen vielversprechenden Verbindungstyp, da ihre räumlichen Pfade Netzkapazitäten signifikant anheben können. In dieser Dissertation wird ein Ansatz untersucht, mit dem ein informationstheoretisch sicherer Datenaustausch in optischen Multimodefasern erreichbar ist, indem physikalische Phänomene im Faserkanal nutzbar gemacht werden. Die Idee ist, dass die inhärente Unordnung in der Multimodefaser von einer Senderin (Alice) ausgenutzt wird, um einem legitimierten Nachrichtenempfänger (Bob) einen entscheidenden Vorteil gegenüber einer Abhörerin (Eve) zu verschaffen. Der Schlüssel sind Modenmischung, sowie modenabhängige Verluste, welche zu einem Ungleichgewicht unter verteilten Empfängern auf dem Faserkanal führen. Folglich gilt eine Entzerrung zwischen Alice und Bob zwingenderweise nicht für Eve. Diese Technik wird Sicherheit auf der Übertragungsschicht (engl.: *physical layer security*) genannt und wurde experimentell erstmalig in einer Multimodefaser umgesetzt. Durch die Messung der optischen Transmissionsmatrix können Alice und Bob einerseits ihren Kanal für eine Kalibrierung charakterisieren und andererseits geeignete räumliche Pfade identifizieren. Hierfür wurden sowohl holografische Methoden, als auch intelligente Techniken auf Basis neuronaler Netze untersucht und gegenübergestellt. Mit der TranSmissionsmatrix können Alice und Bob eine sendeseitige Vorverzerrung bestimmen, um die Lichtausbreitung durch die Faser zu kontrollieren und gezielt Informationen auszutauschen. Eve hingegen muss ihren Kanal mathematisch weiterverarbeiten. Geschickte Sendestrategien können diese Asymmetrie ausnutzen. Hierfür wurde ein Abhörexperiment durchgeführt, in dem sich Bob und Eve jeweils 50 % der übertragenen Leistung von einer 55 Moden führenden Multimodefaser teilen. Es wird gezeigt, dass mittels spezieller Kanalkodierungen ein informationstheoretisch sicherer Datenaustausch erreicht werden kann, bei dem pro Kanalnutzung 2 Bit sicher übertragen werden können, obwohl Eve über Wissen sämtlicher Kanalzustände verfügt. Perspektivisch könnte die erreichbare Informationssicherheit weiter angehoben werden, indem Effekte zu induziertem Modenmischen oder zeitlich veränderlichen Übertragungseigenschaften im Faserkanal untersucht werden. Durch Fasern mit D-Profil oder externe mechanische Einflüsse wie Biegung oder Verdrillung können Modenmischung oder eine Zeitvarianz provoziert werden. Die Ergebnisse dieser Dissertation weisen erstmalig die experimentelle Umsetzbarkeit von physical layer security an einem Multimodefaserkanal nach und zeigen eine Ergänzung zur sicheren Datenübertragung in optischen Kommunikationsnetzen zukünftiger Infrastrukturen, die räumliche Informationspfade nutzen.

Abstract

Digital communication has changed life considerably in a short time and has an impact on all domains. As a result, the risk of novel cyber attacks is increasing rapidly and requires new methods to ensure information security. In particular, optical communication networks have become a crucial environment, because they represent the backbone of the global digital infrastructure. Multimode fibres are a promising link type in this context, as its spatial paths can enhance network capacities significantly. This dissertation investigates an approach to achieve information-theoretic secure data exchange in optical multimode fibres by utilising physical effects in the fibre channel. The objective is for a transmitter (Alice) to exploit inherent disorder in multimode fibre to offer a legitimate message receiver (Bob) a decisive advantage over an eavesdropper (Eve). The clue relies on both modal crosstalk as well as mode-dependent loss that lead to an imbalance among distributed receivers on the fibre channel. Consequently, equalisation between Alice and Bob necessarily does not apply to Eve. This technique is called physical layer security and is experimentally implemented on a multimode fibre for the first time. By measuring the optical transmission matrix, Alice and Bob can characterise their channel for calibration and identify suitable spatial paths. For this purpose, both holographic methods and smart techniques based on neural networks are investigated and compared. By using the tranmsission matrix, Alice and Bob can determine an optical pre-distortion for controlling light propagation through the fibre and exchange information. In turn, Eve must process her channel mathematically. This asymmetry can provide benefit by implementation of sophisticated transmission strategies. Therefore, an attacking experiment was carried out in which Bob and Eve share 50 % each of the transmitted power of a 55-mode fibre. It is shown that through implementation of special channel coding an information-theoretic secure data exchange can be achieved in which 2 bit can be securely transmitted per channel use, although Eve has complete channel state information. Prospectively, the achievable information security could be further enhanced by investigating effects on induced mode mixing or time-varying transmission properties in the fibre channel. D-shaped fibres or external mechanical influences such as bending or twisting can introduce mode mixing or time variance. The results obtained in this dissertation demonstrate the experimental feasibility of physical layer security on a multimode fibre channel for the first time and provide a complement for secure data transmission in optical communication networks of future infrastructures that use spatial information paths.

Acknowledgement

This thesis was written at the Chair of Measurement and Sensor System Technique at TU Dresden. I would like to express my special thanks to the chair holder and my doctoral supervisor Prof. Dr.-Ing. habil. Jürgen Czarske, who made it possible for me to conduct this work at his chair and always offered me his support. I am very grateful for the numerous helpful advises and the constructive discussions on my research. I would also like to express my gratitude for the support I received during my research stay abroad and for the opportunity to attend international conferences. I would also like to thank Prof. Dr.-Ing. Eduard Jorswieck for providing a review and for the great cooperation in the joint research project, which he pushed forward with sophisticated ideas and suggestions. I would like to thank Prof. Dr. Tomáš Čižmár for reviewing my thesis.

Special thanks are due to my group leader and office mate Neki. I greatly appreciate his valuable advises and support in the lab, but also off work as a mentor. I sincerely want to acknowledge him for supporting me in all my ideas and projects. Most of them, I hope, are not gammel. I would like to considerably mention the fact that he raised the project funds together with my former Diploma thesis supervisor Hannes. The outlined project idea has been the foundation for this thesis. In particular, Hannes' infinite expertise and creativity helped me immensely in getting started with the topic. With his tireless helpfulness, he significantly predetermined the direction of this project. I would also like to highlight the fruitful and inspiring exchange with my colleagues Robert, Felix, Johannes, Jiawei and Julian.

I thank all current and former staff members for both a great team spirit and working atmosphere. The professional discussions in the lab and during the coffee and lunch breaks helped me to gather ideas and solutions and had a significant influence on the direction of this thesis. I would also like to thank you for giving me so much confidence to lead our SPIE Student Chapter. The joint work was a lot of fun and I was very happy about all the lecture series, workshops and excursions. In addition, I would also like to highlight the time spent together off work. I enjoyed all the doctoral seminars, AvoBuBs, lunch and coffee breaks, project and paddle days, GFL games, barbecue evenings or red wine Wednesdays.

My sincere thanks go to my former students, who (partially) have become colleagues in the meantime, nameley Qian, Dennis, David and Anna-Lena for willing to do their theses under my supervision. The joint projects, especially on the topic of neural networks, were a lot of fun. I appreciate your eagerness and thank you for your great work.

This work resulted from a cooperation project and would not been possible without partners. My special thank goes to Karl from TU Braunschweig for his excellent

support on coding theory. I want to acknowledge the support of the German Research Foundation (DFG) for funding this collaborative project.

I would also like to thank my colleagues from University College London, namely Filipe, Fabio and Polina. I had an incredibly exciting and inspiring time at Optical Networks Group. It has been an amazing professional and personal exchange and it has been a great pleasure to work with you.

I would like to dedicate special thanks to all my friends and family. First of all, sincere thanks go to my parents, who encourage me from the first day of my life and privileged me with the curiosity to start a PhD. Thank you so much for your unconditional support in all my ways. My friends have amazingly supported me on the path of this thesis, as well. Without you and without your time and care, I would not have been able to do this. I would especially like to mention Fabian, Oliver, Konstantin, Marc, Franz and Florian as my longest friends. The security and joy you bring into life is a huge privilege and give me the required confidence to take these sometimes uncertain paths in research. I would also like to thank all my friends in Dresden and vicinity, who have accompanied and intensively supported me, especially Nico, Simon, Paul, Julian, Lourdes and Lisa.

In conclusion, I would like to express my extraordinary gratitude to my beloved partner and fiancée Marie. You are supporting me each and every day with your charming, hilarious and stunning manner. I would like to thank you for all your patience during my work and for your unconditional kindness.

Contents