Die Geheimnisse der sicheren Datenübertragung durch Glasfasern: sensible Nachrichten mittels Lichtstreuung verschlüsseln

Stefan Rothe

Deutscher Studienpreis
2. Preis Sektion Natur- und Technikwissenschaften

Wir alle vertrauen unsere sensible Daten Glasfasernetzen an, die eine ungeheure Bandbreite ermöglichen und in unserer globalisierten Welt unverzichtbar geworden sind. Allerdings sind Glasfasernetze verschiedenen Sicherheits-bedrohungen ausgesetzt. Die potenziellen Auswirkungen von Sicherheitsverletzungen reichen von finanziellen Verlusten über die Beeinträchtigung der Privatsphäre bis hin zu Bedrohungen der nationalen Sicherheit. Daher ist die Gewährleistung von Sicherheit und Verfügbarkeit bei dem Austausch sensibler Informationen von größter Bedeutung. In meiner Arbeit schlage ich einen Ansatz vor, bei dem Daten mithilfe von zerstreuten Lichtmustern verschlüsselt werden. Durch eine gezielte Lichtdurch-mischung werden Abhörer ausgetrickst und somit geheime Nachrichten in der Glasfaserleitung abgesichert. Anhand meiner Messdaten demonstriere ich einen sicheren Datenaustausch und unterstreiche das Potenzial der Methode, die bereits heute in bestehende Infrastruktur einsetzbar ist.

Stefan Rothe promovierte an der Technischen Universität Dresden im Fachgebiet Optische Messtechnik.

Körber Stiftung

Körber Stiftung

Der vorliegende Beitrag wurde beim Deutschen Studienpreis 2024 mit dem 2. Preis in der Sektion Natur- und Technikwissenschaften ausgezeichnet. Er beruht auf der 2023 an der Technischen Universität Dresden eingereichten Dissertation „Harnessing Disorder of Multimode Fibres to Achieve Information Security on the Physical Layer“ von Dr. Stefan Rothe.

Die Geheimnisse der sicheren Datenübertragung durch Glasfasern: sensible Nachrichten mittels Lichtstreuung verschlüsseln

Einleitung: Informationssicherheit in Glasfasernetzen – die Achillesferse für den Datenaustausch von Privatpersonen und kritischer Infrastruktur

In unserer digitalen Welt ist die zunehmende Ausbreitung von Glasfasernetzen selbstverständlich geworden. Glasfasernetze spielen eine zentrale Rolle bei der globalen Konnektivität, da sie einen immensen Datenaustausch ermöglichen. So werden 90 % der interkontinental ausgetauschten Daten über Glasfaserkabel transportiert, die sich auch quer durch unsere Ozeane erstrecken. Da unsere Gesellschaft bei der Übertragung großer Mengen sensibler Informationen von persönlichen Daten bis hin zur Kommunikation mit kritischen Infrastrukturen zunehmend von diesen Netzen abhängig ist, war der Bedarf an widerstandsfähigen Maßnahmen zur Gewährleistung von Informationssicherheit noch nie so groß wie heute.

Glasfasernetze nutzen Lichtsignale zur Übertragung von Daten und zeichnen sich durch ihre einzigartige (Licht-)Geschwindigkeit und Bandbreite aus. Daher sind sie für moderne Kommunikationssysteme unverzichtbar, aber diese Effizienz macht sie auch anfällig für eine Vielzahl von Sicherheitsbedrohungen. Cyberangriffe werden immer raffinierter, weshalb der Schutz der Vertraulichkeit (*Sicherheit*) und Verfügbarkeit (*Reliabilität*) von Informationen, die diese Netze durchqueren, von größter Bedeutung ist.

Die potenziellen Auswirkungen von Sicherheitsverletzungen in Kommunikationsnetzen reichen von finanziellen Verlusten über die Beeinträchtigung der Privatsphäre bis hin zu Bedrohungen der nationalen Sicherheit. Da Unternehmen, Regierungen und Privatpersonen Glasfasernetzen zunehmend ihre sensiblen Daten anvertrauen, ist die Gewährleistung, dass ein Datenaustausch vor böswilligen Akteuren geschützt ist, ein grundlegendes Anliegen der Gesellschaft.

Jedoch existiert bis zum heutigen Tag keine marktreife Methode, mit der unsere Daten zu 100 % sicher verschickt werden können. Daher erfordert der Schutz vor potenziellen Bedrohungen in Glasfasernetzen (und auch anderen Netzwerken) ein ganzheitliches Konzept, das auf gleich mehreren Netzwerkebenen ansetzt.

Verschlüsselungsprotokolle, robuste Authentifizierungsmechanismen, eine kontinuierliche Überwachung zur Erkennung und Entschärfung von Gefahren sowie die physikalischen Lichtsignale, die das Glasfaserkabel durchqueren, bilden einen umfangreichen Maßnahmenkatalog zur Gewährleistung von Sicherheit unserer Daten. Indem wir diese Herausforderungen aktiv angehen und selbst gestalten, können wir garantieren, dass unsere Glasfasernetze weiterhin als zuverlässige Kanäle für den Informationsaustausch dienen, ohne dabei Vertrauen zu gefährden, auf das unsere digital vernetzte Gesellschaft angewiesen ist.

Zerstreuung von Licht in ungeordneten Glasfasern – ein vielversprechendes Konzept für eine neue Verschlüsselungsmethode

Vor allem in drahtlosen Kommunikationsnetzen hat sich der Ansatz namens *Physical Layer Security* (PLS) zur Stärkung der Schutzmaßnahmen und zur Gewährleistung der Informationssicherheit erwiesen. PLS basiert auf dem Prinzip, die zugrunde liegenden Eigenschaften auf der physikalischen Ebene von Kommunikationsnetzen nutzbar zu machen. In einfachen Worten heißt das, dass die physikalischen Gesetze des Übertragungskanals, wie bspw. die Lichtleitung durch eine Glasfaser, geschickt ausgenutzt werden, um eine sichere Datenverbindung aufzubauen. Mit dieser Technik wird Information „physikalisch verschlüsselt“. Dieses Konzept kann den Sicherheitsstandard in unseren Kommunikationsnetzen über die traditionellen kryptografischen Methoden hinaus verbessern, jedoch wurde PLS bislang noch nicht für Glasfasern untersucht.

Aber auch für Glasfasernetze bietet PLS ein enormes Potenzial. Im Kern erkennt PLS an, dass die physikalischen Eigenschaften der Lichtleitung, wie bspw. Lichtdämpfung, -streuung und Rauschen, gezielt genutzt werden können, um Abhörversuche zu vereiteln und potenzielle Gefahren zu entschärfen. Durch die Integration von PLS in den Bau von Glasfasernetzen können Unternehmen oder nationale Einrichtungen ihre Sicherheitslage um eine zusätzliche Schutzebene erweitern, die die bestehenden Verschlüsselungsprotokolle ergänzt.

Eine herausragende Technik im Rahmen von PLS ist die Quantenschlüsselverteilung (Quantum Key Distribution, QKD), die sich die Prinzipien der Quantenmechanik

zunutze macht, um sichere kryptografische Schlüssel zwischen kommunizierenden Parteien zu erstellen. QKD nutzt die Eigenschaften von Quantenzuständen, wie Superposition und Verschränkung, um Sicherheitsschlüssel zu erzeugen, die von Natur aus gegen Abhörer resistent sind. Es ist jedoch zu beachten, dass QKD zwar ein äußerst vielversprechendes Konzept ist, die praktische Umsetzung jedoch noch in den Kinderschuhen steckt. Die Quantenschlüsselraten liegen derzeit um mehrere Größenordnungen unterhalb konventioneller Datenraten, was eine kommerzielle Einführung vor erhebliche Herausforderungen stellt. Aus diesem Grund müssen alternative Technologien erforscht werden, um die Informationssicherheit in Glasfasernetzen zu erhöhen.

Eine solche Alternative besteht in der Erforschung von ungeordneten Glasfasern wie der Multimodefaser (MMF). Mit der MMF können mehrere Lichtstrahlen nebeneinander übertragen werden, wodurch sich vielversprechendes Potenzial ergibt, die Datenübertragungskapazität in Glasfasernetzen signifikant zu erhöhen. Aus diesem Grund liegen bereits heute enorme Mengen MMF in Rechenzentren, wo ein besonders hoher Bedarf an Bandbreite auf vergleichsweise kurzen Übertragungsstrecken erforderlich ist. Gleichzeitig werden die Lichtstrahlen auf ihrem Weg durch die MMF durchmischt, bzw. zerstreut, und gedämpft, was eine einzigartige Eigenschaft dieses Fasertyps ist. Diese Unordnung innerhalb der MMF wurde jahrzehntelang als Nachteil angesehen, ist aber die wertvolle Ressource für den Einsatz von PLS! Besonders spannend ist hierbei, dass PLS in der MMF mit klassischen Komponenten unserer Glasfaserinfrastruktur vereinbar ist, also nach dem heutigen Stand der Technik realisierbar ist.

Daher lautet die wissenschaftliche Fragestellung meiner Dissertation: Wie kann ein echtes PLS-System aufgebaut werden, mit dem Daten zuverlässig und sicher durch eine ungeordnete MMF transportiert werden? Welche PLS-Strategien können genau implementiert werden?

Analyse von ungeordneten Glasfasern: Wie kann zerstreutes Licht sinnvoll nutzbar gemacht werden?

In einer Glasfaser wird Licht durch den Kern, einen dünnen Glasstrang in der Fasermitte, geleitet. Der Kern ist von einem Mantel umgeben, der das Licht im Kern einschließt. Denn an der Grenze zwischen Kern und Mantel wird eingekoppeltes Licht immer wieder reflektiert und breitet sich somit durch den Faserkern aus. Besonders an der MMF ist, dass sich Licht auf mehreren Wegen parallel ausbreiten kann – anders als

bei der Singlemodefaser, bei der sich Licht nur auf einem möglichen Weg bewegen kann, nämlich entlang der Faserhauptachse. Die MMF hingegen ist meist mit einem etwas größeren Kerndurchmesser ausgestattet, sodass für die sich ausbreitenden Lichtstrahlen mehr Platz vorhanden ist und auch andere nebeneinanderliegende Ausbreitungspfade möglich sind. Somit kann ein ankommender Lichtstrahl nicht nur entlang der Hauptachse, sondern auch im Zickzack entlang der Kern-Mantel-Grenze hin und her reflektieren.

Aufgrund von Weglängenunterschieden vermischen sich jedoch die einzelnen Lichtpfade in der MMF, und es entstehen einzigartige, zerstreute Lichtmuster. Wird bspw. ein Lichtfokus am Fasereingang eingekoppelt, entsteht am Ausgang eine chaotisch erscheinende, granulierte Lichtstruktur ein sogenanntes Specklemuster. Zusätzlich wird Licht auf den verschiedenen Pfaden unterschiedlich stark gedämpft. Diese Streu- und Dämpfungseigenschaften machen die MMF zu einer ungeordneten Glasfaser, und das Licht, dass die Faser verlässt, scheint ein reines Chaos zu sein. Aber wie kann diese Unordnung nun für PLS genutzt werden? Hierfür muss zuerst die Lichtleitung, also das gesamte Lichtübertragungsverhalten der MMF, untersucht werden, um anschließend Ordnung in das Chaos zu bringen.

Daher habe ich ein Experiment entworfen, mit dem die Lichtübertragung in der MMF analysiert werden kann. Zu diesem Zweck muss nacheinander jeder einzelne Lichtpfad nacheinander auf der Eingangsseite der MMF eingekoppelt, und es müssen am Faserausgang die zerstreuten und gedämpften Specklemuster gemessen werden. Jeder einzelne Lichtpfad produziert dabei sein eigenes Specklemuster. Für die gezielte Anregung der Lichtpfade wird häufig ein räumlicher Lichtmodulator (engl. Spatial Light Modulator, SLM) verwendet, mit dem sich beliebige Lichtprofile erzeugen lassen – quasi ein hochgenauer Beamer, mit dessen Hilfe ich jeden einzelnen Lichtpfad in dem haardünnen Glasfaserkern einkoppeln kann. Für die Messung der Specklemuster auf der MMF-Ausgangsseite dient eine einfache Kamera, mit der ich Bilder der Specklemuster aufnehme und anschließend auswerte.

Sind einmal alle Lichtpfade eingekoppelt und die zugehörigen Specklemuster aufgenommen, ist die MMF fertig analysiert, und ich weiß, wie sich Licht durch die MMF ausbreitet. Also kenne ich mich in dem Chaos aus, sodass ich nun Ordnung hineinbringen kann!

Die Lauscherin austricksen: Ordnung in das Chaos bringen und Daten abhörsicher austauschen

Glasfasern haben die besondere Eigenschaft, dass ihre Lichtleitung umkehrbar und die Unordnung korrigierbar ist. Wird ein Specklemuster auf der Ausgangsseite als Resultat eines eingangsseitig eingekoppelten Lichtfokus empfangen und genauso wieder in die MMF zurückgeschickt, entsteht auf der Eingangsseite wieder der Fokus. Das Licht nimmt nämlich wieder den exakt gleichen Weg in die andere Richtung, und die Lichtstreuung kann rückgängig gemacht werden. Für diese Korrektur wird mit dem SLM das Specklemuster geformt, welches nun wieder eingekoppelt wird und den Fokus auf der gegenüberliegenden Glasfaserseite erzeugt. Wie kann aber diese Technik für einen sicheren Datentransport durch die MMF genutzt werden?

Die Umkehrung der Streuung kann auch von nur einer Seite aus durchgeführt werden, indem wir unser Vorwissen über die MMF nutzen. Da jeder Lichtpfad in der MMF sein eigenes Specklemuster produziert und die Unordnung bekannt ist, ist es einer Senderin Alice möglich, ihre Nachricht so schicken, dass der Empfänger Bob einen Lichtfokus erhält, ohne dass er etwas im Voraus schicken muss. Dabei sendet Alice ein zu der bekannten Unordnung komplementäres Specklemuster, welches als geordneter Fokus (oder ein beliebig anderes Muster) bei Bob ankommt.

Wie kann aber Alice etwas an Bob schicken, das nun abhörsicher ist? Dafür muss Alice sicherstellen, dass eine Lauscherin Eve, die sich an die Glasfaser zwischen Alice und Bob koppelt, die geheime Nachricht nicht entschlüsseln kann. Koppelt Eve ihre eigene Glasfaser an die Glasfaser zwischen Alice und Bob an, entstehen hinter der Koppelstelle zwei unterschiedliche Lichtleitungen mit unterschiedlichen Eigenschaften: eine Leitung zwischen Alice und Bob sowie eine zwischen Alice und Eve. Was sich Alice und Bob nun zunutze machen, sind die äußerst diversen Eigenschaften der Lichtpfade in den zwei Leitungen. Einige Pfade neigen eher zur Streuung oder zur Dämpfung als andere. Genauso gibt es Pfade, die an der Abbiegung zwischen Bob und Eves Glasfaser eher die Leitung zu Bob und nicht zu Eve (bzw. umgekehrt) nehmen: Es gibt also „gute“ und „schlechte“ Pfade. Kennt Alice die Eigenschaften beider Lichtleitungen, also sowohl die zu Bob als auch die zu Eve, kann sie besonders sichere Lichtpfade ermitteln. Das sind genau die Pfade, die besonders gut für Bob, aber gleichzeitig schlecht für Eve sind. Da auch beide Lichtleitungen unterschiedlich sind, hat Alice die Möglichkeit, Ordnung in nur eine der beiden Leitungen zu bringen. Korrigiert Alice nun die Lichtübertragung zu Bob und sendet ihm einen Fokus, gilt das nicht für Eve, die weiterhin ein Specklemuster sieht. Alice kann also bei einer ungeordneten

Glasfaser ihre geheime Nachricht nur für bestimmte Empfänger entschlüsselt schicken alle anderen erhalten stets ein verschlüsseltes Specklemuster!

Diese Technik kann nun weiter auf die Spitze getrieben werden und eine maßgeschneiderte Sendestrategie ermittelt werden. Alice hat hierfür die Aufgabe, optimale Pfade für ihr Glasfasernetz mithilfe ihrer Analyse über beide Lichtleitungen zu ermitteln, sodass Eves Möglichkeiten zur Entschlüsselung minimal sind.

In meinem Promotionsprojekt habe ich verschiedene Methoden experimentell ausgetestet. Die vielversprechendste Methode ist die Anwendung von sogenannten Kanalkodierungen. Diese Kodierungen gehören nicht zum Bereich der klassischen Kryptografie, sondern sind errechenbare Sendestrategien, die mit Alice Analyse über ihre Glasfaser angefertigt werden. Ziel dieser Kodierung ist, dass Bob mit möglichst hoher Wahrscheinlichkeit Daten fehlerfrei empfängt, Eve aber gleichzeitig mit möglichst geringer Wahrscheinlichkeit Daten rekonstruieren kann. Dabei werden die „guten“ Pfade zwischen Alice und Bob bevorzugt, oder auch bspw. sogenannte „Dummy-Bits“ gesendet, um Eve zu irritieren. Diese Methodik ist in Drahtlosnetzwerken bereits etablierter Gegenstand aktueller Forschung, aber noch völlig unbekannt für Glasfaserkanäle. Im Rahmen meines Projekts konnte ich Kanalkodierungen erstmalig in einer Laboranwendung an einer MMF einsetzen und den experimentellen Nachweis erbringen, dass sie sich für einen sicheren Datentransfer eignen. So konnte als Ergebnis festgehalten werden, dass eine geheime Nachricht zwischen Alice und Bob fehlerfrei durch die Glasfaser ausgetauscht wird, während Eve nur Rauschen empfängt und die geheime Nachricht nicht entschlüsseln kann.

Für dieses Experiment habe ich das Logo der TU Dresden als geheime Nachricht gewählt, das aus einer Folge von „0“ und „1“ besteht, die nacheinander von Alice gesendet werden (siehe Abbildung 1a). Wenn Alice die Leitung zu Bob korrigiert und die guten Pfade wählt, aber keine spezielle Kodierung verwendet, erhält Bob das Logo aus Abbildung 1b und Eve die Version aus Abbildung 1c. An dieser Stelle ist bereits eine Diskrepanz zwischen den empfangenen Nachrichten auf Bobs und Eves Seite zu erkennen, da Alice die guten Kanäle für Bob wählt. Eve kann jedoch nach wie vor Teile des Logos erkennen und hat Information abgegriffen. Die Verbindung zwischen Alice und Bob darf daher nicht als sicher angenommen werden. Verwendet Alice allerdings Kanalkodierungen und nutzt eine optimierte Sendestrategie, dann ergeben sich die empfangenen Nachrichten aus Abbildung 1d und Abbildung 1e für Bob bzw. Eve. Hier ist zu sehen, dass Bob eine nahezu perfekte Rekonstruktion erhält, Eve aber nur Rauschen detektiert. Diese zwei Kriterien, Reliabilität (Alice sendet Information zu Bob)

und Sicherheit (Alice sendet keine Information zu Eve), sind somit durch den vorgestellten Ansatz erreicht.

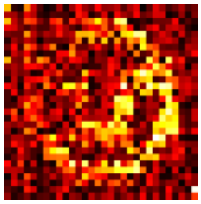
(a)  (b)  (c)  (d)  (e) 

Abbildung 1 *Gemessene Daten im Experiment. (a) geheime Nachricht von Alice – das TU-Dresden-Logo. (b) Von Bob empfangene Nachricht ohne Kanalkodierung. (c) Von Eve empfangene Nachricht ohne Kanalkodierung. (d) Von Bob empfangene Nachricht unter Verwendung von Kanalkodierungen. (e) Von Eve empfangene Nachricht unter Verwendung von Kanalkodierungen.*

Quintessenz: Ist nun alles sicher?

Die Messergebnisse meiner Arbeit zeigen, dass es mithilfe von Physical Layer Security (PLS) tatsächlich möglich ist, eine sichere Datenleitung durch eine Glasfaser herzustellen. Auf dem Weg zu einer echten Anwendung ist es wichtig, das Grundlagenexperiment schrittweise um weitere Netzwerkkomponenten wie Switches, Router oder Verstärker zu erweitern, um die Netzwerktauglichkeit nachzuweisen. Genau dieser Aspekt kann sich allerdings als Stärke von PLS gegenüber quantenbasierten Ansätzen herausstellen. Besonders vielversprechend ist nämlich, dass die erforderlichen Komponenten (Laser, Detektor, Faser etc.) kommerziell erhältlich sind und keine Rücksicht auf spezielle Lichterscheinungen wie bspw. Quantenzustände genommen werden muss. Das ermöglicht prinzipiell die Integrierbarkeit in bereits vorhandene Infrastrukturen, wo Glasfasern verlegt sind. Die für den Einsatz von PLS erforderliche Multimodefaser (MMF) ist bspw. vor allem in Rechenzentren verlegt, da sie auf den relativ kurzen Verbindungsstrecken (wenige Kilometer) im Vergleich zu Langstrecken-Glasfasern (mehrere Tausend Kilometer) effizienter ist. Da insbesondere Rechenzentren durch das immense Datenaufkommen als kritische Infrastruktur gelten, ist hier eine Anwendung von PLS als besonders sinnvoll einzuschätzen.

In meinem Experiment habe ich MMFs von bis zu 100 m Länge untersucht. Längere Faserverbindungen im Kilometerbereich sind ohne grundlegende Hürden möglich, waren aber nicht Gegenstand meiner Untersuchungen. Andere Gruppen konnten Lichtkorrekturen, wie sie für den von mir vorgestellten Ansatz von PLS erforderlich sind, durch die MMF mit mehreren Kilometern Faserlänge zeigen. Für Strecken von vielen Tausend Kilometern Länge werden derzeit spezielle MMFs mit mehreren Kernen und weniger Lichtpfaden pro Kern untersucht, die ähnlich effizient sind wie die Standard-

Langstreckenfasern. Der Einsatz von PLS ist mit solchen Spezialfasern prinzipiell möglich und kann auch dort untersucht werden.

Des Weiteren muss herausgefunden werden, wie die MMF in einer realen Infrastruktur mit echten äußeren Störungen außerhalb des Labors reagiert. Die Eigenschaften der Lichtleitung ändern sich durch mechanische Störeinflüsse, was von Alice und Bob beim Datenaustausch berücksichtigt werden muss. Das Problem ist nämlich, dass die von Alice angenommene Korrektur zu Bob nicht mehr stimmt, wenn sich die Eigenschaften der Lichtleitung geändert haben. Wenn PLS in einem echten Fasernetz integriert werden soll, muss es robust gegenüber Vibrationen und Erschütterungen sein, wenn die Faser bspw. entlang einer befahrenen Straße verlegt ist. Hier ist es wichtig zu klären, ob auch trotz Störfaktoren aus unserer Umwelt die Lichtleitung zwischen Alice und Bob kontinuierlich neu analysiert werden kann, um einen sicheren Kanal zu gewährleisten. Als Abschätzung gilt hier, dass eine Neuvermessung schneller erfolgen muss, als sich das Übertragungsverhalten innerhalb der MMF ändert.

Zusätzlich besteht noch Forschungsbedarf auf der theoretischen Seite von PLS. Die Kanalkodierungen, die in meinem Projekt verwendet wurden, erfordern Wissen über die Leitung zur Lauscherin Eve, was in einer echten Anwendung unrealistisch ist. Es ist daher wichtig, Methoden zu erforschen, mit denen lediglich ein paar wenige Parameter angenommen werden müssen, um ein hohes Maß an Sicherheit zu erreichen.

Während es die Physik von Quantenzuständen per se unmöglich macht, einen Quantenschlüssel zu knacken, besteht bei PLS bislang nur eine beweisbare Sicherheit (informationstheoretische Sicherheit) für den akademischen Fall, dass unendlich lange Kodierungen verwendet werden, also aus einer geheimen Nachricht ein Kode-Wort mit unendlich vielen Elementen gemacht wird. Für realistische Nachrichtenlängen, die endlich sind, ist der Nachweis für informationstheoretische Sicherheit noch ausstehend. Man kann jedoch für eine bestimmte Anwendung, wie in dem von mir durchgeführten Experiment, eine vorliegende Sicherheit empirisch ermitteln. Laut dieser Kennzahl kann Eve nur mit einer bestimmten, möglichst geringen Wahrscheinlichkeit Daten extrahieren. Je nach Anwendungsfall und Sicherheitsrisiko kann mit PLS zu unterschiedlich komplexen und rechenintensiven Kanalkodierungen gegriffen werden, um eine geforderte Schwelle an Sicherheit nicht zu unterschreiten.

Insgesamt zeigt mein Promotionsprojekt, dass sich in ungeordneten Glasfasern mithilfe von gezielter Lichtformung eine sichere Datenleitung erreichen lässt. Ein entscheidender Vorteil dieses Ansatzes ist, dass alle benötigten Komponenten dem

heutigen Stand der Technik entsprechen und für eine Realisierung verwendet werden können. Somit bietet der Einsatz von MMF einen weiteren Sicherheitsaspekt in einem Glasfasernetz und bereits heute eine leistungsfähige Ergänzung zu anderen Sicherheitsmethoden wie Kryptografie.