KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1990/1991
Leitung:
Bundesamt für Übermittlungstruppen
Divisionär J. Biedermann, Waffenchef der Übermittlungstruppen

Abhörsicherheit von Glasfaserübertragungssystemen

Referent: Roland Karl Staubli, Dipl. El. Ing. ETH

ABHÖRSICHERHEIT VON GLASFASER-ÜBERTRAGUNGSSYSTEMEN

R.K. Staubli, Dipl. El-Ing. ETH

INHALTSVERZEICHNIS

Adresse des Autors:

Roland K. Staubli
Institut für Kommunikationstechnik
ETH-Zentrum
8092 Zürich

"Krieg im Aether", Folge XXX, 1991

56354

1. EINLEITUNG

Immer mehr verdrängen optische Datenübertragungssysteme die konventionellen elektrischen Uebertragungseinrichtungen. Die bedeutendsten Vorteile der optischen Uebertragungstechnik sind die extrem grossen Uebertragungskapazitäten, die geringe Signaldämpfung in der Glasfaser (grosse zwischenverstärkerfreie Uebertragungsdistanzen), die Unempfindlichkeit gegenüber elektromagnetischen Interferenzen, das geringe Gewicht und die kleinen Abmessungen der Glasfaserkabel, der günstige Faserpreis sowie auch der oft hervorgehobene inhärente Schutz gegen Abhörversuche.

Mit der zunehmenden Vernetzung von dezentralen Datenverarbeitungsanlagen vergrössert sich auch die Gefahr des Informationsdiebstahls in erheblichem Masse. Das drahtlose Telefon führte uns die Schwäche der heute verwendeten Kommunikationssysteme in Bezug auf ihre Abhörsicherheit eindrücklich vor Augen [1]. So verlangt die Regierung der USA, dass ihre Dienststellen und militärischen Vertragspartner sämtliche Sprach- und Datenübertragungen chiffrieren [2]. Aber auch in vielen Bereichen der Privatwirtschaft ist die Chiffrierung der über das öffentliche Netz zu übertragenden Gespräche und Daten unabdingbar.

Vor diesem Hintergrund ist es nicht erstaunlich, dass die Nachfrage nach optischen Uebertragungssystemen nicht zuletzt auch aufgrund von Sicherheitsüberlegungen laufend zunimmt. Es drängen sich in diesem Zusammenhang für die Benutzer und Betreiber von Datenübertragungseinrichtungen die folgenden Fragen auf:

- Wie sicher sind faseroptische Datenübertragungssysteme wirklich?
- Welche Abhörmöglichkeiten bestehen, und wie gross ist der entsprechende Aufwand für den Abhörer?
- Welche Schutzmassnahmen kann der Betreiber einer optischen Uebertragungseinrichtung ergreifen?

2. GRUNDLAGEN FASEROPTISCHER UEBERTRAGUNGSSYSTEME

Im Unterschied zu den konventionellen leitungsgebundenen Datenübertragungssystemen erfolgt in faseroptischen Systemen eine zusätzliche Umwandlung des elektrischen Nachrichtensignals in ein entsprechendes optisches Signal (Figur 1).

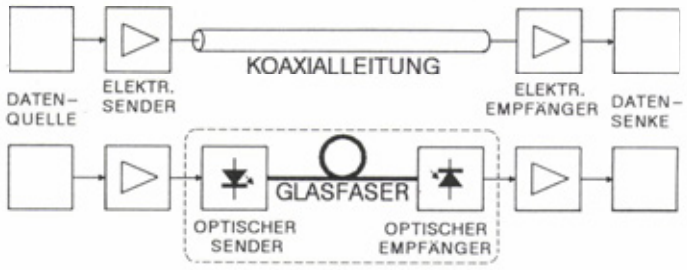

Fig. 1 Konventionelles und faseroptisches Datenübertragungssystem

Letzteres lässt sich über eine Glasfaser mit sehr geringen Verlusten nahezu verzerrungs- und störungsfrei übertragen. Am Ende der Glasfaserstrecke wandelt der optische Empfänger das einfallende Licht wieder in ein entsprechendes elektrisches Signal um. Bei den heute gebräuchlichen optischen Uebertragungssystemen mit Intensitätsmodulation werden die Nachrichten in Form von Aenderungen der optischen Leistung übertragen. Im Falle der binären Datenübertragung entspricht dies einem Ein- und Ausschalten des Lichtsignals.

2.1. DIE GLASFASER

Die Glasfaser ist für die betrachteten optischen Signale ein dielektrischer Wellenleiter. Sie besitzt die geometrische Form von mehreren konzentrisch angeordneten Zylindern. Der Faserkern (Durchmesser: 5-200 µm) mit einer hohen Brechzahl n_1 ist vom Fasermantel (Durchmesser: 125-500 µm) mit einer geringeren Brechzahl n_2 umgeben (Figur 2).

Zum Schutz vor äusseren Einflüssen (mechanische und chemische Beanspruchung) werden zusätzliche Ueberzüge und Schutzschichten ("coating, jacket") aus unterschiedlichen Materialien verwendet. Beim "primary coating" handelt es sich um einen direkt auf den Fasermantel aufgebrachten elastischen Ueberzug (Figur 2). Der "buffer jacket" (Durchmesser: 0.25-1 mm) wird üblicherweise aus Hartplastik gefertigt und dient dem mechanischen Schutz der Glasfaser. Er soll eine zu starke Biegung ("microbending") der Faser verhindern. Geschützt durch eine weitere Polsterung aus Kunststoffgarn ist die Faser vom Kabelmantel (Durchmesser ≈ 2.5 mm) aus einem widerstandsfähigen Kunststoff wie PUR (Polyurethan), PVC (Polyvinylchlorid) oder PE (Polyäthylen) umgeben (Figur 3).

Neben den Einfaserkabeln sind auch Mehrfaserkabel weit verbreitet. Je nach Verwendungszweck und Beanspruchung werden diese durch zusätzliche Stütz- und Zugelemente verstärkt. Es können auch Kupferleitungen für die Stromversorgung von Zwischenverstärkern und Endgeräten in den Kabeln integriert sein.

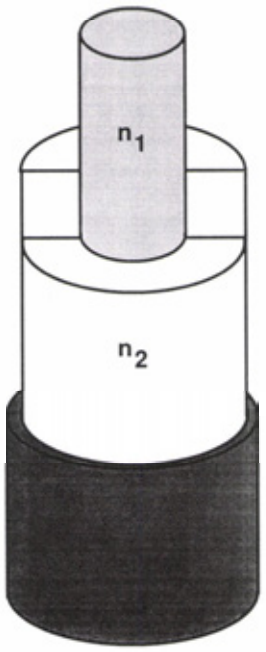

Fig. 2 Glasfaser: Faserkern n_1, Fasermantel n_2, "primary coating"

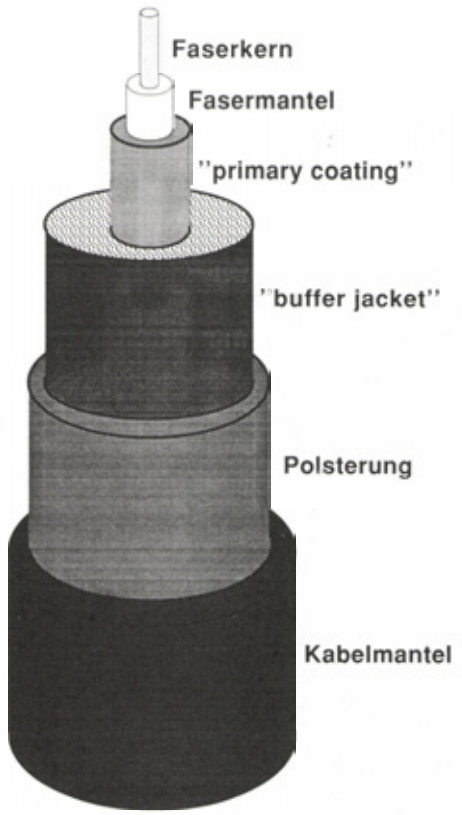

Fig. 3 Glasfaserkabel

Aufgrund der Brechzahldifferenz zwischen Kern und Mantel vermag die Glasfaser optische Signale zu führen. Abhängig von der Wellenlänge, der Brechzahldifferenz und den geometrischen Abmessungen weist eine Glasfaser für Licht mit einer bestimmten Wellenlänge verschiedene Ausbreitungspfade (Moden) auf (Figur 4).

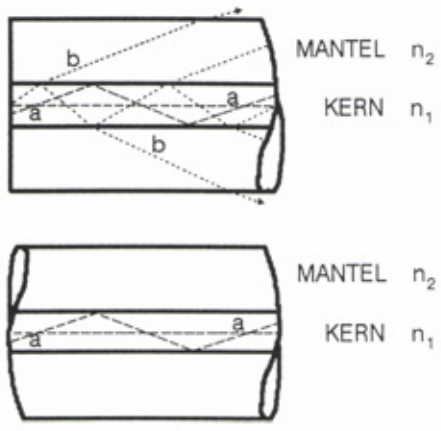

Fig. 4 Moden in einer Glasfaser, unmittelbar nach der Einkopplung (oben), wenige Meter nach der Einkopplung (unten)

Man unterscheidet zwischen den geführten Moden a und den nichtgeführten Moden b. Im Fall der geführten Moden ist an der Grenzfläche zwischen Kern und Mantel die Bedingung für Totalreflexion erfüllt. Es wird die gesamte Leistung des auf die Grenzfläche auftreffenden optischen Strahls in den Kern zurückreflektiert. Bei den nichtgeführten Moden verlässt bei jedem Auftreffen des Strahls auf die Grenzfläche ein Teil der Leistung den Kern. Da die in die nichtgeführten Moden eingekoppelte Leistung bereits nach wenigen Metern nahezu vollständig abgestrahlt ist, tragen diese Moden nicht zur Signalübertragung bei.

Die Mehrmodenfaser (MMF, "multimode fiber") mit Kerndurchmessern im Bereich von 50 bis 200 µm weisen eine grosse Anzahl geführter Moden auf. In der Einmodenfaser (SMF, "singlemode fiber") mit einem Kerndurchmesser von 5-10 µm wird nur ein einziger Mode von der Faser geführt.

Die Verluste, welche die optischen Signale in den geführten Moden der Glasfaser erfahren, sind sehr gering. Absorption und Streuung verursachen die sogenannte Faserdämpfung. Die heutigen Fabrikationsmethoden erlauben die Herstellung von Glasfasern, welche im Bereich der beiden opti-

schen Fenster (1300 und 1550 nm) das theoretische, durch die Rayleigh-Streuung bestimmte Dämpfungsminimum nahezu erreichen. In diesem Wellenlängenbereich ist die Absorption im Fasermaterial im Vergleich zur Streuung vernachlässigbar gering. Typische Werte für die Dämpfung von Einmodenfasern sind 0.4 dB/km bei 1300 nm beziehungsweise 0.2 dB/km bei 1550 nm Lichtwellenlänge.

2.2. STECKER, SPLEISS UND KOPPLER

Durch optische Stecker und Spleissungen lassen sich einzelne Faserstücke zu grösseren Uebertragungsstrecken verbinden. Diese Elemente verursachen zusätzliche Verluste und können einen Teil der Verlustleistung abstrahlen.

Eine weitere passive optische Komponente, welche vorwiegend in faseroptischen Netzwerken, Wellenlängenmultiplex- und bidirektionalen Uebertragungssystemen Verwendung findet, ist der optische Koppler. Mit einem optischen Koppler ist es möglich, das in einer Faser geführte Licht auf mehrere Fasern aufzuteilen oder aber die optischen Signale von mehreren Fasern in einer Faser zu vereinen. Man unterscheidet zwischen wellenlängenselektiven Kopplern (WDM-Koppler) und den wellenlängenunabhängigen Richtkopplern.

2.3. OPTISCHE QUELLEN

Als optische Quellen finden heute überwiegend lichtemittierende Dioden (LED) und Laserdioden (LD) Verwendung. Diese Halbleiterelemente erzeugen Licht im nahen Infrarot (800-1600 nm). Durch eine spezielle Anordnung der optischen Quelle, des Faserendes sowie zusätzlicher optischer Komponenten (Linsen usw.) wird sichergestellt, dass ein möglichst grosser Teil der von der Quelle abgestrahlten Leistung in die geführten Moden der Faser eingekoppelt wird. Die einkoppelbare Leistung hängt von der Quelle und vom Fasertyp ab.

2.4. OPTISCHE EMPFAENGER

In optischen Empfängern finden als Detektoren in erster Linie Photodioden Verwendung. Sie erzeugen einen der Leistung des einfallenden optischen Signals proportionalen elektrischen Strom, welcher in den nachfolgenden elektronischen Schaltungen verstärkt, aufbereitet und demoduliert wird.

Verschiedene Rauschprozesse wie z.B. das Dunkelstrom- und Schrotrauschen in der Photodiode sowie das thermische Rauschen des Verstärkers beeinträchtigen den Empfang der optischen Datensignale. Da die empfangenen Signale gestört sind, müssen diese für eine zuverlässige Detektion eine minimale Energie aufweisen. Optische Empfänger werden durch ihre Empfindlichkeit charakterisiert. Es handelt sich dabei um die für eine bestimmte Uebertragungsgeschwindigkeit im Empfänger benötigte mittlere Leistung des optischen Signals, um die übertragenen Daten mit der geforderten Fehlerwahrscheinlichkeit P_b von beispielsweise 10^{-9} detektieren zu können. Weil das Schrotrauschen durch technische Massnahmen (Kühlung usw.) nicht verringert werden kann, bestimmt es die physikalische untere Grenze für die Empfängerempfindlichkeit, wobei die Leistungsfähigkeit der heute gebräuchlichen optischen Empfänger durch das thermische Verstärkerrauschen begrenzt ist.

Es gilt zu beachten, dass die Preise für optische Empfänger mit zunehmender Empfindlichkeit sehr stark ansteigen und dass für zahlreiche Anwendungen mit moderaten Uebertragungsgeschwindigkeiten und Uebertragungsdistanzen auch mit kostengünstigen, wenig empfindlichen Empfängern die gestellten Anforderungen erfüllt werden können. In vielen Fällen steht ausreichend optische Sendeleistung zur Verfügung, oder es erweist sich als wirtschaftlicher, eine Verbesserung der Empfängerempfindlichkeit durch eine Erhöhung der Sendeleistung zu umgehen.

3. INHAERENTE ABHOERSICHERHEIT OPTISCHER NACHRICHTENSYSTEME

Die Glasfaser ist nicht abhörsicher, aber sie besitzt zahlreiche Eigenschaften, die sie zu einem attraktiven Uebertragungsmedium für schützenswerte Information machen.

- Die Glasfaser ist ein dielektrischer Wellenleiter für extrem hochfrequente elektromagnetische Felder (Licht). Im Unterschied zu konventionellen Kupferkabeln werden im Glasfaserkabel bei der Signalübertragung keine Ladungen verschoben. Es entstehen in der Umgebung des Glasfaserkabels keine elektromagnetischen Felder mit Frequenzen im Radiofrequenzbereich, die mit einer entsprechenden Antenne detektiert werden könnten.

- Im Glasfaserkabel ist die Leistung der sich ausbreitenden optischen Signale grösstenteils im Faserkern und zu einem sehr geringen Teil in kernnahen Bereichen des Fasermantels konzentriert (Figur 4 (unten)). Das von einer gebräuchlichen Glasfaser abgestrahlte Licht weist eine zu geringe Leistung auf, um es mit realisierbaren optischen Empfängern detektieren zu können. Es ist also ohne direkten Zugriff nicht möglich, eine Glasfaser abzuhören. Unmittelbar nach der Einkopplung kann die in den nichtgeführten Moden noch vorhandene Leistung dazu führen, dass die Faser stärker strahlt (Figur 4 (oben)).

- Die Dynamik (Differenz zwischen maximaler Sende- und minimal erforderlicher Empfangsleistung) der Signale ist in Glasfasersystemen im allgemeinen geringer als in elektrischen Uebertragungssystemen. Da die Signalverluste durch Absorption und Streuung in der Glasfaser sehr gering sind, ist dennoch eine Uebertragung über sehr grosse Distanzen möglich. Schwieriger gestaltet sich aufgrund der beschränkten Dynamik die Verteilung der Signale in einem rein optischen Netzwerk. Bedingt durch die kleinere Signaldynamik ist auch die theoretisch maximale Abhörleistung geringer.

- Die sehr grosse Uebertragungskapazität der Glasfaser würde grundsätzlich den Einsatz spezieller Datenformate und kryptografischer Methoden zum zusätzlichen Schutz der Daten erlauben. Es gilt allerdings zu beachten, dass für die heute in Glasfasersystemen üblichen Datenraten (> 100 Mbit/s) zur Zeit noch keine Chiffriergeräte zur Verfügung stehen.

- Wegen den im allgemeinen sehr grossen Uebertragungsgeschwindigkeiten in optischen Systemen und der zeitlichen Verschachtelung vieler Datenkanäle (Zeitmultiplex) sieht sich der Gegner auch dann, wenn der Abhörversuch erfolgreich verlaufen ist, vor das Problem gestellt, aus dem anfallenden Datenstrom die gewünschte Information extrahieren zu müssen. Zu diesem Zweck benötigt er eine sehr aufwendige elektronische Ausrüstung. Ausserdem wird das Abhören auch dadurch erschwert, dass bis heute im Bereich der optischen Uebertragungstechnik Normen für die Uebertragungsgeschwindigkeiten und Uebertragungsformate weitgehend fehlen.

- Das Abhören einer Glasfaser verursacht immer einen zusätzlichen lokalen Verlust an optischer Uebertragungsleistung. Die Beobachtung der empfangenen Leistung oder des Dämpfungsprofils der Glasfaser ermöglichen eine Ueberwachung der Uebertragungsstrecke. Mit denselben Einrichtungen, welche bei der Installation und Ueberprüfung von Faserstrecken Verwendung finden, lassen sich auch Abhörversuche aufklären.

- Da die Glasfasern aus dielektrischen Materialen bestehen und nur sehr geringe Ausmasse aufweisen, sind sie örtlich nur schwer lokalisierbar. Metalldetektoren eignen sich nicht, um Fasern aufzufinden.

- Die kleinen Abmessungen, die Flexibilität und das geringe Gewicht der Glasfaser ermöglichen eine einfache Integration in die meisten konventionellen Schutzmassnahmen, welche einen unerlaubten Zugriff verhindern sollen.

Abgesehen von diesen erheblichen Vorteilen sind auch die folgenden Schwachpunkte optischer Übertragungssysteme zu erwähnen:

- Von optischen Steckern und Spleissen kann ein grosser Teil der verursachten Verlustleistung abgestrahlt werden. Ueberschreitet die Leistung dieser Abstrahlung einen bestimmten Betrag, lässt sie sich mit Hilfe eines optischen Empfängers ohne Eingriff an der Glasfaserstrecke detektieren. Es ist deshalb darauf zu achten, dass Stecker und Spleisse nur geringe Verluste aufweisen. Eine Ueberprüfung der Glasfaserstrecke im Hinblick auf vorhandene Leckstellen sollte bereits bei der Installation erfolgen.

- Abhängig von der Dimensionierung des Uebertragungssystems und von der örtlichen Lage der Anzapfstelle entlang der Glasfaserstrecke muss der Abhörer nur einen sehr geringen Teil der totalen optischen Leistung abzweigen, um eine unchiffrierte Meldung zu empfangen. Geht man von den Annahmen aus, dass der Abhörer eine grössere Fehlerwahrscheinlichkeit (z.B. $P_e = 10^{-3}$) toleriert als der Betreiber ($P_e = 10^{-9}$) und dass wirtschaftliche Uebertragungssysteme mit kostengünstigen, weniger empfindlichen Empfängern arbeiten, kann der Abhörer bei einem 2 Mbit/s-System mit Hilfe eines teuren, hochempfindlichen Empfängers sein Ziel durch Auskoppeln von nur 0.001 % der optischen Leistung erreichen [3].

- Systeme mit überdimensionierter Sendeleistung lassen sich schlecht überwachen und weisen eine grosse potentielle Abhörleistung auf. Abhörsichere Systeme sollten mit möglichst geringen Leistungsreserven arbeiten. Die Verwendung von teuren, hochempfindlichen Empfängern und die gleichzeitige Reduktion der Sendeleistung ermöglichen eine Verbesserung des Abhörschutzes.

- Die elektrischen Komponenten der Uebertragungsstrecke wie Sender, Empfänger sowie allfällige Zwischenverstärker strahlen elektromagnetische Felder mit Frequenzen im Radiofrequenzbereich ab. Diese Felder lassen sich mit einer Antenne detektieren. Wird die Abstrahlung nicht durch spezielle Massnahmen reduziert, kann dies auch aus erheblicher Entfernung erfolgen.

4. ABHOERMOEGLICHKEITEN

Da die optischen Signale bei der Uebertragung über die Glasfaser nur sehr geringe Verluste erfahren, ist auch die dabei abgestrahlte Lichtleistung sehr gering. Es ist mit einem realisierbaren optischen Detektor unmöglich, genügend abgestrahlte Lichtleistung aufzufangen, um die Verbindung ohne direkten Zugriff auf die Glasfaser abhören zu können.

Ist aber ein physikalischer Zugriff auf das Glasfaserkabel möglich, lässt sich mit verschiedenen Methoden ein Teil der optischen Signalleistung auskoppeln und detektieren. Zu diesem Zweck müssen zuerst die verschiedenen Schutzüberzüge der Glasfaser mechanisch oder chemisch entfernt werden. Ist das Schutzmaterial für optische Signale im nahen Infrarot transparent, kann dieser Schritt teilweise entfallen.

Um Licht aus der nackten Glasfaser auszukoppeln, müssen deren Wellenleitereigenschaften verändert werden. Dies lässt sich beispielsweise durch Biegung der Glasfaser erreichen. Es sind heute verschiedene Techniken bekannt, um durch Biegung zerstörungsfrei einen Teil der optischen Leistung aus einem Glasfaserkabel auskoppeln und detektieren zu können (Figur 5). Diese Techniken finden auch in optischen Verteilnetzwerken, Spleissgeräten und Kabeltestausrüstungen praktische Verwendung.

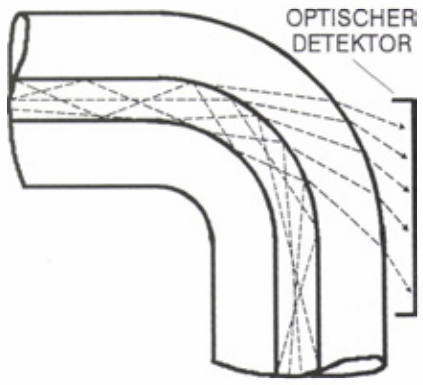

Fig. 5 Abhören einer Glasfaser durch Biegung

Wird eine Beschädigung der Glasfaser in Kauf genommen, kann ein Teil des Fasermantels entfernt und durch ein Material ersetzt werden, dessen Brechzahl grösser als derjenige des Faserkerns ist. Dies bewirkt ebenfalls, dass ein Teil des optischen Signals die Faser verlässt [4].

Es besteht auch die Möglichkeit, die Faserstrecke kurzzeitig zu unterbrechen und einen passiven optischen Koppler in die Strecke einzufügen. Der Koppler teilt das optische Signal auf, der eine Teil wird einem optischen Empfänger zugeführt und detektiert, der zweite Anteil gelangt in die angezapfte Glasfaser zurück (Figur 6).

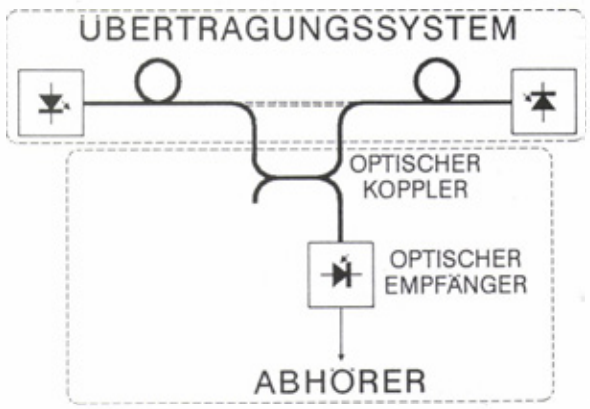

Fig. 6 Abhören einer Glasfaser mit einem optischen Koppler

Alle beschriebenen passiven Abhörtechniken verursachen eine zusätzliche Abnahme der optischen Leistung am Empfängereingang. Koppelt ein Abhörer an einem bestimmten Ort entlang der Faser einen Anteil a ≦ 1 der dort vorhandenen mittleren optischen Leistung P_t aus, so nimmt die Leistung am optischen Empfänger um den Faktor (1 - a) ab (Figur 7).

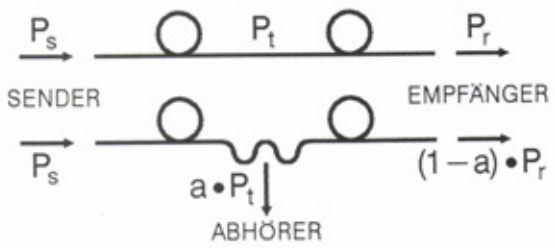

Fig. 7 Durch den Abhörer verursachte Leistungsabnahme

Soll ein faseroptisches Uebertragungssystem möglichst abhörsicher dimensioniert werden, ist darauf zu achten, dass die eingekoppelte Leistung nicht grösser gewählt wird, als dies für eine zuverlässige Uebertragung unbedingt notwendig ist. Wird die mittlere Senderleistung P_s verkleinert, nimmt auch die Leistung an der Anzapfstelle P_t proportional dazu ab, und der Abhörer ist gezwungen, einen grösseren Signalanteil auszukoppeln, um die Daten fehlerfrei detektieren zu können. Zapft aber der Abhörer mehr Leistung ab, steigt die Wahrscheinlichkeit einer Aufklärung des Abhörversuchs.

An Stelle eines passiven Kopplers wäre es auch denkbar, einen aktiven Zwischenverstärker in die Uebertragungstrecke einzufügen und die durch das Abhören verursachte Lichtleistungsabnahme auszugleichen (Figur 8).

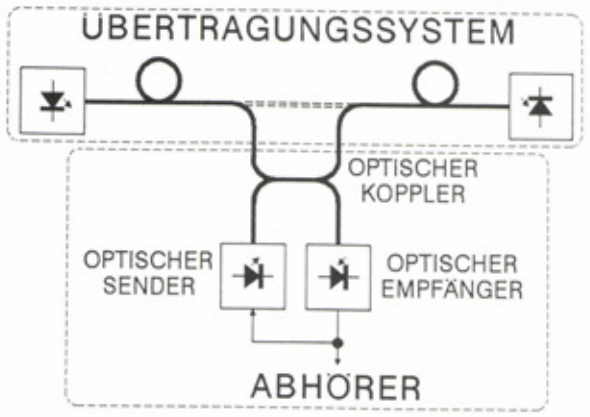

Fig. 8 Abhören einer Glasfaser mit einem aktiven Zwischenverstärker

5. SCHUTZMASSNAHMEN

Man kann die Verfahren zum Schutz vertraulicher Information während der Uebertragung über Glasfasern in zwei Gruppen unterteilen.

Mit den Schutzmassnahmen der ersten Gruppe versucht man zu verhindern, dass es einem Gegner überhaupt gelingt, eine Glasfaserstrecke abzuhören. Entweder wird ein Zugriff durch herkömmliche Sicherheitsmassnahmen ausgeschlossen, oder es wird sichergestellt, dass jeder Abhörversuch sofort zu einer Unterbrechung der Uebertragung vertraulicher Information führt. Das aufkommende Bewusstsein, dass auch eine Glasfaser nicht abhörsicher ist, hat vor allem in den USA zu einem starken Interesse an den mit der Abkürzung IDOCS ("Intrusion Detection Optical Communications Systems") bezeichneten Systemen mit integrierter Streckenüberwachung geführt [5].

Es existieren verschiedene Methoden, um bei Glasfaserverbindungen Abhörversuche aufzuklären.

Glasfasern werden mit dünnen leitenden Schichten überzogen, welche dazu dienen, jede Beschädigung des Schutzüberzugs und damit jeden Abhörversuch zu detektieren. Ein äquivalenter Schutz liesse sich auch durch das Verlegen der Glasfaserkabel in einem Rohr aus leitendem Material erzielen.

Den geringsten zusätzlichen Aufwand erfordert eine Ueberwachung der im Empfänger einfallenden Lichtleistung. Wie bereits erwähnt, bewirkt jeder Abhörversuch eine Abnahme der Empfangsleistung oder mindestens eine kurzzeitige Unterbrechung der Glasfaserstrecke. Sicherheitssysteme mit Empfangsleistungsüberwachung weisen zwei wesentliche Nachteile auf. Da die Empfangsleistung zusätzlich noch stark von äusseren Einflüssen (Temperatur usw.) abhängen kann, stellt sich das Problem, einen Abhörversuch von anderen Umwelteinflüssen unterscheiden zu müssen. Ausserdem müssen diese Systeme über eine sichere Verbindung vom Empfänger zum Sender verfügen, um im Fall eines aufgeklärten Abhörversuchs die Informationsübertragung sofort unterbrechen zu können.

Bei "Hughes Aircraft" wird anstelle der gesamten empfangenen optischen Leistung die durch ein Abhören verursachte Veränderung der Leistungsaufteilung auf die verschiedenen Modengruppen einer Mehrmodenfaser detektiert [4].

Der von "Photon Resources" entwickelte "Optical Line Intrusion Detector" OLID verwendet zur Ueberwachung ein sich in der entgegengesetzten Richtung ausbreitendes Kontrollsignal. Mit diesem System ist es möglich, einen Leistungsabfall von mehr als 7 % festzustellen [4].

Auch die für Kontroll- und Unterhaltsarbeiten an Glasfaserstrecken weitverbreitete Technik der Rückflussdämpfungsmessung lässt sich für die Ueberwachung einer Glasfaserverbindung einsetzen. Hierbei wird im Sender aus den vom Fasermaterial in Rückwärtsrichtung gestreuten und an Stosstellen (Stecker, Spleisse) reflektierten Lichtanteilen P_r ein Dämpfungsprofil der Glasfaserstrecke bestimmt. Zweigt ein Abhörer Leistung ab, zeigt sich dies im Dämpfungsprofil als zusätzlicher lokaler Leistungsabfall P_a (Figur 9). Mit modernen Messgeräten lassen sich Leistungsänderungen von ungefähr 5 % zuverlässig detektieren [6]. Obwohl für die Rückflussdämpfungsmessung eine aufwendige Messeinrichtung benötigt wird, weist diese Technik gegenüber einer reinen Leistungsüberwachung erhebliche Vorteile auf. Da die Information über den Zustand der Glasfaserstrecke im Sender zur Verfügung steht, ist bei dieser Methode kein sicherer Uebertragungskanal vom Empfänger zum Sender erforderlich, um die Informationsübertragung zu unterbrechen. Mit der Rückflussdämpfungsmessung lässt sich wie mit dem OLID-System auch ein Abhörversuch aufklären, bei welchem die abgezweigte Leistung mit Hilfe einer aktiven optischen Schaltung wieder ersetzt wird. Sicherheitssysteme mit Rückflussdämpfungsmessung ermöglichen zusätzlich die Lokalisierung des Abhörers.

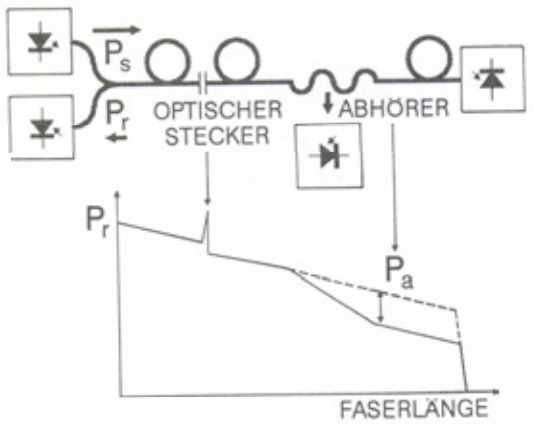

Fig. 9 Rückflussdämpfungsmessung

In [3] wurde gezeigt, dass unter gewissen Umständen nur ein sehr geringer Teil der optischen Leistung (0.001 %) abgezapft werden muss. Eine derart geringe Leistungsentnahme liesse sich weder durch eine Rückflussdämpfungsmessung noch durch eine Empfangsleistungsüberwachung aufklären. Das von Ericsson entwickelte Sicherheitssystem ZAT 4 arbeitet deswegen mit einem sehr geringen Modulationsindex (1 %) [7]. Die Empfindlichkeit des Empfängers wird in diesem Fall durch das Schrotrauschen des Detektorstroms bestimmt. Da es sich hierbei um eine physikalische Grenze handelt, ist es dem Abhörer nicht möglich, durch zusätzlichen Aufwand einen empfindlicheren Empfänger zu realisieren. Um eine Fehlerwahrscheinlichkeit von 10^{-9} zu erreichen, müssen 25 % der optischen Leistung abgezapft werden. Zusätzlich ist das ZAT 4 mit einer Alarmeinrichtung ausgerüstet. Diese spricht an, wenn eine plötzliche Aenderung der übertragenen optischen Leistung auftritt, wenn die Empfangsleistung einen Grenzwert unterschreitet oder wenn die Fehlerrate ansteigt. Damit ist sichergestellt, dass entweder die abgezapfte Leistung für ein erfolgreiches Abhören nicht ausreicht oder aber der Abhörversuch mit sehr grosser Wahrscheinlichkeit aufgeklärt werden kann.

Bei den Sicherheitssystemen, welche der zweiten Gruppe angehören, wird durch Chiffrierung sichergestellt, dass der Gegner aus dem abgehörten Datenstrom keine für ihn nützliche Informationen gewinnen kann. Abgesehen von den bekannten Chiffrierverfahren (Kryptographie) finden hierbei auch spezielle, auf die Eigenschaften der faseroptischen Uebertragungseinrichtungen abgestimmte Techniken Verwendung.

In [6] wird ein abhörsicheres Singlemode-Uebertragungssystem mit einer von A. Wyner vorgeschlagenen Codierung untersucht. Anstelle eines "0"- oder "1"-Symbols pro Informationsbit sendet man eine Sequenz von n zufälligen Symbolen mit gerader oder ungerader Parität zur Uebertragung eines Informationsbits mit dem Wert "0" beziehungsweise "1". Durch geeignete Wahl von n kann eine Decodierung der Nachricht durch den Abhörer selbst für relativ geringe Symbolfehlerwahrscheinlichkeiten (10^{-3}) verunmöglicht werden. Dies entspricht einer Situation, in welcher der Abhörer nur über eine um wenig geringere optische Leistung als der rechtmässige Empfänger verfügt. Durch eine zusätzliche Ueberwachung der Glasfaserstrecke mittels Rückflussdämpfungsmessung lässt sich verhindern, dass der Abhörer die für eine erfolgreiche Decodierung notwendige Leistung abzapft.

Den besten Schutz bietet die Uebertragung von chiffrierten Daten über ein Glasfasersystem mit einer Abhördetektionseinrichtung und ausreichend abgeschirmten elektronischen Endgeräten. Fachleute vertreten die Meinung, dass es dem Abhörer bei modernen Systemen mit Abhördetektionseinrichtungen nicht gelingt, auch nur einen Drittel des für eine erfolgreiche Attacke benötigten Chiffrats zu erhalten, bevor ein Alarm ausgelöst und die Uebertragung unterbrochen wird [5].

6. SCHLUSSFOLGERUNGEN

Optische Datenübertragungssysteme können abgehört werden. Der wahre Wert der Glasfaser als sicheres Uebertragungsmedium besteht nicht darin, dass ein Abhören unmöglich ist, sondern dass dies einen direkten Zugriff auf die Faser erfordert.

Ein erstes zu lösendes Problem für den Abhörer besteht darin, das Glasfaserkabel genau zu lokalisieren und sich einen Zugang zum Kabel zu verschaffen.

Um ein Glasfaserkabel abzuhören, benötigt der Gegner spezielle Kenntnisse und eine sehr aufwendige Ausrüstung. Ausserdem ist auch der erforderliche Zeitaufwand nicht zu unterschätzen.

Die in optischen Systemen üblichen, sehr hohen Uebertragungsgeschwindigkeiten und die fehlende Normierung der Uebertragungsformate erschweren das Abhören wesentlich. Das angezapfte Lichtsignal überträgt, abgesehen von den Zieldaten im Zeitmultiplexverfahren, gleichzeitig noch mehrere andere Nachrichtensignale. Der Abhörer muss also über ein Gerät verfügen, welches es ihm erlaubt, eine sehr grosse Datenmenge aufzunehmen und daraus die gewünschte Information zu extrahieren. Es handelt sich dabei nicht um eine Eigenschaft der optischen Uebertragung an sich, sondern um eine durch die für optische Systeme üblichen grossen Uebertragungsgeschwindigkeiten verursachte Erschwernis für den Abhörer.

Da es möglich ist, Abhörversuche auf Glasfaserverbindungen aufzuklären, strebt der Abhörer an, möglichst wenig Leistung auszukoppeln, um die Aufklärungswahrscheinlichkeit zu verringern. Anderseits ist aber eine möglichst grosse Leistung des abgezapften optischen Signals für eine zuverlässige Detektion erforderlich. Der Abhörer kann seine Chancen verbessern, indem er versucht, möglichst in der Nähe des optischen Senders auf die Glasfaser zuzugreifen. Die Betreiber von Uebertragungsstrecken mit Reichweiten im Bereich von einigen Kilometern besitzen die Möglichkeit, durch Reduktion der Sendeleistung den für einen erfolgreichen Abhörversuch erforderlichen prozentualen Anteil der Leistung des Lichtsignals zu erhöhen und damit die Aufklärungswahrscheinlichkeit zu verbessern.

Das Abhören eines faseroptischen Uebertragungssystems ist auf jeden Fall viel aufwendiger und kostspieliger als das Abhören einer konventionellen metallischen Uebertragungsleitung.

Die Glasfaser ist kein abhörsicheres Uebertragungsmedium. Es gilt aber zu beachten, dass es vermutlich in den meisten Fällen eine kostengünstigere Lösung geben wird, um sich die gewünschte Information zu beschaffen, als diejenige, eine Glasfaserübertragungsstrecke abzuhören.

In Bezug auf die Abhörsicherheit sind in erster Linie die elektronischen Schaltungen in Sendern, Empfängern und Zwischenverstärkern als die Schwachpunkte einer optischen Uebertragungseinrichtung zu betrachten.

Diese Schaltungen emittieren elektromagnetische Strahlungen, welche mit Hilfe einer Antenne auch aus einiger Entfernung detektiert werden können.

Die zukünftige Einführung von Wellenlängenmultiplex- und kohärenten Uebertragungssystemen wird zu einer zusätzlichen Erschwernis für einen potentiellen Abhörer führen.

REFERENZEN

[1] Update, "Secure comms: into the commercial cauldron", Communications Engineering International, April 1988.

[2] J. Parker, "Protecting the Message", Lightwave - The Journal of Fiber Optics, Juni 1988.

[3] R.S. Erkander, G.S. Forsberg, "Tapping Information from Fibre Optic Systems - A Comparison Between a Security System and a Conventional Fibre Optic System", Proceedings from International Carnahan Conference on Security Technology, Gothenburg, Sweden, August 1986.

[4] P. Susca, N.H. Rindge, "Fiber becomes tappable, but eavesdroppers can be detected", Lightwave - The Journal of Fiber Optics, Juni 1987.

[5] J. Kreidl, "Use of fiber for security", Lightwave - The Journal of Fiber Optics, Juni 1988.

[6] P.L. Heinzmann, "Fiber optics and secure communications", IBM Research Report, RZ 1759, 1988.

[7] R.S. Erkander, "Optical Fibre Security System ZAT 4", Ericsson Review, No. 1, 1987.