3 Effiziente Realisierung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten

Um in Abschnitt 2.5 die Beschreibung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten nicht mit zum ersten Verständnis unnötigen Details zu überfrachten, werden in diesem Kapitel ihre effizienten Realisierungsmöglichkeiten separat beschrieben. Um strukturelle Zusammenhänge der Grundverfahren zu verdeutlichen, ist die Gliederung dieses Kapitels nicht primär an den Grundverfahren orientiert, sondern an deren Schichtung gemäß Abschnitt 2.6, wobei von den höheren zu den tieferen Schichten vorgegangen wird.

Zuerst wird also in Abschnitt 3.1 die effiziente Realisierung der Schichten beschrieben, die die Anoymität erhalten müssen. Aus der Vielzahl möglicher Aufgaben werden implizite Adressierung und Mehrfachzugriff herausgegriffen und vertieft behandelt, da sie in den jeweiligen Kommunikationsnetzen zum Betrieb nötig sind.

In Abschnitt 3.2 wird dann die effiziente Realisierung der (Teil)Schichten beschrieben, die (innerhalb des Kommunikationsnetzes) Anonymität (und Unverkettbarkeit) schaffen. Wie am Ende von Abschnitt 2.6 schon erwähnt, muß in beiden Schichtgruppen darauf geachtet werden, daß die Realisierung keine zusätzlichen, Abläufe unterscheidenden Charakteristika einführt. Sei dies – wie in den Beispielen von Abschnitt 2.6 – mittels Charakteristika beabsichtigter Ausgaben, sei es mittels unbeabsichtigter Ausgaben, beispielsweise akustische, mechanische oder elektromagnetische Abstrahlung. Es sei auch noch einmal auf den in Abschnitt 2.6 beschriebenen aktiven Verkettungsangriff über Betriebsmittelknappheit hingewiesen und daran erinnert, daß die Dimensionierung und Aufteilung der Betriebsmittel für seine Erschwerung oder gar Verhinderung wesentlich ist.

Schließlich werden dann in Abschnitt 3.3 die Schichten behandelt, deren Realisierung ohne Rücksicht auf Anonymität oder Unverkettbarkeit erfolgen kann.

Wer sich nur für die Realisierung bestimmter Grundverfahren interessiert, kann anhand der nächstfeineren Gliederungsstufe natürlich auch nur diese selektiv lesen, da die Unterabschnitte zweiter Stufe dieses Kapitels gewissermaßen eine Matrix bilden.

Genauso wie der Inhalt dieses Kapitels aus Abschnitt 2.5 weitgehend herausgehalten wurde, so werden aus diesem Kapitel drei Aspekte herausgehalten:

- Nur ein sehr effizienter Einsatz der Grundverfahren ermöglicht genügend leistungsfähige Kommunikationsnetze. Deshalb wird in Kapitel 4 behandelt, wie die Grundverfahren durch Einführung verschieden geschützter Verkehrsklassen und/oder hierarchische Gliederung des Kommunikationsnetzes und dadurch induzierte Klasseneinteilung der Teilnehmer bezüglich Anonymität (vgl. Abschnitt 2.1.1) genügend effizient eingesetzt werden können.

- Fehlertoleranz-Maßnahmen zur Erreichung einer genügend hohen Verfügbarkeit des Kommunikationsnetzes trotz der Forderung nach Datenschutz, d. h. die Interaktionen zwischen Fehlertoleranz und Datenschutz, insbesondere Anonymität, werden in Kapitel 5 behandelt. Fehlertoleranz-Maßnahmen per se, d. h. ohne Betrachtung der Interaktionen mit den in den Abschnitten 2.3 und 2.5 beschriebenen speziellen Verfahren werden seit langem erforscht und partiell eingesetzt und sind somit (zumindest theoretisch) Standard. Sie werden deshalb an den jeweiligen Stellen nur kurz erwähnt.
- In Kapitel 6 wird der etappenweise Ausbau der heutigen Kommunikationsnetze zu einem preiswerten und zuverlässigen, zunächst schmalbandigen, später breitbandigen Kommunikationsnetz mit überprüfbarem Datenschutz beschrieben.

3.1 Anonymität erhaltende Schichten: effiziente implizite Adressierung und effizienter Mehrfachzugriff

In diesem Abschnitt wird zu den Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten die effiziente Realisierung der Schichten beschrieben, die die Anonymität erhalten müssen.

Zunächst werden einige allgemeine grundsätzliche Bemerkungen gemacht.

Danach wird, um eine vertiefte Behandlung zu ermöglichen, aus der Vielzahl möglicher Aufgaben dieser Schichten implizite Adressierung und Mehrfachzugriff herausgegriffen, da sie viele Stationen koordinieren und insoweit von der Forderung nach Erhalt der Anonymität besonders betroffen sind. Der Reihe nach werden Verteilung, das bezüglich Mehrfachzugriff sehr interessante DC- sowie das ihm bezüglich Mehrfachzugriff ähnliche, aber einfachere BAUM-Netz und danach sehr ausführlich das bezüglich Mehrfachzugriff wiederum interessante (und schwierigere) RING-Netz in jeweils eigenen Unterabschnitten behandelt.

Viele Protokolle höherer Schichten verwenden heutzutage feste (Netz)Adressen, die, wenn sie wie die heutigen Telefonnummern einen physischen Ort im Kommunikationsnetz beschreiben, die Anonymität untergraben und selbst wenn dies nicht der Fall ist, auf jeden Fall die Unverkettbarkeit. Auch das von den (internationalen) Normungsgremien vorbereitete Ersetzen der festen (Netz)Adressen durch Namen, denen über einen Adreßbuchdienst (directory service) (Netz)Adressen, die einen physischen Ort im Kommunikationsnetz beschreiben, zugeordnet sind [ECMA93_87 Seite 11, ECMATR42_87 Seite 36], ändert daran nichts.

Für viele Anwendungen dürften zufällig oder gar deterministisch (etwa durch anonyme und unverkettbare Anfragen an eine zentrale Instanz) eindeutig gewählte Transaktionsnummern, Kanalnummern, private implizite Adressen etc. vollkommen ausreichen.

In Kommunikationsnetzen ohne Datenschutz kann es aus Leistungs- und Kostengründen sinnvoll sein, die Vermittlungsart, nämlich Kanal-, Nachrichten- oder Paketvermittlung (channel -, message -, packet switching), über verschiedene Teilstrecken einer Verbindung oder in verschiedenen Schichten des Kommunikationssystems verschieden zu wählen. Hierbei trans-

portiere ein *Kanal* eine kontinuierliche und gleichmäßige Folge von Zeichen, die möglicherweise erst nach seiner Einrichtung entstehen. Ein Kanal ist also durch seine zeitlich konstante Bitrate charakterisiert. Kanalvermittlung zwischen zwei Stationen bedeutet, daß diese in die Lage versetzt werden, miteinander über eine kontinuierliche und gleichmäßige, im Allgemeinen mit kurzer Verzögerungszeit übertragenen Folge von Zeichen zu kommunizieren. *Nachrichten* seien Informationseinheiten individuell wählbarer, danach aber konstanter Länge. Die Wahl ihrer Länge wird durch die Anwendung, nicht etwa durch das Kommunikationsnetz bestimmt. Nachrichtenvermittlung bedeutet, daß eine in einer Station vollständig vorliegende Nachricht ggf. mittels Zwischenspeicherungen in anderen Stationen als ganzes zu einer anderen Station vermittelt wird. Hierbei kann jede Station prüfen, ob die Nachricht bisher unversehrt übermittelt wurde und ggf. von der vorherigen Station eine Wiederholung der Übermittlung anfordern. *Pakete* seien Informationseinheiten fester, durch das Kommunikationsnetz vorgegebener Länge. Paketvermittlung bedeutet, daß ein in einer Station vollständig vorliegendes Paket ggf. mittels Zwischenspeicherungen in anderen Stationen zu einer anderen Station vermittelt wird. Hierbei kann jede Station prüfen, ob das Paket bisher unversehrt übermittelt wurde und ggf. von der vorherigen Station eine Wiederholung der Übermittlung anfordern. (Für den nachrichtentechnisch interessierten Leser sei angemerkt, daß sich bezüglich Anonymität nichts Erwähnenswertes ändert, wenn Nachrichten oder Pakete in den Stationen im Allgemeinen *nicht* vollständig vorliegen. Im ersten Fall wird dann von büschelweiser Vermittlung (burst switching [Amst_83, Rei1_86]), im zweiten Fall von asynchronem Übertragungsmodus (asynchronous transfer mode = ATM [ATM_88, BaCh_89, Lutz_88]) gesprochen.)

In Kommunikationsnetzen mit Datenschutz ist es nicht sinnvoll, die Vermittlungsart, nämlich Kanal-, Nachrichten- oder Paketvermittlung, über verschiedene Teilstrecken einer Verbindung oder in verschiedenen Schichten des Kommunikationssystems verschieden zu wählen:

Bei einem Dienst, der einen häufigen Informationstransfer verlangt, wird man entweder versuchen, die Verkettung dieser Informationstransfers durch Unbeteiligte zu verhindern, indem man Nachrichten- oder Paketvermittlung nicht verbindungsorientiert (Datagrammdienst, datagram service) einsetzt, oder man wird Anzahl sowie Beginn und Dauer dieser Informationstransfers vor Unbeteiligten verbergen, indem man mit einer Stromchiffre (Abschnitt 2.2.2.1) einen gleichmäßigen Zeichenstrom Ende-zu-Ende-verschlüsselt. Während ersteres einen Übergang von nicht verbindungsorientierter Nachrichten- oder Paketvermittlung auf verbindungsorientierte Nachrichten-, Paket- oder Kanalvermittlung unmöglich macht, verhindert letzteres einen effizienten Übergang von Kanalvermittlung auf Nachrichten- oder Paketvermittlung, sei sie verbindungsorientiert oder nicht, da Übertragungspausen, etwa Sprechpausen beim Telefonieren, nicht erkannt und deshalb auch nicht zur Einsparung von Übertragungs- und Vermittlungsaufwand genutzt werden können.

Bei einem Dienst, der keinen häufigen Informationstransfer verlangt, wird man immer versuchen, die Verkettung dieser Informationstransfers durch Unbeteiligte zu verhindern, indem man Nachrichten- oder Paketvermittlung nicht verbindungsorientiert (Datagrammdienst, datagram service) einsetzt, was – wie oben – einen Übergang auf eine verbindungsorienterte Vermittlungsart unmöglich macht.

3.1.1 Implizite Adressierung bei Verteilung nur in wenigen Kanälen

In Abschnitt 2.5.1 wurde der Aufwand und der Einsatzbereich verschiedener Möglichkeiten zur impliziten Adressierung bereits ausführlich diskutiert: Zur Kontaktaufnahme mittels einer öffentlichen Adresse sollte, ungeachtet ihres sehr hohen Aufwands, aus Gründen der Unverkettbarkeit von Kommunikationsereignissen ausschließlich verdeckte implizite Adressierung verwendet werden. Ansonsten sollte wegen ihrer größeren Effizienz beim Adreßvergleich immer offene implizite Adressierung mit privaten Adressen verwendet werden.

Weitere erhebliche Effizienzverbesserungen sind allerdings durch Einsparung von Adressierung (und damit sowohl von Adreßauswertung, als auch – wie in Abschnitt 3.2.1 erläutert – von physischem Empfangen) bei Diensten möglich, bei denen man sich aus den in Abschnitt 3.1 geschilderten Gründen dafür entschieden hat, statt der Verkettung einzelner Informationstransfers lieber deren Anzahl sowie Beginn und Dauer vor Unbeteiligten zu verbergen.

Die zur Verteilung von Information zur Verfügung stehende Bandbreite wird in Kanäle passender Bandbreite aufgeteilt. Implizite Adressen werden dann nur noch in wenigen **I-Kanälen** verwendet, so daß alle Teilnehmerstationen erheblich weniger implizite Adressen auswerten müssen. In den anderen Kanälen werden keine mit impliziten Adressen versehenen Nachrichten oder Pakete verteilt, sondern entweder kontinuierliche Informationsströme ganz ohne Adressen (Kanalvermittlung in **K-Kanälen**) oder aber mit (kurzen) Verbindungsadressen versehene Nachrichten oder Pakete (verbindungsorientierte Nachrichten- oder Paketvermittlung in **V-Kanälen**). Die I-Kanäle fungieren hierbei als *Signalisierungskanäle* für die K- und V-Kanäle, d. h. eine Teilnehmerstation, die einer anderen einen kontinuierlichen Informationsstrom oder mit Verbindungsadressen versehene Nachrichten oder Pakete senden will, kündigt ihr dies in einem der I-Kanäle an bzw. handelt es ggf. mit ihr aus.

Natürlich braucht die Anzahl der I-, K- und V-Kanäle nicht statisch festgelegt sein, sondern kann der momentanen Verkehrsverteilung angepaßt werden. K-Kanäle ermöglichen – wie schon implizit gesagt – die Reduktion des Adressierungsaufwands für einen ganzen Informationsstrom auf den der Signalisierungsnachrichten. V-Kanäle können mit erheblich kürzeren Adressen arbeiten, die zudem für die Dauer der Verbindung fest bleiben können. Ersteres spart Übertragungsbandbreite und Größe des Assoziativspeichers für die Adreßerkennung (vgl. Abschnitt 2.5.1), letzteres eliminiert den Aufwand für den ständigen (informationstheoretisch sicheren oder kryptographisch starken) Wechsel der offenen impliziten Adressen.

In den von allen Stationen genutzten I- und V-Kanälen ist in jedem Fall ein die Anonymität des Senders erhaltendes Mehrfachzugriffsverfahren nötig, das zudem keine Verkehrsereignisse, außer den sowieso schon über Verbindungsadressen verketteten, verketten sollte.

Die **Aufteilung der Bandbreite** in I-, V- und K-Kanäle nimmt zweckmäßigerweise eine entweder statisch oder dynamisch ausgewählte Station vor, ebenfalls die Vergabe von K-Kanälen. Anderenfalls entsteht bei letzterem auch ein Mehrfachzugriffsproblem und für ersteres ein Einigungs- und Koordinations-Problem.

3.1.2 Mehrfachzugriff beim DC-Netz für Pakete, Nachrichten und Kanäle

In Abschnitt 3.1.2.1 werden zunächst allgemeine *Kriterien* für die Anonymitäts- und Unverkettbarkeitserhaltung (vgl. Abschnitt 2.6) von Mehrfachzugriffsverfahren für das DC-Netz (und RING-2-f-Netz) aufgestellt.

Danach werden die bekannten, die Anonymität des Senders erhaltenden und Verkehrsereignisse nicht verkettenden Mehrfachzugriffsverfahren in Abschnitt 3.1.2.2 *in Klassen eingeteilt*, und in Abschnitt 3.1.2.3 beschrieben und so modifiziert, daß ihre Leistung beim überlagernden Senden durch die bestimmbare *Anzahl kollidierter Informationseinheiten* oder *globales überlagerndes Empfangen* oder beides ohne signifikanten Mehraufwand ganz erheblich gesteigert wird.

Anschließend wird in Abschnitt 3.1.2.4 die Eignung der die Anonymität des Senders erhaltenden und Verkehrsereignisse nicht verkettenden Mehrfachzugriffsverfahren für das Senden von *Paketen*, *Nachrichten* und *kontinuierlichen Informationsströmen* (Kanäle) diskutiert.

Darauf aufbauend wird in Abschnitt 3.1.2.5 der Einsatz von *paarweisem überlagernden Empfangen* erläutert.

Schließlich wird in Abschnitt 3.1.2.6 untersucht, wie die Bandbreite des DC-Netzes bei (anonymen) *Konferenzschaltungen* möglichst effizient genutzt werden kann.

In Abschnitt 3.1.2.7 als globales Resümee wird zu einer *Kombination von Mehrfachzugriffsverfahren* in jeweils separaten Kanälen geraten.

3.1.2.1 Kriterien für die Erhaltung von Anonymität und Unverkettbarkeit

Mehrfachzugriffsverfahren sollten, um die Anonymität des Senders zu erhaltenden und Verkehrsereignisse nicht zu verketten,

1. *alle Stationen absolut gleich behandeln bzw. handeln lassen* (beispielsweise sollten Stationen keine eineindeutige Nummer wie in dem Bitleisten-Protokoll (Bit-Map Protocol) in [Tane_81 Seite 296] oder in dem Gruppentest-Protokoll (Group Testing Protocol) in [BMTW_84 Seite 771] haben),
2. *keine Beziehungen zwischen Verkehrsereignissen herstellen* (beispielsweise „Wenn dies von Station *A* gesendet wurde, wurde jenes von Station *B* gesendet.“ oder „Wenn dies von Station *A* gesendet wurde, wurde jenes nicht von Station *B* gesendet.“, wobei in beiden Fällen in der Praxis häufig *A=B* vorkommt),
3. jeder Station *erlauben, die gesamte Bandbreite zu nutzen*, wenn keine andere Station etwas sendet.

1. ist notwendig und hinreichend für *perfekte Anonymitätserhaltung* des Senders. Mit dem in Abschnitt 2.5.3.1.2 für das überlagernde Senden bzw. in Abschnitt 2.5.3.2.1 für das RING-2-f-Netz geführten Beweis ist 1. auch hinreichend für perfekte informationstheoretische Anonymität des Senders, sofern dieser sich nicht über den Nachrichteninhalt oder verkettbare Nachrichten explizit identifiziert.

2. ist notwendig und hinreichend für *perfekte Unverkettbarkeitserhaltung*. Mit dem in Abschnitt 2.5.3.1.2 für das überlagernde Senden bzw. in Abschnitt 2.5.3.2.1 für das RING-2-f-Netz geführten Beweis ist 2. auch hinreichend für perfekte informationstheoretische Unverkettbarkeit von Sendeereignissen, sofern diese nicht über den Nachrichteninhalt oder Adressen explizit verkettet sind.

3. ist notwendig für *perfekte Unverkettbarkeitserhaltung*. Dürfte nicht jede Station die gesamte Bandbreite nutzen, wären alle nahezu gleichzeitig stattfindenden Sendeereignisse insoweit verkettbar, daß sie nicht alle von derselben Station (sofern nur manche Stationen nicht die gesamte Bandbreite nutzen dürfen: ... sie nicht alle von einer dieser Stationen) stammen.

3.1.2.2 Klasseneinteilung von Anonymität und Unverkettbarkeit erhaltenden Mehrfachzugriffsverfahren

1. Welche Anforderung bezüglich Verzögerungszeit des zu verwaltenden, durch überlagerndes Senden gebildeten Verteil-Kanals stellt das Mehrfachzugriffsverfahren? Kommt es mit einem Kanal von beliebig großer Verzögerungszeit zwischen dem Senden eines Zeichens und der Rückmeldung, was das Ergebnis der globalen Überlagerung war, aus oder sinkt seine Effizienz mit Erhöhung der Verzögerungszeit des Kanals drastisch, so daß es im Grunde auf einen Kanal mit einer Verzögerungszeit, die kurz bezüglich der Übertragungszeit eines Paketes oder einer Nachricht ist, zugeschnitten ist?
2. Darf ein Paket oder eine Nachricht vom Sender einfach gesendet werden, oder muß zuvor eine Reservierung erfolgen? Im letzteren Fall kann die Verzögerungszeit für die Übertragung von Paketen oder Nachrichten natürlich nie kleiner als die zweifache Verzögerungszeit des Kanals sein, während im ersteren Fall, sofern keine Kollision auftritt, die Verzögerungszeit für die Übertragung genau eine Verzögerungszeit des Kanals ist. (Hier wie im ganzen Rest dieses Abschnitts bezieht sich Kollision immer auf die Überlagerung und nicht auf die Übertragung, so daß die längere Schreibweise Überlagerungs-Kollision vermieden werden kann.)
3. Schreibt das Mehrfachzugriffsverfahren vor, was im Falle einer Kollision zu tun ist, oder regelt es das Verhalten bei erfolgreichem Senden, d. h. keinem Auftreten einer Kollision?
4. Was ist im Falle einer Kollision vorgeschrieben: Nochmaliges Senden nach zufälliger Zeitdauer, Kollisionsauflösung oder nochmaliges Senden nach zufälliger, aber angekündigter Zeitdauer?

Mit dieser Klasseneinteilung und der Beschränkung auf die leistungsfähigeren **synchronen Mehrfachzugriffsverfahren** (die in anderen Netzen wichtigen *asynchronen Mehrfachzugriffsverfahren* sind beim überlagernden Senden deshalb uninteressant, da bei ihm bereits aus Gründen der sich gegenseitig aufhebenden Überlagerung von Schlüsseln Synchronität herrschen muß und diese für das Mehrfachzugriffsverfahren ohne zusätzlichen Aufwand mitverwendet werden kann), ergeben sich folgende interessante Klassen:

beliebiger Kanal
- direkte Übertragung
  - bei Kollision
    - nochmaliges Senden nach zufälliger Zeitdauer (slotted ALOHA)
    - Kollisionsauflösung (splitting algorithm)
    - nochmaliges Senden nach zufälliger, aber angekündigter Zeitdauer (ARRA)
  - bei Erfolg Reservierung (R-ALOHA)
- Reservierungsschema (Roberts' scheme)

Kanal mit kurzer Verzögerungszeit
- direkte Übertragung bei ungenutztem Kanal
  - bei Kollision
    - nochmaliges Senden nach zufälliger Zeitdauer (CSMA)
    - Abbruch und nochmaliges Senden nach zufälliger Zeitdauer (CSMA/CD)
    - Kollisionsauflösung (CSMA/splitting algorithm)
    - nochmaliges Senden nach zufälliger, aber angekündigter Zeitdauer (CSMA/ARRA)
  - bei Erfolg Reservierung (R-CSMA)

Diese Klassen werden im folgenden der Reihe nach behandelt.

Die in der Literatur beschriebenen und kurz wiedergegebenen gebräuchlichen Mehrfachzugriffsverfahren dieser Klassen verwenden nur die Information „keine Übertragung", d. h. niemand sendet, „erfolgreiche Übertragung", d. h. genau einer sendet, oder „Übertragungs-Kollision", d. h. mehr als einer sendet (so daß alle Übertragungen gestört sind), da eine genauere Analyse bei den üblicherweise betrachteten Funk-, Satelliten- und Busnetzen entweder überhaupt nicht möglich oder zu aufwendig ist. In diesen Funk-, Satelliten- und Busnetzen wird diese **ternäre Rückmeldung** in die analogen Signalcharakteristika nutzender Weise implementiert. Dies kann in der rein digitalen Welt des überlagernden Sendens simuliert werden, indem an jede Ende-zu-Ende-verschlüsselte Nachricht (die für alle außer dem Empfänger genausogut die Summe einiger Nachrichten sein könnte) ein nichtlinear gebildetes Prüfzeichen angehängt wird (Vorsicht: die üblichen Prüfzeichen sind linear, z. B. CRC = cyclic redundancy check). Dann kann jeder prüfen, ob das Prüfzeichen zu der Nachricht paßt. Die Summe mehrerer Nachrichten und der zugehörigen Prüfzeichen ergibt dann mit sehr hoher Wahrscheinlichkeit eine „Nachricht", zu der das „Prüfzeichen" nicht paßt. Lauter der 0 entsprechende Zeichen als Ergebnis der globalen Überlagerung entsprechen mit sehr großer Wahrscheinlichkeit „keiner Übertragung".

Bei jeder Klasse von Mehrfachzugriffsverfahren wird untersucht, ob und wie ihre Leistung durch Benutzung der Kenntnis der Anzahl kollidierter Informationseinheiten oder überlagerndes Empfangen oder beides gesteigert werden kann.

Hierbei kann die Kenntnis der Anzahl kollidierter Informationseinheiten exakt oder probabilistisch sein. Sie ist genau dann exakt, wenn die Größe g des zum überlagernden Senden verwendeten Alphabets größer als die maximal kollidierende Anzahl von Informationseinheiten i ist. Sofern jede der s Stationen maximal m Informationseinheiten gleichzeitig senden darf, und damit $i = s \cdot m$, muß also gelten: $g > s \cdot m$. Dann kann einfach vereinbart werden, daß das erste Zeichen jeder Informationseinheit immer das der 1 entsprechende ist, so daß die Summe aller

ersten Zeichen immer das der Anzahl der gleichzeitig gesendeten Informationseinheiten entsprechende Zeichen ergibt. In allen bisher veröffentlichten Mehrfachzugriffsverfahren ist m=1.

Nun werden Mehrfachzugriffsverfahren bisher immer so entworfen, daß sie versuchen, die Anzahl der gleichzeitig kollidierenden Informationseinheiten klein zu halten, da nur dann die Wahrscheinlichkeit eines erfolgreichen, d. h. Übertragungs-kollisionslosen Sendens groß ist und nur dann Übertragungs-Kollisionsauflösungen effizient stattfinden können. Auch für sehr große Stationsanzahlen s wird man also mit einem g in der Größenordnung von 50 bei den bisher entworfenen Mehrfachzugriffsverfahren fast immer die richtige Anzahl kollidierter Informationseinheiten vermuten. Da bei sehr großen Stationszahlen die Wahl solch eines g mit $g << s \bullet m$. durchaus Bandbreite einsparen kann, stellt sich mit der Berechnung des jeweils optimalen g für die im folgenden hergeleiteten Mehrfachzugriffsverfahren mit Benutzung der Kenntnis der Anzahl kollidierter Informationseinheiten (unter Berücksichtigung der Verkehrsverteilung und ggf. sogar der Kosten für die Implementierung des Überlagerungskanals, insbesondere genügend schneller Additionsglieder modulo g – vgl. Abschnitt 3.2.3 – sowie der physischen Fehlerrate bei der Überlagerung und Übertragung, die in realen Kommunikationsnetzen „exakte“ Kenntnis sowieso probabilistisch macht) ein interessantes Thema für weitere Arbeiten.

Da die Optimierung von g zahlreiche Parameter enthält und das Verständnis der folgenden Mehrfachzugriffsverfahren erschweren würde, werde ich bei ihrer Untersuchung nur die Fälle des besonders einfach zu implementierenden binären überlagernden Sendens (g=2) und überlagernden Sendens modulo g mit $g > s \bullet m$ unterscheiden. Eine weitere Begründung für die Einschränkung ist, daß die im folgenden hergeleiteten Mehrfachzugriffsverfahren den Durchsatz (im Sinne des Anteils der nutzbaren Bandbreite) im Falle direkter Übertragung von knapp 50% auf weit über 90% steigern, während durch die skizzierte Optimierung von g nur Effizienzverbesserungen im Promille-Bereich zu erwarten sind.

3.1.2.3 Beschreibung und ggf. Anpassung der in Klassen eingeteilten Mehrfachzugriffsverfahren

Bis auf den letzten Unterabschnitt behandeln alle Unterabschnitte Mehrfachzugriffsverfahren, die bei einem Kanal beliebiger Verzögerungszeit verwendet werden können.

Die ersten drei Unterabschnitte behandeln Mehrfachzugriffsverfahren, die eine direkte Übertragung erlauben. In Abschnitt 3.1.2.3.1 wird bei einer Kollision nach einer zufälligen Zeitdauer noch einmal gesendet (slotted ALOHA), in Abschnitt 3.1.2.3.2 findet dann eine Kollisionsauflösung statt und Abschnitt 3.1.2.3.3 nach einer zufälligen, aber angekündigten Zeitdauer (ARRA) noch einmal gesendet.

In Abschnitt 3.1.2.3.4 wird der Fall behandelt, daß eine kollisionslose Übertragung zugleich als als Reservierung genutzt wird. Abschnitt 3.1.2.3.5 behandelt dann ein konventionelles Reservierungsschema.

Schließlich wird in Abschnitt 3.1.2.3.6 diskutiert, welche Verbesserungen der Mehrfachzugriffsverfahren dann möglich sind, wenn der Kanal eine kurze Verzögerungszeit besitzt.

3.1.2.3.1 Direkte Übertragung, bei Kollision nochmaliges Senden nach zufälliger Zeitdauer (slotted ALOHA)

Wie bereits in Abschnitt 2.5.3.1.1 erwähnt, wurde die Verwendung dieses Anonymität perfekt erhaltenden Mehrfachzugriffsverfahrens, mit dem ein Durchsatz von maximal 1/e ≈ 36,8% erzielt werden kann [Tane_81 Seite 256], bereits in [Cha3_85] vorgeschlagen. Damit es auch die Unverkettbarkeit von Sendeereignissen perfekt erhält, müssen allerdings – wie in Abschnitt 2.5.3.1.2 schon erwähnt – kollidierte Informationseinheiten vor nochmaligem Senden umgeschlüsselt werden, sofern nicht $m>1$ ist und global überlagernd Empfangen wird.

Durch exakte wie auch durch probabilistische Kenntnis der Anzahl kollidierter Informationseinheiten kann die Verteilung der Zeitdauern bis zum nochmaligen Senden geregelt werden, wodurch die in [Rive_87, ApSP_87, GrFL_87] analysierten kürzeren mittleren Übertragungszeiten sowie Stabilität des ansonsten instabilen (wenn viele senden, kann so gut wie niemand mehr erfolgreich senden, durch das nochmalige Senden wird die Senderate erhöht,...) Mehrfachzugriffsverfahrens erzielt werden.

Globales überlagerndes Empfangen ist möglich, doch wird es vom Mehrfachzugriffsverfahren in keiner Weise unterstützt: Jedes Kollisionsergebnis muß möglicherweise sehr lange aufgehoben werden. Von jedem Kollisionsergebnis müssen im Falle binären überlagernden Sendens alle Teilmengen der folgenden Informationseinheiten (egal ob es sich um das Ergebnis einer Kollision handelt oder nicht) immer wieder versuchsweise subtrahiert werden, bis eine Informationseinheit mit passendem Prüfzeichen entsteht. Diese sollte dann wie eine gesendete Informationseinheit behandelt, d. h. in die Teilmengenbildung einbezogen werden. Im Falle des verallgemeinerten überlagernden Sendens müssen bei der Teilmengenbildung jeweils bezüglich aller folgenden Informationseinheit noch alle relevanten Möglichkeiten des Überlagerns, nämlich Addition und Subtraktion sowie bis zur Anzahl der überlagerten Kollisionsergebnisse auch mehrfache Addition oder Subtraktion ausprobiert werden. Natürlich kann (und muß) man die Zahl der von allen Stationen jeweils in gleicher Weise zu untersuchenden Möglichkeiten einschränken. Dadurch „verliert“ man aber im Prinzip bereits übertragene Information.

Durch zusätzliche Verwendung exakter wie auch probabilistischer Kenntnis der Anzahl kollidierter Informationseinheiten brauchen nur noch Teilmengen bis zu dieser Anzahl minus 1 probeweise subtrahiert zu werden. Aber auch dies ist immer noch unnötig aufwendig, wie das als nächstes beschriebene Mehrfachzugriffsverfahren mit Kollisionsauflösung zeigt, und kann – wegen dem immer noch in der Zahl der seit einer Kollision übertragenen Informationseinheiten exponentiellen Aufwand – insbesondere nicht bis in eine beliebig zurückliegende Vergangenheit erstreckt werden, so daß man auch hier bereits übertragene Information „verliert“.

3.1.2.3.2 Direkte Übertragung, bei Kollision Kollisionsauflösung (splitting algorithm)

Wie bereits in [Pfi1_85 Seite 41] erwähnt, sollte aus Leistungsgründen statt nochmaligem Senden nach zufälliger Zeitdauer eine anonyme Kollisionsauflösung mit einem der in [Mass_81, Gall_85, Li_87] beschriebenen Kollisionsauflösungsalgorithmen durch rekursive Teilung der Sendenden (splitting algorithm) durchgeführt werden. Ein einfacher, von Massey

beschriebener, anonymer Kollisionsauflösungsalgorithmus (collision resolution algorithm) durch **rekursive Teilung der Sendenden** arbeitet folgendermaßen:

Findet eine Kollision statt, dürfen solange nur noch die an der Kollision Beteiligten senden, bis die Kollision aufgelöst, d. h. alle beteiligten Informationseinheiten erfolgreich übertragen sind.

Jeder an der Kollision Beteiligte schließt sich zufällig, etwa indem er eine faire Münze wirft, einer von zwei disjunkten Teilmengen an: die erste Teilmenge sendet sofort wieder, während die zweite solange wartet, bis die erste erfolgreich übertragen hat.

Findet beim Senden einer Teilmenge eine Kollision statt, so teilt sie sich und jede (Unter-)Teilmenge verfährt rekursiv nach demselben Algorithmus.

Findet eine erfolgreiche Übertragung der ersten bzw. zweiten Teilmenge statt, so weiß die zweite Teilmenge bzw. die übergeordnete zweite Teilmenge, daß jetzt sie an der Reihe ist.

Findet bei einer ersten Teilmenge keine Übertragung statt, so weiß die zweite Teilmenge, daß sie mindestens zwei Elemente enthält, deren Senden sicher kollidieren würde, wenn sie jetzt einfach alle sofort senden würden. Deshalb teilt sich in diesem Fall die zweite Teilmenge sofort in abermals zwei Teilmengen, die je wie gerade geschildert verfahren.

Der Ablauf dieses mit ternärer Rückmeldung auskommenden rekursiven Teilungsalgorithmus ist in Bild 31 an einem Beispiel veranschaulicht.

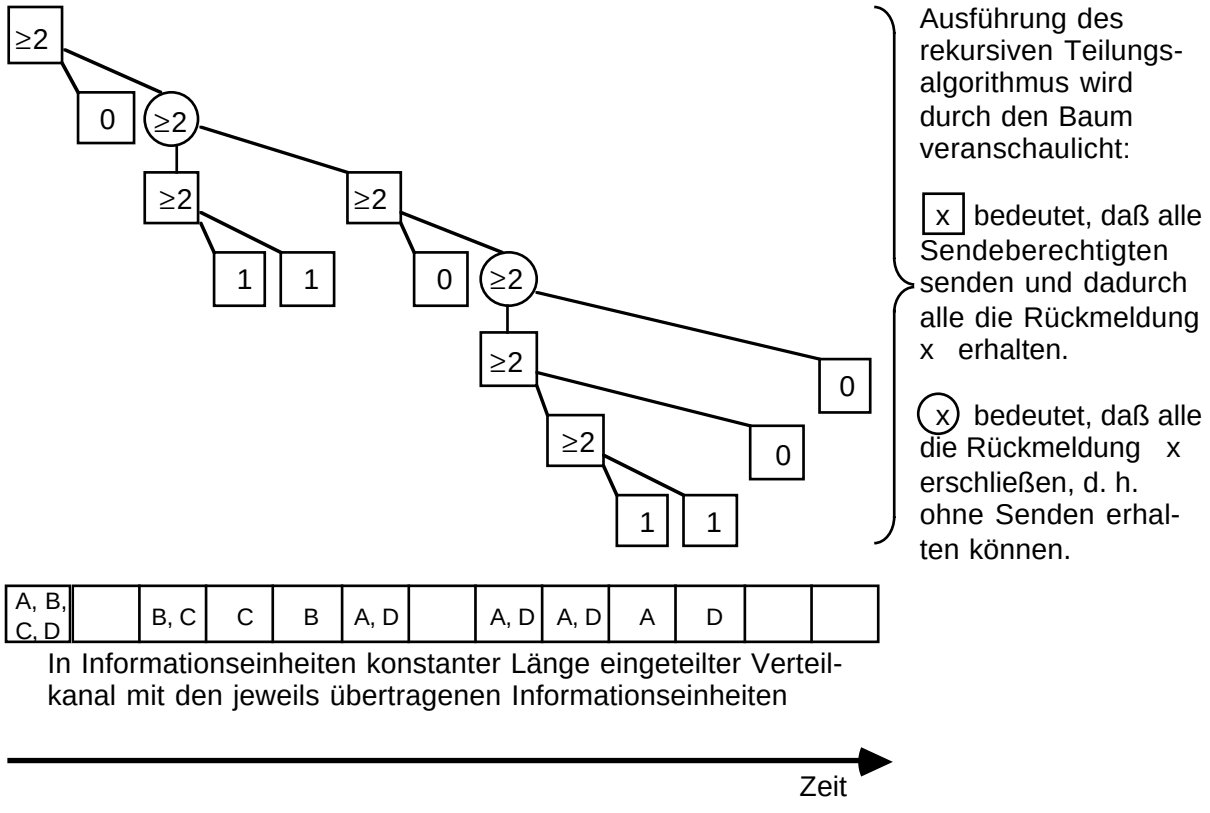


Bild 31: Eine Möglichkeit der Auflösung einer Kollision von 4 Informationseinheiten A, B, C und D mit dem von Massey beschriebenen einfachen Kollisionsauflösungsalgorithmus

Wie in [Mass_81 Seite 120] beschrieben, kann statt einem Münzwurf auch die genaue Ankunftszeit der jeweils zu übertragenden Informationseinheit verwendet werden. Informationseinheiten dürfen nur dann gesendet werden, wenn ihre Ankunftszeit innerhalb eines global bekannten Zeitintervalls liegt (*Zeitintervallverfahren*). Durch Halbierung des global bekannten Zeitintervalls kann dann, wie durch das Werfen einer Münze, eine „Halbierung" der Sendeberechtigten erreicht werden. Dies Verfahren erlaubt es zu erreichen, daß Informationseinheiten gemäß ihren Ankunftszeiten übertragen werden (First Come First Serve = FCFS), was für manche Anwendungen ein großer Vorteil sein mag. Bezüglich der Unverkettbarkeit von Informationseinheiten ist die Verwendung ihrer Ankunftszeiten beim Kollisionsauflösungsalgorithmus jedoch schädlich: Weiß ein Angreifer, wann eine Teilnehmerstation eine Informationseinheit erhalten hat und wie schnell sie sie verarbeitet, kann er bei Verwendung der Ankunftszeiten beim Kollisionsauflösungsalgorithmus beide Informationseinheiten einander mit größerer Wahrscheinlichkeit zuordnen. Sind ihm die bei der momentanen Verkehrssituation benutzten Zeitintervalle dazu zu groß, so kann er Kollisionen provozieren und dadurch eine beliebige Verkleinerung der Zeitintervalle erzwingen. Ebenfalls schädlich ist das Zeitintervallverfahren, wenn nicht alle Teilnehmerstationen gleiche Eigenschaften bezüglich der Informationsverarbeitung haben: Sendet ein Angreifer einer Teilnehmerstation eine Informationseinheit und registriert das beim Erhalt der Antwort gültige Zeitintervall (das er – wie gerade beschrieben – beliebig verkleinern kann), so kann er mehr über die Teilnehmerstation (und ggf. den Teilnehmer) erfahren als bei Verwendung des Münzwurfs zur „Halbierung" der Sendeberechtigten. Bezogen auf das Zeitintervallverfahren stellt die Verwendung des Münzwurfs also eine „zeitlich entkoppelte Verarbeitung" im Kleinen dar, vgl. Abschnitt 2.4. Statt Zeitintervallen könnten natürlich auch Intervalle irgendeiner anderen Art zusammen mit passenden Kriterien für Informationseinheiten verwendet werden, z. B. räumliche Intervalle und Ort des Senders. Es ist offensichtlich, daß in diesem Beispiel die Senderanonymität untergraben würde. Vor der Verwendung von Intervallen ist also nachzuweisen, daß sie weder die Unverkettbarkeit noch die Anonymität untergraben.

Nötig ist noch ein Algorithmus, der regelt, wann neue Informationseinheiten erstmals übertragen werden. Er sollte verhindern, daß nach einer besonders langen Kollisionsauflösung im Mittel besonders viele Informationseinheiten zur Übertragung anstehen, gesendet werden und kollidieren (was im Mittel wieder eine besonders lange Kollisionsauflösung nötig machen würde). Kombiniert man einen geeigneten Entkopplungsalgorithmus mit dem obigen Kollisionsauflösungsalgorithmus, ergibt sich für diesen einfachen rekursiven Teilungsalgorithmus ein Durchsatz von maximal 46,2%, während kompliziertere, aber ebenfalls anonyme 48,785% erreichen, was das bisherige Maximum für Kanäle mit Mehrfachzugriff und ternärer Rückmeldung ist [Mass_81 Seite 120].

Eine dediziertere als ternäre Rückmeldung (beispielsweise $g > s \bullet m$) kann nun verwendet werden, um die Sendenden ggf. in mehr als zwei Gruppen zu teilen und dabei im Mittel Kollisionen zu vermeiden.

Der Einsatz **globalen überlagernden Empfangens** steigert den Durchsatz und senkt die mittlere Verzögerungszeit aber selbst bei ternärer Rückmeldung weit mehr:

> Findet eine Kollision statt, dürfen solange nur noch die an der Kollision Beteiligten senden, bis die Kollision aufgelöst, d. h. alle beteiligten Informationseinheiten erfolgreich übertragen sind.

Jeder an der Kollision Beteiligte schließt sich zufällig, etwa indem er eine faire Münze wirft, einer von zwei disjunkten Teilmengen an: die erste Teilmenge sendet sofort wieder, während die zweite solange wartet, bis die erste erfolgreich übertragen hat.
Die erste Gruppe sendet und ihr Ergebnis wird von der „übergeordneten“ Kollision subtrahiert. Hierdurch wird in jedem Fall bereits die Summe aller Informationseinheiten der zweiten Gruppe erhalten, was beim obigen Kollisionsauflösungsalgorithmus ohne überlagerndes Empfangen teilweise erst durch eine explizite Übertragung erreicht wird.
Findet beim Senden einer Teilmenge eine Kollision statt, so teilt sie sich und jede (Unter-)Teilmenge verfährt rekursiv nach demselben Algorithmus.
Findet eine erfolgreiche Übertragung statt, so weiß die zweite Teilmenge bzw. ggf. die übergeordnete zweite Teilmenge etc., daß jetzt sie an der Reihe ist.
Findet keine Übertragung statt, so weiß die zweite Teilmenge, daß sie mindestens zwei Elemente enthält, deren Senden sicher kollidieren würde, wenn sie jetzt einfach alle sofort senden würden. Deshalb teilt sich in diesem Fall die zweite Teilmenge sofort in abermals zwei Teilmengen, die je wie gerade geschildert verfahren.

Der Ablauf dieses mit ternärer Rückmeldung auskommenden rekursiven Teilungsalgorithmus mit globalem überlagernden Empfangen ist in Bild 32 am in Bild 31 verwendeten Beispiel veranschaulicht.

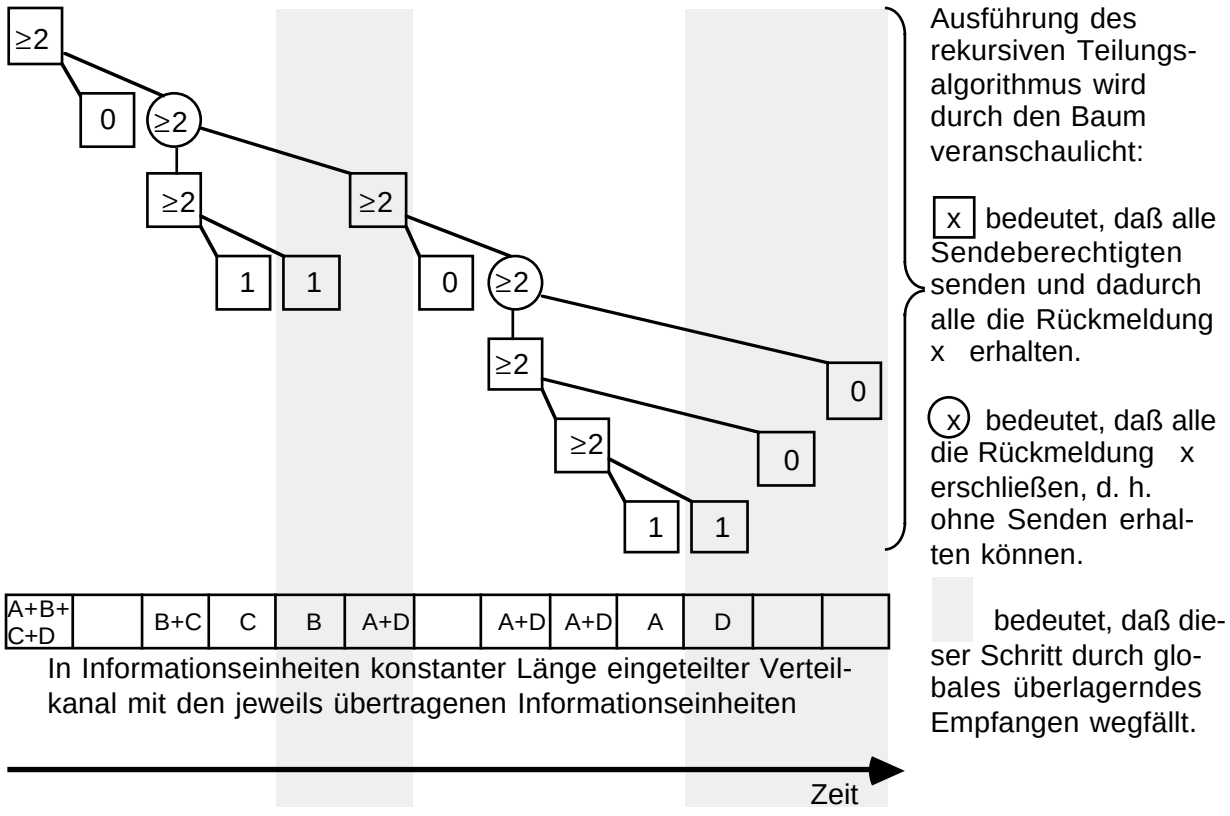


Bild 32: Eine Möglichkeit der Auflösung einer Kollision von 4 Informationseinheiten A, B, C und D mit dem von Massey beschriebenen einfachen Kollisionsauflösungsalgorithmus und globalem überlagerndem Empfangen

Wie der Beschreibung des modifizierten Kollisionsauflösungsalgorithmus direkt zu entnehmen ist, braucht nach jeder gesendeten Informationseinheit zum Zwecke des globalen überlagernden Empfangens maximal eine Subtraktion und ein Vergleich durchgeführt zu werden, so daß der Aufwand für globales überlagerndes Empfangen bereits minimal ist. Allerdings kann der **Kollisionsauflösungsalgorithmus** noch erheblich verbessert werden, indem er für den Fall einer Kollision von genau **zwei Informationseinheiten deterministisch** gemacht wird:

> Subtrahiert im Falle einer Kollision jeder Sender seine gesendete Informationseinheit vom Kollisionsergebnis und überprüft, ob das Subtraktionsergebnis eine kollisionsfreie Informationseinheit ist, so können die Sender feststellen, ob 2 oder mehr Informationseinheiten kollidierten. Waren es mehr als zwei, wird wie im gerade beschriebenen Kollisionsauflösungsalgorithmus verfahren. Waren es genau 2, so sendet deterministisch nur derjenige seine Informationseinheit noch mal, dessen Informationseinheit (interpretiert als Zahl) größer ist, so daß diese direkt und die andere durch globale Überlagerung empfangen werden kann. Dies ist mit dem oben beschriebenen Kollisionsauflösungsalgorithmus verträglich, da derjenige mit der größeren Informationseinheit sich zufällig der ersten, und derjenige mit der kleineren Informationseinheit sich zufällig der zweiten Teilmenge hätte anschließen können.
>
> Die Wahrscheinlichkeit, daß zwei kollidierende Informationseinheiten gleich sind und deshalb dieses Verfahren zwischen ihnen keine „deterministische“ Kollisionsauflösung erreichen kann, ist so klein, daß sie bei der Begriffsbildung bewußt ignoriert wurde: Informationseinheiten, die unabhängig von anderen übertragen und deshalb von diesem Mehrfachzugriffsverfahren behandelt werden, haben schon aus Gründen der impliziten Adressierung mindestens 50 Bit Länge. Außerdem kann bei Ende-zu-Ende-Verschlüsselung von einer Gleichverteilung der Bitmuster bei den Nutzdaten der Informationseinheiten ausgegangen werden. Zusammen ergibt dies so geringe Wahrscheinlichkeiten, daß zwei kollidierende Informationseinheiten gleich sind, daß die Wahrscheinlichkeit von Fehlern um Größenordnungen höher ist. Da Fehler sowieso geeignet behandelt werden müssen (vgl. Kapitel 5) und die dazu verwendeten Verfahren diese Situation gleich mitbehandeln können, wird auf sie im folgenden nicht weiter eingegangen.
>
> Obwohl bei einer Kollision von genau 2 Informationseinheiten die beiden an der Kollision beteiligten Stationen die Informationseinheit der anderen früher als die nicht beteiligten durch paarweises überlagerndes Empfangen erhalten könnten, sollten sie dies nicht nutzen: Reagiert eine Station auf eine nicht Empfänger-anonyme Informationseinheit nach einer Kollision von genau 2 Informationseinheiten schneller als sie das als nicht beteiligte könnte, kann sie dadurch als Sender einer möglicherweise mit dem Vorsatz der Sender-Anonymität gesendeten Informationseinheit identifiziert werden.

Der Ablauf dieses mit ternärer Rückmeldung auskommenden rekursiven Teilungsalgorithmus mit globalem überlagernden Empfangen und deterministischer Auflösung von Zweierkollisionen ist in Bild 33 am in den Bildern 31 und 32 verwendeten Beispiel veranschaulicht.

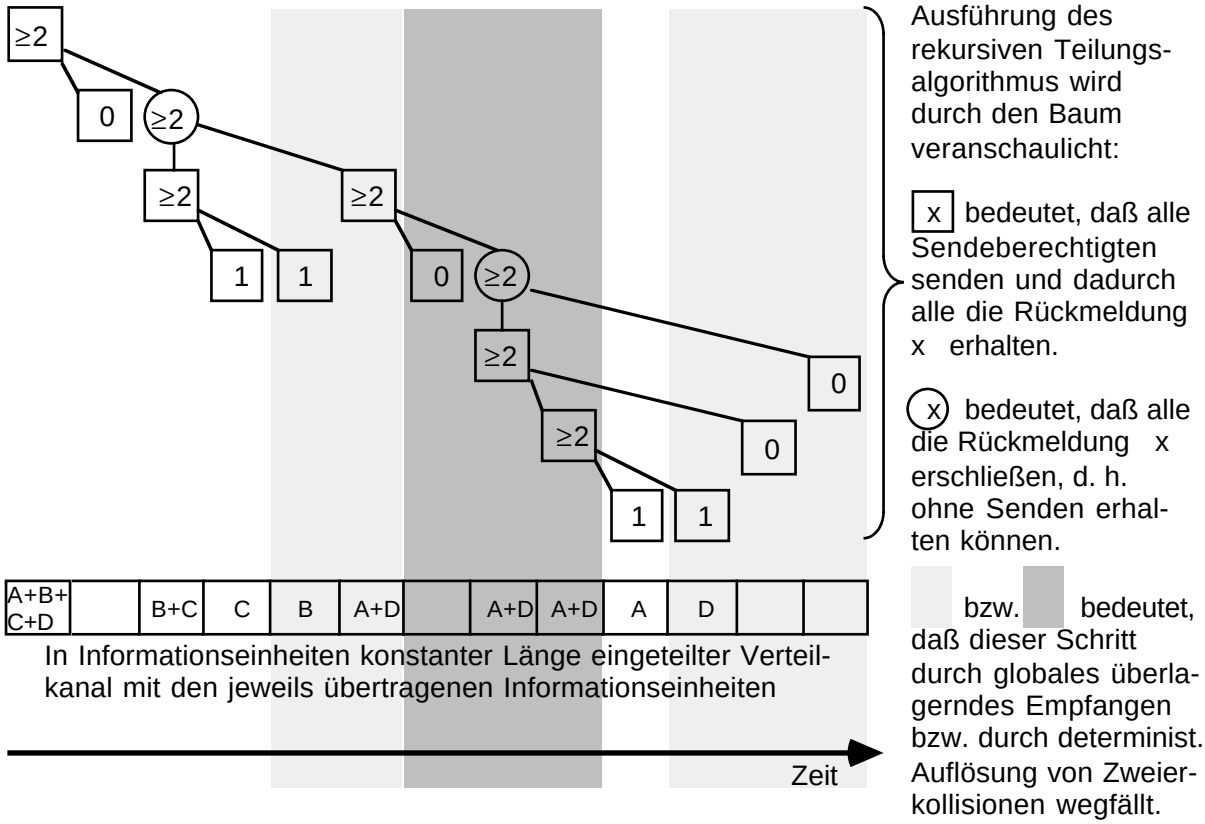


Bild 33: Eine Möglichkeit der Auflösung einer Kollision von 4 Informationseinheiten A, B, C und D mit dem von Massey beschriebenen einfachen Kollisionsauflösungsalgorithmus, deterministischer Auflösung von Zweierkollisionen und globalem überlagerndem Empfangen

Im folgenden ist dieser zweifach verbesserte Kollisionsauflösungsalgorithmus in einer der Programmiersprache Ada [REFE_83] ähnlichen Syntax beschrieben. Dies ist lohnend, da er hinreichend kompliziert und Umgangssprache bekanntlich hin und wieder mehrdeutig ist. Mein Ziel war es, eine möglichst verständliche, d. h. an die umgangssprachliche Formulierung anknüpfende formale Beschreibung zu finden. Durch Vermeiden der Rekursion effizientere, d. h. realisierungsnähere Beschreibungen mit expliziter Ausprogrammierung der Kellerung von Kollisionsergebnissen sind in [Marc_88] enthalten.

Der Kollisionsauflösungsalgorithmus ist in ein kombiniertes Sende- und Empfangsprotokoll eingebettet, das von allen Stationen in gleicher Weise ausgeführt wird und in drei, teilweise rekursiven Prozeduren formuliert ist:

Die äußere Prozedur *Sende-_und_Empfangsprotokoll* verwendet einen in ihrer Umgebung geeignet definierten Datentyp *puffer*, dessen Variablen jeweils eine bzw. auch 0 oder mehrere überlagerte Informationseinheiten speichern können. Werte dieses Datentyps liefere die ebenfalls in der Umgebung definierte Funktion *Sendewunsch*, wobei die Station genau dann einen Sendewunsch hat, wenn *Sendewunsch* einen Wert ≠ 0 liefert. *Sende-_und_Empfangsprotokoll* ruft die mittlere Prozedur *Zugriff* auf, wobei beim Aufruf deren erster Parameter *Sendeerlaubnis* genau dann mit TRUE initialisiert wird, wenn die Station einen Sendewunsch hat. Der zweite Parameter von *Zugriff*, der bei rekursivem Aufruf von *Zugriff* zur Übergabe des von

Zugriff empfangen Wertes an den Aufrufer verwendet wird, wird in der Prozedur *Sende-_und_Empfangsprotokoll* nicht verwendet.

Die mittlere Prozedur *Zugriff* verwendet die in der Umgebung geeignet vordefinierten Prozeduren *Sende* und *Empfange*, die jeweils einen Wert des Datentyps *puffer* senden bzw. empfangen. Danach ruft *Zugriff* die innere Prozedur *Analysiere_Empfangenes* auf.

Analysiere_Empfangenes verwendet die in der Umgebung geeignet vordefinierte Funktion |...| vom Wertebereich des Datentyps *puffer* in den Wertebereich des Datentyps NATURAL (die natürlichen Zahlen inklusive Null). |*e*| gibt die Zahl der in *e* überlagerten Informationseinheiten an. In der angegeben Form kann |...| nur bei $g > s \bullet m$ realisiert werden. Da von all diesen Werten aber nur die Werte 0, 1, 2, und > 2 unterschieden werden, kann die Funktion |...| selbst bei binärem überlagernden Senden realisiert werden:

|*e*| = 0 gdw. *e*=0,
|*e*| = 1 gdw. das nichtlinear gebildete Prüfzeichen paßt,
|*e*| = 2 gdw. der die Funktion auswertende Sendeerlaubnis besitzt und für das von ihm Gesendete *s* gilt: |*e-s*| = 1, sowie
|*e*| > 2 sonst.

Dies bedeutet, daß an einer Zweierkollision nicht Beteiligte sie nicht als solche erkennen (können) und |*e*| > 2 unterstellen. Wie eine Analyse des untenstehenden kombinierten Sende- und Empfangsprotokolls mittels Vergleich der Fälle |*e*| = 2 und |*e*| > 2 in *Analysiere_Empfangenes* ergibt, führt dies zu keinen Problemen, da die nicht Beteiligten keine Sendeerlaubnis haben und sich bezüglich des Empfangens kompatibel verhalten: Wird statt dem Zweig |*e*| = 2 der Zweig |*e*| > 2 durchlaufen,

- besteht in ihm keine Sendeerlaubnis, so daß das Ergebnis des „Münzwurfs“ der in der Umgebung geeignet vordefinierten Funktion *Münze* für den Ablauf irrelevant ist,
- wird beim Aufruf von *Zugriff* ebenfalls genau eine (andere) Station senden,
- wird danach die zweite Informationseinheit durch einen weiteren Aufruf von *Analysiere_Empfangenes* ebenfalls durch globales Überlagern, d. h. ohne nochmaliges Senden empfangen,
- endet der Aufruf der ursprünglichen Prozedur(inkarnation) *Analysiere_Empfangenes* ebenfalls.

Analysiere_Empfangenes gibt mittels der in der Umgebung geeignet vordefinierten Prozedur *output* die Informationseinheiten einzeln, d. h. nicht überlagert aus.

```
procedure Sende-_und_Empfangsprotokoll is
   s : puffer;   -- zu Sendendes
   r : puffer;   -- vom (rekursiven) Aufruf von Zugriff Empfangenes

   procedure Zugriff(Sendeerlaubnis : in BOOLEAN; e : out puffer) is
                                                  -- Empfangenes

      procedure Analysiere_Empfangenes(Sendeerlaubnis : in BOOLEAN; e : in puffer) is
         r : puffer;    -- durch rekursiven Aufruf von Zugriff Empfangenes
         m : BOOLEAN;     -- Ergebnis des Münzwurfs
      begin
         -- für |e| = 0 ist nichts zu tun
         if    |e| = 1  then       output(e);
         elsif |e| = 2  then       Zugriff(Sendeerlaubnis and e-s < s, r);
```

```
                    output(e-r);
                    -- Analysiere_Empfangenes(Sendeerlaubnis and not e-s < s, e-r);
                    -- hätte dieselbe Wirkung wie output(e-r);
        elsif  |e| > 2  then      m := Münze;
                    Zugriff(Sendeerlaubnis and m, r);
                    Analysiere_Empfangenes(Sendeerlaubnis and not m, e-r);
        end if;
      end Analysiere_Empfangenes;

    begin  -- Zugriff
      if   Sendeerlaubnis   then Sende(s);
      end if;
      Empfange(e);
      Analysiere_Empfangenes(Sendeerlaubnis, e);
    end Zugriff;

begin  -- Sende-_und_Empfangsprotokoll
    loop
      s := Sendewunsch;
      Zugriff(s ≠ 0, r);
    end loop;
end Sende-_und_Empfangsprotokoll;
```

In [Marc_88] wird gezeigt, daß mit diesem Mehrfachzugriffsverfahren unter den üblichen Annahmen [Mass_81] ein maximaler Durchsatz von mindestens 92,33% und höchstens 92,51% erreicht werden kann. Obiger Algorithmus ist auf leichte Verständlichkeit hin optimiert. Für eine praktische Nutzung wird man ihn so modifizieren, daß, wenn immer eine Informationseinheit berechnet werden kann, dies *sofort* geschieht, um die Verzögerungszeit möglichst gering zu halten. Die mittlere Verzögerungszeit dieses Mehrfachzugriffsverfahren ist in [Marc_88] genau untersucht.

Die in den beschriebenen Kollisionsauflösungsalgorithmen angegebenen Verbesserungen durch globales überlagerndes Empfangen und dadurch bedingtes Auslassen von Unterbäumen sowie deterministische Auflösung von Kollisionen von genau zwei Informationseinheiten können auch bei den ein klein wenig effizienteren, aber komplizierteren Kollisionsauflösungsalgorithmen [Mass_81, Gall_85, Li_87] angewendet werden. Mir ist allerdings unklar, ob dadurch ein höherer Durchsatz oder eine geringere (mittlere) Verzögerungszeit als der bzw. die des angegebenen Kollisionsauflösungsalgorithmus erzielt werden kann.

Nun bleibt noch zu untersuchen, ob die nutzbare Leistung (großer Durchsatz, geringe (mittlere) Verzögerungszeit) durch generelle und exakte Kenntnis der Anzahl kollidierter Informationseinheiten weiter gesteigert werden kann.

Die mittlere Verzögerungszeit kann bei genereller und exakter Kenntnis der Anzahl kollidierter Informationseinheiten gesenkt werden, indem nach einem Münzwurf immer mit der Teilmenge geringerer Kardinalität fortgefahren wird: Ist nach einem Münzwurf die Anzahl kollidierender Informationseinheiten größer als die Hälfte der vorher kollidierten, so invertieren alle Stationen lokal ihr Münzwurfergebnis und verwenden statt dem beobachteten Kollisionsergebnis die Differenz zwischen dem übergeordneten Kollisionsergebnis und dem beobachteten Kol-

lisionsergebnis. Da Informationseinheiten dadurch im Mittel früher empfangen werden können, sinkt dadurch die mittlere Verzögerungszeit. Der Durchsatz allerdings bleibt gleich.

Eine zur gerade beschriebenen Idee orthogonale zur Steigerung des Durchsatzes knüpft an folgender Beobachtung an: Der obige Kollisionsauflösungsalgorithmus verschwendet dann und nur dann Bandbreite, wenn bei einem Münzwurf alle dasselbe Münzwurfergebnis erhalten. Da immer mindestens 3 Stationen gleichzeitig ihre Münze werfen, ist die Wahrscheinlichkeit hierfür zwar immer ≤ 2/8. Die Wahrscheinlichkeit kann jedoch noch weiter gesenkt werden, wenn bei Münzwurf mit 3 (oder auch 4) Stationen im Mittel einer (oder auch zwei) Stationen erlaubt wird, sofort nach dem Münzwurf zusätzlich eine (neue) Informationseinheit zu senden. Hierbei wird vereinbart, daß jede neue Informationseinheit nicht mit dem 1 entsprechenden Zeichen beginnt, sondern bei einem Münzwurf mit *s* Stationen mit dem *s*+1 entsprechenden Zeichen. Dies deshalb, damit alle Empfänger aus dem Ergebnis *z* der Überlagerung der ersten Zeichen der nach dem Münzwurf gesendeten Informationseinheiten die Anzahl *t* der Stationen errechnen können, die TRUE gewürfelt haben, und ebenso die Anzahl *n* der Stationen, die eine neue Informationseinheit gesendet haben. Es gilt: $t = z \bmod s+1$ und $n = (z-t) / (s+1)$ immer, wenn $s+1 \leq m$ (wobei *m*, wie bereits definiert, die Anzahl Informationseinheiten ist, die eine Station maximal gleichzeitig senden darf), ansonsten mit hoher Wahrscheinlichkeit. Werfen alle ursprünglich beteiligten Stationen ihre Münze gleich, so können die zusätzlich gesendeten (neuen) Informationseinheiten, sofern es nicht mehr als 2 sind, deterministisch und ohne das Risiko der Bandbreitenverschwendung empfangen werden (ansonsten kann auch für sie eine indeterministische Kollisionsauflösung, ggf. unter nochmaliger Anwendung des gerade beschrieben Verfahrens des Zulassens der Übertragung neuer Informationseinheiten, erfolgen. Hierbei ist noch festzulegen, welche Kollisionsauflösung zuerst erfolgen soll. Um die zeitliche Reihenfolge ungefähr einzuhalten, schlage ich vor, die Auflösung der Kollision der neuen Informationseinheiten zurückzustellen). Werfen nicht alle ursprünglich beteiligten Stationen ihre Münze gleich, so können bei $s=3$ in beiden Teilmengen und bei $s=4$ mindestens in einer, mit der Wahrscheinlichkeit 6/14 sogar in beiden Teilmengen die Informationseinheiten deterministisch und ohne das Risiko der Bandbreitenverschwendung empfangen werden. (Bei $s=4$ kann das gerade beschriebene Verfahren ggf. nochmal angewendet werden.) Wurden beim Senden der ersten Teilmenge auch neue Informationseinheiten gesendet, so werden diese entweder zuerst empfangen und können dabei subtrahiert werden, oder aber sie werden später empfangen. Dann sendet die erste Teilmenge einfach noch einmal, wonach nicht nur die Summe ihrer Informationseinheiten, sondern auch die Summe der neuen Informationseinheiten global bekannt ist.

Die aus der beschriebene Idee resultierenden Kollisionsauflösungsalgorithmen sind noch nicht vollständig untersucht. Insbesondere ist festzulegen, für welche *s* das beschriebene Verfahren durchgeführt werden soll und wie in jedem dieser Fälle die Wahrscheinlichkeiten, daß eine, zwei, ... neue Informationseinheiten gesendet werden, gewählt werden sollen. Letzteres kann dadurch implementiert werden, daß jede Station, die eine Informationseinheit zu senden hat, eine Zufallsvariable mit passender Wahrscheinlichkeitsverteilung auswertet. Wie stark der Durchsatz mit diesem Verfahren gesteigert werden kann und wie es sich auf die Verzögerungszeiten auswirkt, ist mir unbekannt. Auch in dieser Richtung wären weitere Untersuchungen wünschenswert.

Bei dem beschriebenen Kollisionsauflösungsverfahren wird nach einem Münzwurf nicht primär versucht, eine Informationseinheit möglichst bald zu übertragen, sondern es wird gewis-

sermaßen mittels der Zulassung neuer Informationseinheiten „abgewartet“, wie das Ergebnis des Münzwurfs ist. Deshalb stellt das beschriebene Kollisionsauflösungsverfahren einen Übergang zu den im folgenden besprochenen Reservierungsschema dar.

In einem Gespräch über diese Kollisionsauflösungsalgorithmen schlug Klaus Echtle vor, die modulo-*g*-Addition des überlagernden Sendens zur (echten) Addition bis zum Wert *g*-1 zu verwenden, um mittels dieser Addition den abgerundeten Mittelwert $\lfloor Ø \rfloor$ aller an einer Kollision beteiligten Informationseinheiten zu berechnen. Statt eines Münzwurfergebnisses läßt jede Station die Größe ihrer Informationseinheit im Vergleich zu $\lfloor Ø \rfloor$ darüber entscheiden, wann sie nochmals sendet (**Mittelwertvergleich**). Damit es sich bei der modulo-*g*-Addition um eine (echte) Addition handelt, muß die Summe aller beteiligten Informationseinheiten kleiner *g* sein. Dies ist bei *s* Stationen, von denen jede maximal *m* Informationseinheiten gleichzeitig senden darf, und einer maximalen Größe *G* (im Sinne der Interpretation der Binärcodierung der Informationseinheiten als Dualzahl) von Informationseinheiten mit Sicherheit immer dann der Fall, wenn $g > s \cdot m \cdot G$. Klaus Echtle versprach sich davon eine Verbesserung der mittleren Balanciertheit des bei der Kollisionsauflösung entstehenden Binärbaumes, vgl. die Bilder 31, 32 und 33. Im Fortgang des Gespräches wurde auf der Basis meiner oben beschriebenen Analyse der Bandbreitenverschwendung gemeinsam herausgearbeitet, daß die mittlere Balanciertheit gar nicht der eigentlich wesentliche Punkt ist: Der wesentliche Punkt ist, daß – sofern nicht alle kollidierten Informationseinheiten gleich sind – es immer mindestens eine kleiner und eine größer als $\lfloor Ø \rfloor$ gibt. Da dann nie alle dasselbe „Münzwurfergebnis“ erhalten und entsprechend nie sofort alle noch mal oder keiner sofort noch mal sendet, wird keinerlei Bandbreite verschwendet.

Dies ist in Bild 34 am in den Bildern 31, 32 und 33 verwendeten Beispiel veranschaulicht. Bild 35 zeigt ein passendes Nachrichtenformat für eine sendende Station. Bei einer nicht sendenden Station sind alle Bits der Nachricht, auch das letzte, 0. Die führenden Nullen in Bild 35 sind nötig, um einen Überlauf bei der Addition zu verhindern. Bild 36 zeigt ein detaillierteres Beispiel mit dem in Bild 35 angegebenen Nachrichtenformat. Weder in Bild 35 noch in Bild 36 noch im folgenden Text ist dargestellt, daß bei Verwendung dieses Mehrfachzugriffsverfahrens im DC-Netz zusätzlich noch paarweise ausgetauschte Schlüssel überlagert werden. Da deshalb die führenden Nullen im allgemeinen nicht als Nullen übertragen werden, müssen die ihnen entsprechenden Zeichen tatsächlich übertragen werden.

Im Nachrichtenformat kann die Anzahl der führenden Nullen während der Ausführung des Kollisionsauflösungsalgorithmus gesenkt werden, wenn jeweils nur noch genügend wenig Informationseinheiten überlagert gesendet werden. Diese dynamische Verkleinerung spart zwar Übertragungsaufwand bzw. erlaubt bei gegebener Übertragungsrate einen höheren Durchsatz. Es ist jedoch für jede Implementierung abzuwägen, ob sich der Aufwand für diese dynamische Anpassung des Nachrichtenformates und der zur Überlagerung verwendeten zyklischen Gruppe lohnt.

Von eher theoretischem Interesse ist, daß bei Mittelwertvergleich nicht nur „Determinismus“ mit exponentiell kleiner Mißerfolgswahrscheinlichkeit erzielt werden kann, sondern sogar **„echter“ Determinismus**: wird nach einer Überlagerungs-Kollision im nächsten Schritt nichts oder dasselbe nochmal übertragen, so sind alle kollidierten Informationseinheiten gleich. Da die Zahl der kollidierten Informationseinheiten schon für die Mittelwertbildung allen bekannt

sein muß (etwa durch das früher bereits erwähnte Aufaddieren der der 1 entsprechenden Zeichen), können alle das vorherige gespeicherte Kollisionsergebnis durch die Zahl der kollidierten Informationseinheiten teilen und die resultierende Informationseinheit entsprechend oft empfangen.

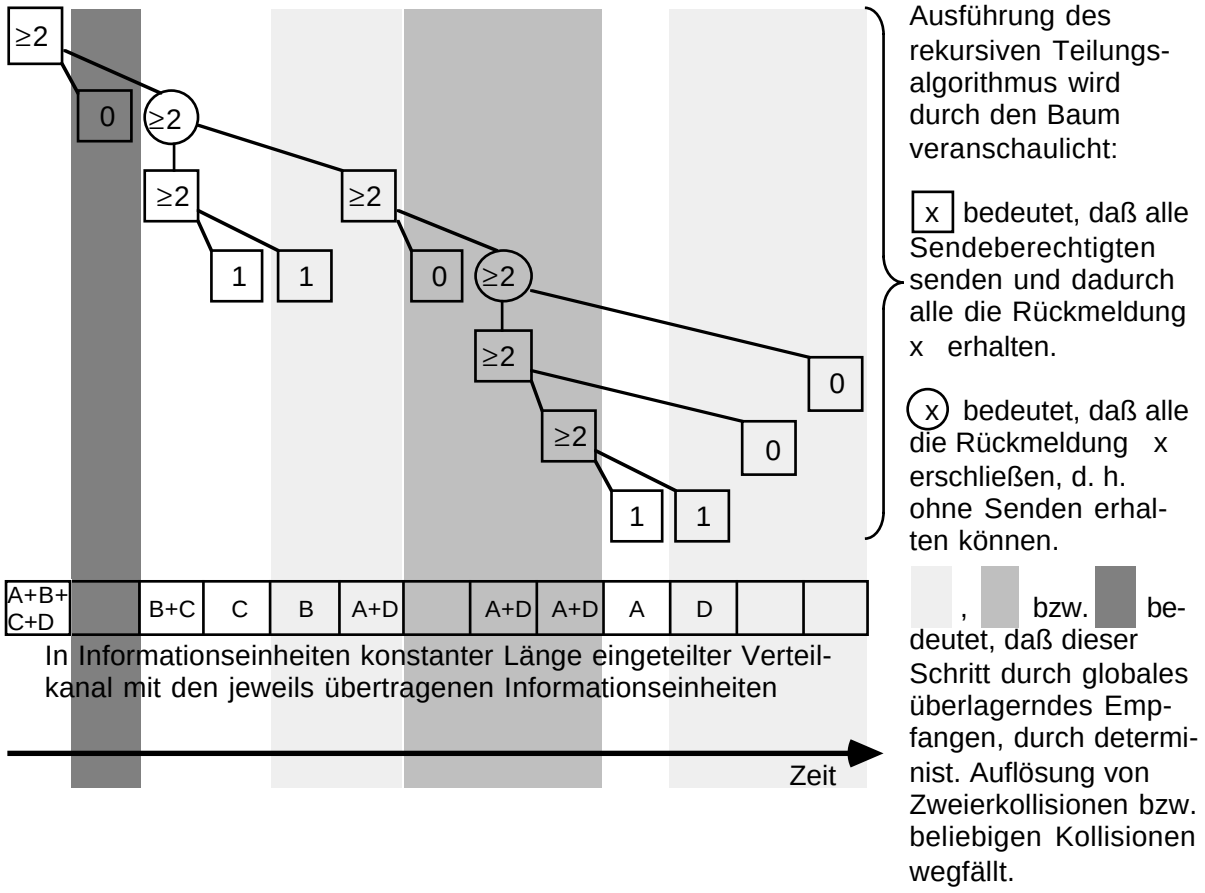


Bild 34: Eine Möglichkeit der Auflösung einer Kollision von 4 Informationseinheiten A, B, C und D mit dem von Massey beschriebenen einfachen Kollisionsauflösungsalgorithmus, deterministischer Auflösung von Kollisionen und globalem überlagerndem Empfangen

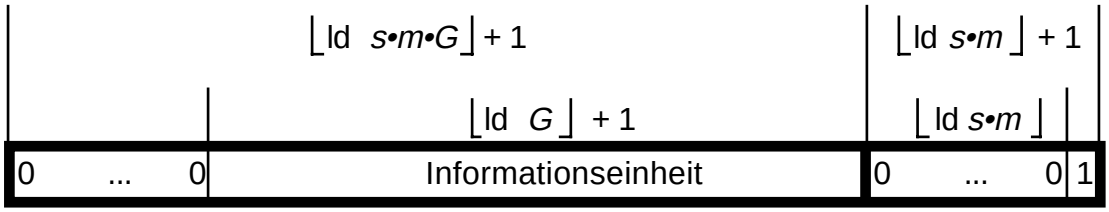
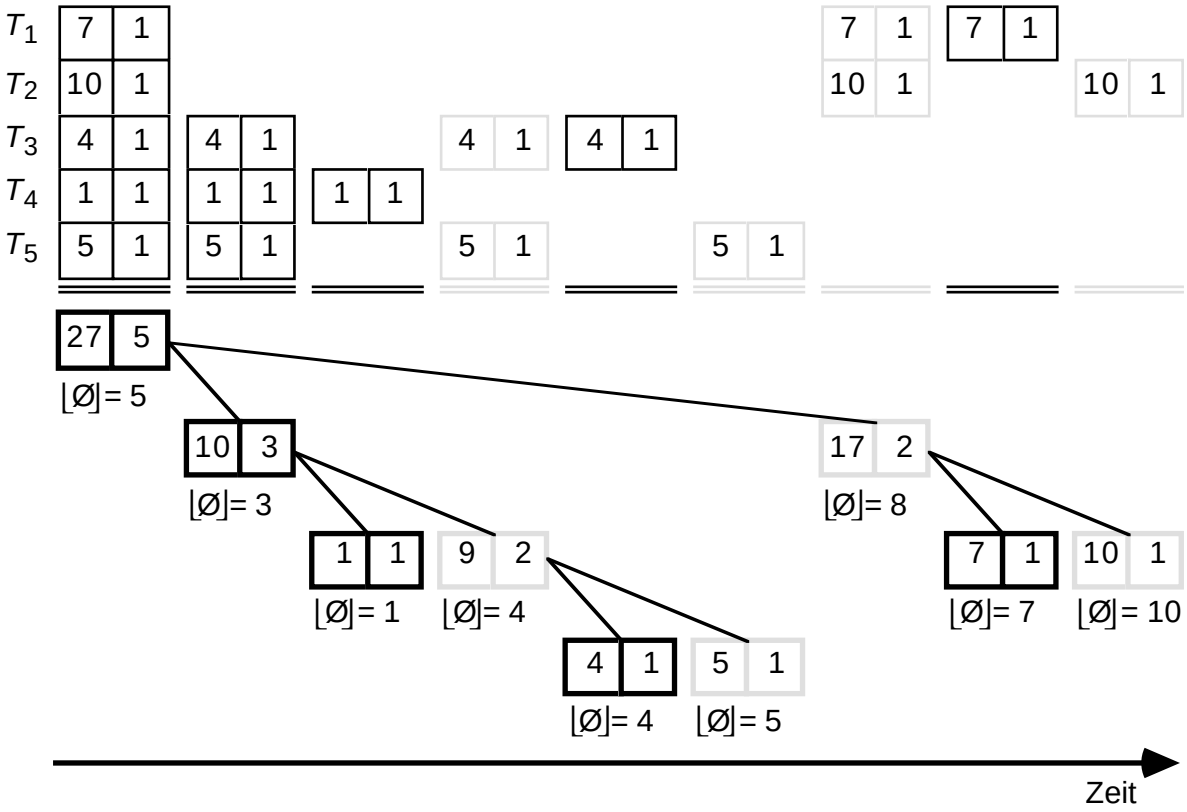


Bild 35: Nachrichtenformat für Kollisionsauflösungsalgorithmus mit Mittelwertbildung und überlagerndem Empfangen



Oben ist zeilenweise dargestellt, was die Teilnehmerstationen T_1 bis T_5 senden,
unten jeweils das globale Überlagerungsergebnis, die Summe.
Gilt für eine Station *Informationseinheit* $\leq \lfloor \varnothing \rfloor$, so sendet sie sofort wieder, anderenfalls später.
Das globale überlagernde Empfangen ist durch graue Quadrate symbolisiert.

Bild 36: Detailliertes Beispiel zum Kollisionsauflösungsalgorithmus mit Mittelwertbildung und überlagerndem Empfangen

Unter den üblichen (idealisierenden) Annahmen erzielt dieses Mehrfachzugriffsverfahren also einen Durchsatz von 100%.

Bei Verwendung eines genügend großen Alphabets und des gerade beschriebenen Mittelwertvergleichs kann ein realer Durchsatz von nahezu 100% erzielt werden. Bei binärer Codierung ist der Durchsatz des Mehrfachzugriffsverfahrens

$$\frac{\text{Anzahl der zur Codierung der Informationseinheiten nötigen Bits}}{\text{Anzahl aller zu übertragenden Bits}} \cdot 100\%.$$

Ist die Codierung der Informationseinheiten redundant, so geht der daraus resultierende Verlust an Durchsatz zu Lasten der Quellcodierung oder der binären Kanalcodierung, jedoch nicht zu Lasten des Mehrfachzugriffsverfahrens. Denn dies schränkt die Codierung der Informationseinheiten in keiner Weise ein.

Bei feldweiser binärer Codierung gemäß Bild 35 ist der reale Durchsatz des Mehrfachzugriffsverfahrens also mindestens

$$\frac{\lfloor \mathrm{ld}\ G \rfloor + 1}{\lfloor \mathrm{ld}\ s \bullet m \bullet G \rfloor + \lfloor \mathrm{ld}\ s \bullet m \rfloor + 2} \bullet 100\%,$$

da bei binärer Codierung der ganzen Zahlen des geschlossenen Intervalls $[0, x]$ genau $\lfloor \mathrm{ld}\ x \rfloor + 1$ Bits benötigt werden. Hierbei bezeichnet ld (logarithmus dualis) den Logarithmus zur Basis 2 und $\lfloor y \rfloor$ die größte ganze Zahl z mit $z \leq y$.

Außerdem ist garantiert, daß jede Station in $s \bullet m$ zur Übertragung einer Informationseinheit benötigten Zeiteinheiten m Informationseinheiten übertragen kann: Jeder Station ist also, sofern sie etwas zu senden hat, ein fairer Anteil an der Bandbreite des DC-Netzes ebenso „echt“ deterministisch garantiert wie eine obere Schranke, nach der sie spätestens erfolgreich senden konnte. Andererseits kann eine einzelne Station, wenn die anderen nichts zu senden haben, die Bandbreite des DC-Netzes vollständig nutzen.

Die bereits beschriebene Verbesserung der mittleren Verzögerungszeit, indem immer mit der Teilmenge geringerer Kardinalität fortgefahren wird, kann und sollte mit dem Mittelwertvergleich kombiniert werden.

Die mittlere Verzögerungszeit dieses Mehrfachzugriffsverfahren ist in [Marc_88] genau untersucht.

Ist einem die zur Erfüllung der Bedingung $g > s \bullet m \bullet G$ nötige Alphabetgröße zu groß, so kann bei großem $s \bullet m$ statt $s \bullet m$ in der Ungleichung ein kleinerer Wert k, beispielsweise k=10, verwendet werden. Die Mittelwertaussage ist dann für Kollisionen von mehr als k Informationseinheiten möglicherweise falsch. Ist k geeignet gewählt, so treten die Bandbreite verschwendenden Fälle, daß der falsche, nämlich modulo g berechnete, Mittelwert kleiner oder größer als alle beteiligten Informationseinheiten ist, selten genug auf. Sie sind von allen Beteiligten erkennbar und werden durch Münzwurf aufgelöst.

Eine andere Möglichkeit zur Verwendung einer kleineren Alphabetgröße ist, den Mittelwertvergleich nicht auf ganze Informationseinheiten, sondern nur Teile (etwa den Anfang) zu erstrecken. Hierdurch steigt allerdings die Wahrscheinlichkeit, daß alle an einer Kollision beteiligten Informationseinheiten jeweils gleiche Teile, beispielsweise Anfänge, haben. Haben die verwendeten Teile jeweils mindestens 20 Bit Länge und sind die Werte auch nur näherungsweise gleichverteilt (etwa implizite Adressen oder Ende-zu-Ende-verschlüsselte Teile), so dürfte diese Wahrscheinlichkeit aber hinreichend klein sein, um die nutzbare Leistung nur unmerklich zu senken.

In beiden Fällen ist der Verlust des „echten“ Determinismus der Preis für die kleinere Alphabetgröße.

Der **Kollisionsauflösungsalgorithmus mit Mittelwertbildung und überlagerndem Empfangen** ist, sieht man vom (allerdings geringen, vgl. Abschnitt 3.2.3) Aufwand der Realisierung eines sehr großen Alphabets und vom Aufwand für das globale überlagernde Empfangen ab, das in jeder Hinsicht **optimale Mehrfachzugriffsverfahren für das DC-Netz** – es sei denn paarweises überlagerndes Empfangen oder Konferenzschaltung sind möglich, vgl. die folgenden Abschnitte 3.1.2.5 und 3.1.2.6.

Jedes für überlagerndes Senden mit großem Alphabet geeignete Kommunikationsnetz arbeitet mit diesem (und ggf. weiteren) Mehrfachzugriffsverfahren für so viele Dienste so effizient, daß sein Einsatz zumindest im lokalen Bereich auch für Zwecke, bei denen es nicht auf Senderanonymität ankommt, zweckmäßig erscheint – Schlüsselerzeugung und synchronisierte Überlagerung können dann natürlich weggelassen werden, vgl. Abschnitt 9.4.

3.1.2.3.3 Direkte Übertragung, bei Kollision nochmaliges Senden nach zufälliger, aber angekündigter Zeitdauer (ARRA)

In [Rayc_85] sind zwei Mehrfachzugriffsprotokolle dieser Klasse detailliert beschrieben und analysiert. Das mit dem größeren Durchsatz (extended ARRA = extended announced retransmission random access) erreicht einen von 60%. Es kann zwar noch leicht verbessert werden, indem, statt allen, die für denselben Zeitpunkt nochmaliges Senden angekündigt haben, dieses zu verbieten (und von allen nochmal eine Ankündigung zu fordern), es genau einer Station, etwa der, deren Ankündigung im Nachrichtenzeitschlitz (message slot) mit der kleinsten Nummer erfolgte, das Senden erlaubt wird, doch dürfte diese Verbesserung die Leistung nur um wenige Promille steigern.

In [Pfi1_85 Seite 41] steht erstmals, daß Mehrfachzugriffsprotokolle dieser Klasse für anonymen und unverkettenden Mehrfachzugriff geeignet sind, und wie sie in der rein digitalen Welt des überlagernden Sendens bei binärem überlagernden Senden leider nur mäßig gut, bei verallgemeinertem überlagernden Senden perfekt implementiert werden können.

Leider ist die Situation bei dieser Reaktionsart auf Kollisionen für globales überlagerndes Empfangen fast genauso schlecht wie bei nochmaligem Senden nach zufälliger Zeitdauer (slotted ALOHA): Die an einer Kollision beteiligten Informationseinheiten lassen sich nicht „verfolgen“, wenn ihrem angekündigten nochmaligen Sendezeitpunkt nicht entsprochen werden kann (etwa weil viele denselben wählten). Dies ist bei Kollisionsauflösung bei weitem besser, so daß sich durch sie die weit höhere nutzbare Leistung erzielen läßt. Anders herum gesagt: durch die Erfindung des globalen überlagernden Empfangens wurde diese Klasse, die vorher der Klasse Kollisionsauflösung überlegen war, ihr unterlegen, weshalb sie hier nicht vertieft behandelt wird.

3.1.2.3.4 Direkte Übertragung, bei Erfolg Reservierung (R-ALOHA)

Diese in [Tane_81 Seite 272, Tasa_83] und für anonyme Kommunikation erstmals in [Pfi1_85 Seite 40] erwähnte Klasse von Mehrfachzugriffsprotokollen verkettet natürlich alle Informationseinheiten, die hintereinander übertragen werden. Wie bereits erwähnt ist dies für manche Dienste jedoch akzeptabel. Es erlaubt je nach ihrer Verkehrscharakteristik einen Durchsatz bis nahe 100%, wobei es bei wenigen hintereinander übertragenen Informationseinheiten günstig ist, in ihnen ein Bit vorzusehen, das anzeigt, daß dies die letzte „reservierte“ Informationseinheit ist, während es bei vielen Informationseinheiten günstiger ist, dies Bit in jeder Informationseinheit einzusparen und dafür am Schluß eine leere Informationseinheit zu übertragen.

3.1.2.3.5 Reservierungsschema (Roberts' scheme)

Wie bereits in Abschnitt 2.5.3.1.1 erwähnt, wurde die Verwendung dieses Anonymität perfekt erhaltende Mehrfachzugriffsverfahrens, mit dem ein Durchsatz von nahe 100% erzielt werden kann [Tane_81 Seite 272], bereits in [Cha3_85] mit der folgenden Implementierung in der digitalen Welt des binären überlagernden Sendens vorgeschlagen:

> Die Bandbreite wird in Rahmen (frames) eingeteilt, deren Länge zwischen einem minimalen und maximalen Wert liegt. Um die Sprechweise der folgenden Funktionsbeschreibungen zu vereinfachen, bezeichne „der nächste" Rahmen nicht den physisch folgenden, sondern den *n*-ten der physisch folgenden, wobei *n* fest und minimal so gewählt wird, daß vor dessen Senden alle Stationen das Überlagerungsergebnis des „vorherigen" Rahmens (auch bei Rahmen minimaler Länge dazwischen) so rechtzeitig erhalten haben, daß sie zum Ausführen des Mehrfachzugriffsverfahrens in der Lage sind. Jeder Rahmen beginnt mit einem Datenübertragungsteil variabler Länge und endet mit einem Reservierungsteil fester Länge. Das Überlagerungsergebnis des Reservierungsteils eines Rahmens bestimmt die Länge des Datenübertragungsteils des nächsten Rahmens, indem in ihm für jede signalisierte Reservierung Platz (genauer: Zeit) für eine Informationseinheit vorgesehen wird, in der exklusiv diejenige Station senden darf, die diese Reservierung tätigte. Wird in einem Rahmen keine Reservierung getätigt, ist der Datenübertragungsteil des nächsten Rahmens leer. In [Cha3_85, Chau_88] schlägt David Chaum vor, den Reservierungsteil als eine Bitleiste aufzufassen, wobei jede 1 einer Reservierung entspricht. Der Datenübertragungsteil kann also maximal soviele Informationseinheiten enthalten, wie der Reservierungsteil Bits enthält. Um eine (oder mehrere) Reservierungen zu tätigen, sendet eine Station eine (oder mehrere) 1 an zufälligen Stellen des Reservierungsteils. Ist das Überlagerungsergebnis an einer (oder mehreren) dieser Stellen 1, so sendet sie in den entsprechenden Stellen (genauer: Zeiten) des Datenübertragungsteils des nächsten Rahmens.

Leider ist nun nicht garantiert, daß es keine Kollision gibt: haben 3, 5, 7, ... Stationen an dieser Stelle reserviert, so gehen alle davon aus, daß nur sie an der entsprechenden Stelle des nächsten Rahmens senden. Die Wahrscheinlichkeit dieses Trugschlusses ist bei binärem überlagernden Senden nicht auf 0 zu senken, kann jedoch erheblich verkleinert werden, indem jeweils x Bits für jede Reservierung verwendet werden, von den jeweils y ($y<x$) als 1 gesendet werden, um eine Reservierung zu signalisieren. Durch geeignete Wahl von x und y kann zwar die Wahrscheinlichkeit, daß eine Kollision bei der Reservierung nicht erkannt wird, beliebig gesenkt werden, allerdings werden zur Reservierung auch x mal soviele Bits verwendet. Zu gegebener Verkehrsverteilung die optimalen Werte für x und y zu finden, ist eine lohnende Aufgabe.

Stattdessen sei hier noch einmal darauf hingewiesen, daß verallgemeinertes überlagerndes Senden mit $g > s \bullet m$ dazu verwendet werden kann, die Wahrscheinlichkeit von Kollisionen bei der Übertragung von Informationseinheiten auf 0 zu senken, wie vor der Beschreibung der einzelnen Mehrfachzugriffsverfahrensklassen erklärt wurde. Dieses in Bild 37 dargestellte Mehrfachzugriffsverfahren ist die älteste Anwendung von verallgemeinertem überlagerndem Senden [Pfi1_85 Seite 40].

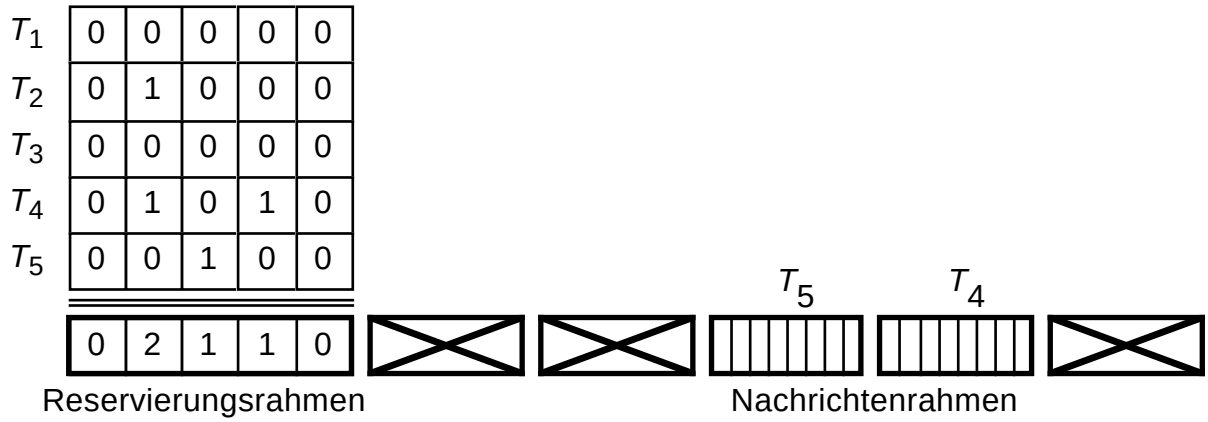


Bild 37: Reservierungsschema mit verallgemeinertem überlagerndem Senden und den Teilnehmerstationen T_i

Eine Kombination dieser Reservierungsverfahren mit überlagerndem Empfangen erscheint weitgehend unnötig. Lediglich im Falle, daß bei verallgemeinertem überlagernden Senden eine Reservierung den Wert 2 ergibt, kann ohne Einbuße an Durchsatz, aber mit Verringerung der durchschnittlichen Wartezeit bis zur erfolgreichen Übertragung vereinbart werden, daß an der entsprechenden Stelle des nächsten Rahmens beide ihre Informationseinheit senden, im übernächsten dann nur noch derjenige, der die größere Informationseinheit gesendet hat. Dies ist genau das bereits früher beschriebene Verfahren der deterministischen Kollisionsauflösung bei Kollision von zwei Informationseinheiten.

3.1.2.3.6 Verfahren für einen Kanal mit kurzer Verzögerungszeit

Alle Mehrfachzugriffsverfahren mit direkter Übertragung können bei einem Kanal mit kurzer Verzögerungszeit in natürlicher Weise um die Regel erweitert werden, daß nur gesendet werden darf, wenn auf dem Kanal gerade keine Übertragung stattfindet (CSMA = carrier sense multiple access). Damit sich auch hier wiederum alle Stationen gleich verhalten, sollten für die Zwecke des Mehrfachzugriffsprotokolls alle das Überlagerungsergebnis nach derselben Zeit berücksichtigen, was natürlich nicht voraussetzt, daß alle das Überlagerungsergebnis nach derselben Zeit erhalten: die Ausgabe von Zeichen *i* aller Stationen berücksichtigt nur das Überlagerungsergebnis aller Zeichen bis *i-j*, wobei *j* so gewählt wird, daß alle Stationen das Überlagerungsergebnis der Zeichen *i-j* rechtzeitig erhalten [Pfi1_85 Seite 42].

Bezüglich Anonymitäts- und Unverkettbarkeitserhaltung ist es gleichgültig, ob eine Station, die Senden will und auf dem Kanal eine Übertragung hört, bis zum Ende der Übertragung wartet und dann deterministisch sofort sendet (1-persistent CSMA [Tane_81 Seite 290]), nur mit der Wahrscheinlichkeit p sofort sendet (p-persistent CSMA) oder es erst nach einer zufälligen Zeitdauer noch einmal versucht (nonpersistent CSMA).

Ebenso ist es bezüglich Anonymitäts- und Unverkettbarkeitserhaltung gleichgültig, ob eine Station, die sendet und dabei eine Kollision erkennt, ihr Senden abbricht (CSMA/CD = carrier

sense multiple access / collision detection) oder nicht. Nicht gleichgültig ist dies natürlich bezüglich der nutzbaren Leistung, da einerseits CSMA/CD, wenn der Abbruch relativ früh innerhalb von Informationseinheiten erfolgt, die nutzbare Leistung in einem Kommunikationsnetz ohne überlagerndes Empfangen erheblich steigert, andererseits natürlich überlagerndes Empfangen unmöglich macht und damit für große *j* ein Umschlüsseln kollidierter Informationseinheiten zum Zwecke der Unverkettbarkeit erfordert. Wie in [Pfi1_85 Seite 43] beschrieben, sollte ein Abbrechen des Sendens beim Erkennen einer Kollision in der Form erfolgen, daß die Station das 0 entsprechende Zeichen sendet, solange nicht alle anderen ihr Senden auch abgebrochen haben. Dies ist anders als in der analogen Welt, beispielsweise Ethernet [Tane_81 Seite 293], wo jede Station, die eine Kollision erkennt, den Kanal kurzzeitig bewußt stört (jamming), damit alle Stationen konsistent erfahren, daß eine Kollision stattfand. In der digitalen Welt ist dies nicht nötig, da erstens die Sicht aller Stationen bezüglich des Überlagerungsergebnisses konsistent ist (während das auf einem analogen Bus Empfangbare durchaus von der Anschlußstelle abhängen kann) und zweitens Ende-zu-Ende-Verschlüsselung und implizite Adressierung als fehlererkennender Code wirken. Für die nutzbare Leistung wirkt sich der Verzicht auf bewußte Störung doppelt positiv aus: Erstens wird die Störzeit eingespart. Zweitens kann sich bei einer Kollision eine Station durchsetzen, d. h. sie bemerkt gar nicht, daß auch andere etwas gesendet haben, sich dies aber gegenseitig aufhob.

Natürlich sind vielerlei Kombinationen denkbar, von denen ich nur eine zur *deterministischen Auflösung von Kollisionen von 2, 3, 5, 7, 9, 11, ... Informationseinheiten bei einem binären Überlagerungskanal optimal kurzer Verzögerungszeit* (*j*=1) beschreiben will:

Wie schon früher beschrieben, beginne jede Informationseinheit mit dem 1 entsprechenden Zeichen, das bei binärem überlagerndem Senden zur probabilistischen Bestimmung der Anzahl der kollidierenden Informationseinheiten benutzt wird.

Ergibt die Überlagerung dieses Zeichens das 0 entsprechende, so gehen alle Stationen, die gesendet haben, davon aus, daß es sich um eine Zweierkollision handelt und überlagern ihre Informationseinheiten vollständig (und diejenige mit der größeren Informationseinheit sendet ihre direkt danach noch mal, so daß beide überlagernd empfangen werden können).

Ergibt die Überlagerung dieses Zeichens 1, so wissen alle Stationen, daß es sich entweder um keine oder um eine ungeradzahlige Kollision handelt. Sie senden ihr erstes Informationsbit und brechen ihr Senden sofort ab, falls das Überlagerungsergebnis nicht ihrem Informationsbit entspricht. Die Ungeradzahligkeit garantiert, daß sich immer genau eine Station durchsetzt: Senden alle dasselbe Zeichen, ist das Überlagerungsergebnis dies Zeichen und keine der ungeradzahlig vielen Stationen bricht ihr Senden ab. Senden nicht alle dasselbe Zeichen, so ist das Überlagerungsergebnis das von der Gruppe mit ungeradzahliger Anzahl gesendete Zeichen. Deshalb hört eine geradzahlige Anzahl Stationen auf zu senden, so daß danach wieder eine ungeradzahlige Anzahl sendet.

3.1.2.4 Eignung für das Senden von Paketen, Nachrichten und kontinuierlichen Informationsströmen (Kanäle)

In diesem Abschnitt wird die Eignung der die Anonymität des Senders erhaltenden und Verkehrsereignisse nicht verkettenden Mehrfachzugriffsverfahren für das Senden von Paketen, Nachrichten und kontinuierlichen Informationsströmen (Kanäle) diskutiert.

Außer den Verfahrensklassen „bei Erfolg Reservierung“ sind alle beschriebenen Klassen von Mehrfachzugriffsverfahren (inkl. der beschriebenen Beispielverfahren) für das Senden von Paketen geeignet.

Die Verfahrensklassen „bei Erfolg Reservierung“ sind sowohl zur Übertragung von Nachrichten mittels ggf. mehrerer Pakete als auch zur dezentralen Belegung von Kanälen geeignet. Das gleiche gilt für eine geeignete Anpassung des „Reservierungsschemas“.

Die Klassen „nochmaliges Senden nach zufälliger Zeitdauer (CSMA)“ und „Abbruch und nochmaliges Senden nach zufälliger Zeitdauer (CSMA/CD)“ sind auch für die direkte, d. h. nicht in Pakete zerlegte Übertragung von Nachrichten geeignet.

3.1.2.5 Einsatz von paarweisem überlagernden Empfangen

Paarweises überlagerndes Empfangen ist genau dann sinnvoll möglich, wenn

1. beide Partner jeweils exakt gleichzeitig senden können, d. h. sich beide darüber verständigt haben, wann sie senden werden, und
2. dies nach dem jeweiligen Mehrfachzugriffsverfahren erlaubt ist.

Es ist sehr sinnvoll, wenn zusätzlich

3. allen anderen mitgeteilt wurde, wann die beiden Partner senden werden.

Um 2. zu erfüllen, müßten beispielsweise bei einem Kollisionsauflösungsalgorithmus die anderen Beteiligten die beiden paarweise überlagerten Informationseinheiten als eine betrachten oder zumindest behandeln.

Bei mittels nichtlinearem Prüfzeichen realisierter ternärer Rückmeldung ist dies nicht ohne weiteres, d. h. ohne Abänderung des Kollisionsauflösungsalgorithmus, möglich. Jedoch kann auf die ansonsten zweckmäßige Eigenschaft, daß die Redundanz zur Erkennung von Kollisionen ein Prüfzeichen zum Nachrichteninhalt darstellt, verzichtet werden, und irgendein (separater) nichtlinearer Code verwendet werden, z. B. ein *m*-aus-*n*-Code.

Bei exakter oder probabilistischer Kenntnis der Anzahl der kollidierten Informationseinheiten durch Verwendung eines großen Alphabets zum überlagernden Senden und die Vereinbarung, daß jede Informationseinheit mit dem 1 entsprechenden Zeichen beginnt, ist dies sehr einfach möglich: genau einer der beiden am paarweise überlagernden Empfangen Beteiligten läßt seine Informationseinheit jeweils mit dem 0 entsprechenden Zeichen beginnen.

Aus dem Gesagten folgt, daß paarweises überlagerndes Empfangen vor allem bei kontinuierlichen Informationsströmen (Kanälen) sinnvoll eingesetzt werden kann. Benötigen beide am paarweise überlagernden Empfangen beteiligten Partner für exklusiv für den anderen bestimmte Information insgesamt einen Duplex-Kanal, so wird – wie in Abschnitt 2.5.3.1.3 bereits erwähnt, durch das paarweise überlagernde Empfangen die Bandbreite des DC-Netzes doppelt so gut genutzt.

3.1.2.6 (Anonyme) Konferenzschaltungen

Zunächst ist zu erörtern, was genau unter einer Konferenzschaltung verstanden wird.

Wird unter einer Konferenzschaltung verstanden, daß eine Gruppe von Teilnehmerstationen jeweils separat erhält, was die anderen Mitglieder der Gruppe senden, so daß jedes Gruppenmitglied selektiv das Gesendete jeder beliebigen Teilmenge der Gruppe gleichzeitig wahrnehmen kann, so eröffnet das überlagernde Senden keine Möglichkeiten zur effizienten Nutzung, die nicht jedes Verteilnetz bietet: Jedes Mitglied der Gruppe sendet separat und verschlüsselt dabei mit einem jeweils allen anderen bekannten Schlüssel, so daß jede Informationseinheit nur einmal gesendet zu werden braucht.

Wird unter einer Konferenzschaltung einschränkend verstanden, daß eine Gruppe von Teilnehmern gleichzeitig wahrnehmen kann, was die anderen insgesamt senden, so eröffnet das überlagernde Senden Möglichkeiten zur effizienten Nutzung, die nicht jedes Verteilnetz bietet. Dabei sollte beachtet werden, daß Teilnehmerstationen in Abhängigkeit der Teilnehmerzahl einen Schwellwert für die Lautstärke ihres Sprechers festlegen sollten, unterhalb dessen sie das 0 entsprechende Signal übertragen, damit sich das Rauschen der Mikrophone oder Nebengeräusche nicht unnötig aufaddieren und damit ab einer gewissen Teilnehmerzahl stören. Zunächst wird eine Möglichkeit beschrieben, die ohne zusätzliche Annahmen auskommt. Danach eine effizientere, die jedoch nur dann angewendet werden kann, wenn zum überlagernden Senden ein großes Alphabet verwendet wird.

Bei der ersten Möglichkeit fungiert eine der Teilnehmerstationen als *Zentrale*. Zwischen ihr und allen anderen Gruppenmitgliedern jeweils einzeln kann – wie oben beschrieben – paarweises überlagerndes Empfangen praktiziert werden. Die Zentrale (entschlüsselt und) bildet das Summensignal aus allen erhaltenen Signalen und ihrem eigenen (verschlüsselt) und verteilt es. Werden beispielsweise Kanäle geschaltet, so ist eine (anonyme) Konferenzschaltung zwischen n Teilnehmern auf diese Weise in n-1 statt n Kanälen möglich. Der „Preis“ für die Einsparung eines Kanals ist, daß die Verzögerungszeit verdoppelt wird.

Bei der zweiten Möglichkeit erfolgt die Bildung des Summensignals „*dezentral*“, nämlich durch die zum Zwecke der Senderanonymität angewendete Überlagerung. Hierzu muß die Zeichenanzahl des zur Überlagerung verwendeten Alphabetes mindestens so groß wie die Anzahl der Quantisierungsschritte des Konferenzsignals sein. Dem Signalwert 0 muß das 0 entsprechende Zeichen zugeordnet werden, die Signalcodierung muß linear erfolgen und ebenso dürfen die Signalcodes nicht in nichtlinearer Weise (Ende-zu-Ende-)verschlüsselt werden. Ende-zu-Ende-Verschlüsselung kann beispielweise in der Form erfolgen, daß jede der Teilnehmerstationen ihren Signalcode mit einem den anderen bekannten Schlüssel überlagert und alle Teilnehmerstationen diese Schlüssel vom globalen Überlagerungsergebnis subtrahieren und so den Signalcode des Summensignals erhalten. Möchten die Teilnehmer ihr eigenes „Echo“ nicht wahrnehmen, so brauchen ihre Teilnehmerstationen nur vom Signalcode des Summensignals ihren Signalcode zu subtrahieren. Werden beispielsweise Kanäle geschaltet, so ist eine (anonyme) Konferenzschaltung zwischen n Teilnehmern auf diese Weise in einem statt n Kanälen möglich. Es kann sinnvoll sein, diesen einen (Summen-)Kanal mit einem etwas größeren Amplitudenbereich des Signals und bei der notwendigen linearen Signalcodierung auch entsprechend größerer Bandbreite vorzusehen. Dann können auch wenige Signale großer Amplitude störungsfrei überlagert werden – anderenfalls ergäbe beispielsweise die Summe aus einem

maximal und einem minimal positiven Signalwert den betragsmässig maximal negativen Signalwert. Allerdings wird zumindest für größere *n* im (Summen-)Kanal nicht die *n*-fache Bandbreite benötigt, da etwa bei drei gleichlaut Redenden der Zuhörer sowieso nichts mehr versteht.

(Nach dem Schreiben dieses Unterabschnitts erschien [BrLY_88]. E. F. Brickell, P. J. Lee und Y. Yacobi untersuchen für ein *Vermittlungsnetz* Techniken für eine Konferenzschaltung. Eine „bridge“ genannte (Vermittlungs-)Zentrale führt bei ihnen im wesentlichen das oben beschriebene, „dezentrale“ Verfahren durch. Da ihrer (Vermittlungs-)Zentrale mitgeteilt wird, welche Konferenzteilnehmer gerade senden, kann ihre (Vermittlungs-)Zentrale die Signale der anderen unterdrücken, d. h. nicht aufaddieren, um Rauschen zu vermeiden, bzw., falls zu viele senden, wenige auswählen, um Unverständlichkeit für den menschlichen Hörer oder Übersteuerung zu vermeiden. Dadurch erhält ihre (Vermittlungs-)Zentrale aber in meinen Augen sensitive Information, was bei den oben beschriebenen, für das DC-Netz entworfenen aber auch auf einem Vermittlungsnetz möglichen – die (Vermittlungs-)Zentrale müßte global überlagern – Verfahren vermieden wird.)

3.1.2.7 Resümee

Da kein Mehrfachzugriffsverfahren für alle möglichen Kommunikationsdienste optimal ist, sollte die Bandbreite des DC-Netzes (ggf. dynamisch) in Kanäle im Sinne von Abschnitt 3.1.1 eingeteilt und diese Kanäle jeweils mit einem passenden Mehrfachzugriffsverfahren (oder ggf. von einer ausgewählten Station) verwaltet werden.

3.1.3 Mehrfachzugriff beim BAUM-Netz auch für Kanäle

Die Bandbreite des BAUM-Netzes sollte von einer ausgezeichneten Station – etwa der Wurzel des Baumes – in Abhängigkeit des Verkehrs in einen Bereich für Nachrichten (Pakete sind beim BAUM-Netz ein uninteressanter, weil keine substantiellen Optimierungen ermöglichender Spezialfall von Nachrichten) und einen für Kanäle unterteilt werden.

Gibt die Station auch die Aufteilung in einzelne Kanäle vor, so ist der Zugriff auf sie trivial, nämlich genau wie für Nachrichten beschrieben. Anderenfalls sollten Kanäle unter Angabe der gewünschten Bandbreite bei ihr mittels Nachrichten angefordert werden.

3.1.4 Mehrfachzugriff beim RING-Netz

Wie in Abschnitt 2.5.3.2.1 schon erwähnt, sollte zur effizienten Nutzung des Verteil-Kanals „Ring“ ein Verfahren zum (hoffentlich!) Anonymität und Unverkettbarkeit erhaltenden Mehrfachzugriff, genannt Ringzugriffsverfahren, verwendet werden. Dadurch hat der Angreifer allerdings nicht nur die Möglichkeit, ein- und auslaufende Signalmuster (für preiswerte Ringe: Bitmuster) zu vergleichen, sondern er kann auch seine Kenntnis des Ringzugriffsverfahrens verwenden, um Schlüsse zu ziehen, wer gerade senden darf.

In [HöPf_85, Höck_85] wurde sehr detailliert (nämlich bis auf Übertragungsbitebene) und ausführlich gezeigt, daß bei geeigneten Zugriffsverfahren für Ringe mit „Senden durch Erset-

zen“ ein Angreifer, der eine Station nicht direkt eingekreist hat, tatsächlich das Senden dieser Station auch anhand der Kenntnis des Ringzugriffsverfahrens, der genauen Ringkonfiguration und seiner Beobachtung nie feststellen kann. Deshalb beschränke ich mich hier auf die Darstellung der wesentlichen Definitionen, Beweisideen und Ergebnisse.

In Abschnitt 3.1.4.1 werden Angreifermodelle aufgestellt, d. h. es wird genau gesagt, was die Fähigkeiten realistischer und im folgenden betrachteter Angreifer sind. Hieraus ergeben sich einige grundlegende Begriffsdefinitionen und Beweismethoden.

In Abschnitt 3.1.4.2 wird ein sowohl für das Verständnis, als auch für den praktischen Einsatz besonders wichtiges, da effizientes und anonymes Ringzugriffsverfahren angegeben sowie die Idee seines Anonymitäts-Beweises dargestellt.

In Abschnitt 3.1.4.3 wird skizziert, wie dieses Ringzugriffsverfahren für effiziente und anonyme Kanalvermittlung oder Konferenzschaltung abgewandelt werden kann.

In Abschnitt 3.1.4.4 wird das in Abschnitt 2.5.3.2.1 schon angekündigte Ringzugriffsverfahren beschrieben, das maximal viel Anonymität erhält und trotzdem eine auch bezüglich des Empfangszeitpunktes konsistente Sicht von Sender und Empfänger herstellt.

In Abschnitt 3.1.4.5 wird eine Klassifikation der Ringzugriffsverfahren dazu benutzt, alle bekannten Ergebnisse bezüglich ihrer Anonymitätserhaltung kompakt darzustellen.

3.1.4.1 Angreifermodelle, grundlegende Begriffe und Beweismethoden

Nach dem zu Anfang von Abschnitt 2.5.3.2.1 Gesagten ist die Stärke eines Angreifers dadurch bestimmt, wie nahe er an die zu beobachtende Station herankommt, wobei er entweder Leitungen abhören oder andere Stationen kontrollieren kann. Da letzteres ihm mehr Möglichkeiten eröffnet und ersteres voll umfaßt – jede Station erfährt natürlich, was auf den beiden angrenzenden Leitungen übertragen wird – wird nur die Frage untersucht: Wieviele Stationen müssen mindestens zwischen den Angreiferstationen liegen, damit der Angreifer den Sender bzw. Empfänger von Informationseinheiten (Pakete, Nachrichten, Übertragungseinheit eines Kanals) nicht deterministisch identifizieren kann?

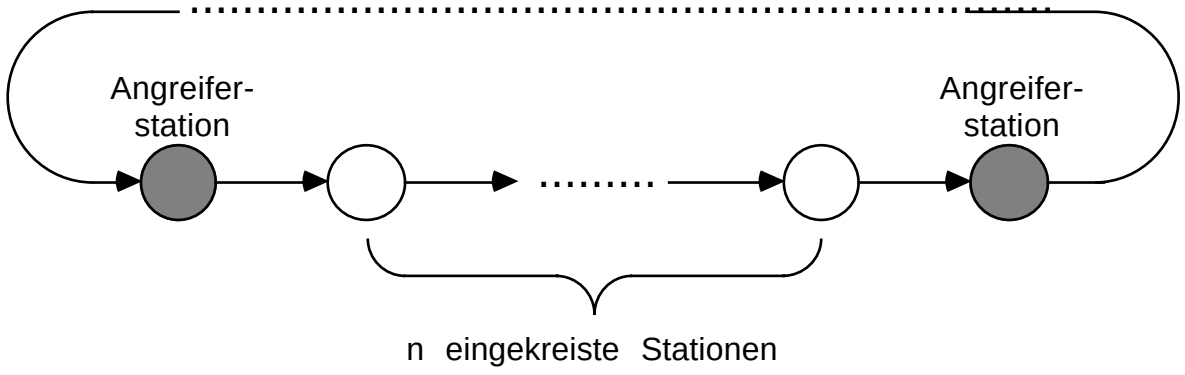


Bild 38: Relevanter Ringabschnitt

Damit ist die Einführung folgender **Begriffe** und zugehöriger **Angreifermodelle** motiviert.

Ein Ring mit gegebenem Zugriffsprotokoll heiße ***n*-anonym**, wenn es keine Situation gibt, in der ein Angreifer bei Einkreisung von *n* hintereinander liegenden Stationen *durch beliebig viele Angreiferstationen* eine davon als Sender bzw. Empfänger einer Informationseinheit identifizieren kann.

Diese Defintion unterstellt den stärkstmöglichen Angreifer, während die in [Höck_85 Seite 6] ohne den kursiven Teil gegebene Definition unterstellt, daß die eingekreisten Stationen von *genau zwei* Angreiferstationen eingekreist sind, was einen eher schwachen Angreifer definiert und von mir als **schwach *n*-anonym** bezeichnet wird.

Es sei darauf hingewiesen, daß der Angreifer selbst Empfänger von Informationseinheiten sein kann und damit durch den Inhalt der Informationseinheiten deren Sender kennt, sofern dieser sich zu erkennen gibt. Dies kann dem Angreifer, wie in Abschnitt 3.1.4.2 gezeigt wird, auch den Sender von anderen Nachrichten verraten. Die Ringe mit gegebenem Zugriffsprotokoll heißen jedoch trotzdem anonym, da der Angreifer die notwendige Zusatzinformation erst durch Nachrichteninhalte bekommt. Dies soll hier nicht modelliert werden, da es sich gemäß Abschnitt 2.6 um Einschränkungen möglicher Alternativen auf Schicht 2 durch höhere Schichten handelt.

Ein Ring mit gegebenem Zugriffsprotokoll heiße ***n*-identifizierbar**, wenn es Situationen gibt, bei denen ein passiver Angreifer nur durch Beobachtungen der Angreiferstationen eine der *n* eingekreisten Stationen als Sender bzw. Empfänger einer Informationseinheit identifizieren kann.

Ein Ring mit gegebenem Zugriffsprotokoll heiße ***n*-testbar**, wenn ein Angreifer für eine der *n* eingekreisten Stationen eine Sendegelegenheit herbeiführen kann, so daß er die Station als Sender einer Informationseinheit identifizieren kann, sofern sie die Sendegelegenheit nutzt.

Müssen hierzu noch weitere, vom Angreifer zwar erkennbare, aber nicht erzwingbare Randbedingungen gelten, so heiße der Ring **partiell *n*-testbar**.

Sind die Eigenschaften identifizierbar, testbar und partiell testbar unabhängig von *n*, der Anzahl der eingekreisten Stationen, so heiße der Ring mit gegebenem Zugriffsprotokoll **ω-identifizierbar**, **ω-testbar**, **partiell ω-testbar**. Dies bedeutet, daß der Angreifer durch Kontrolle einer Station schon etwas herausfinden kann.

Ist ein Ring mit gegebenem Zugriffsprotokoll (schwach) anonym für irgend ein *n*, so ist er natürlich auch anonym, wenn der Angreifer nur eine Station kontrolliert. In diesem Fall heiße der Ring mit gegebenem Zugriffsprotokoll **ω-anonym**.

Zur Herbeiführung oder Verhinderung von Sendegelegenheiten werden einem Angreifer alle Maßnahmen erlaubt, die keine der eingekreisten Stationen zu nicht spezifiziertem Verhalten zwingen. Diese Einschränkung ist notwendig, da zu Beweiszwecken klar sein muß, wie die Stationen auf Eingangsbelegungen reagieren.

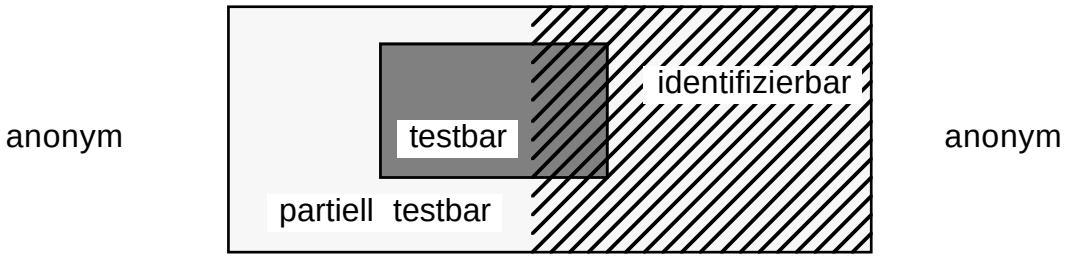


Bild 39: Zusammenhang zwischen den eingeführten Begriffen

Nach Definition gelten die Implikationen

$$n\text{-anonym} \Rightarrow (n+1)\text{-anonym} \qquad \text{(A 1)}$$

$$n\text{-anonym} \Rightarrow \text{schwach } n\text{-anonym} \qquad \text{(A 2)}$$

während die intuitiv einsichtige Implikation

$$\text{schwach } n\text{-anonym} \Rightarrow \text{schwach } (n+1)\text{-anonym} \qquad \text{(A 3)}$$

selbst bei restriktiver Definition, was ein RING-Netz mit „Senden durch Ersetzen“ ist, nicht bewiesen werden konnte. Das Problem beim Beweis dieser Behauptung ist, daß der schwache Angreifer bei n+1 eingekreisten Stationen durch Beobachtung nicht eine Teilmenge der Information erhält, die er durch Beobachtung bei n eingekreisten Stationen bekommt. Dies wäre nur dann der Fall, wenn die zwei Angreiferstationen in eine zusammenfallen würden. Damit ist also die Implikation

$$\text{schwach } n\text{-anonym} \Rightarrow \omega\text{-anonym} \qquad \text{(A 4)}$$

bewiesen. Aufgrund der Tatsache, daß die erhaltenen Informationen bei n+1 eingekreisten Stationen keine Teilmenge der Information sein muß, die der Angreifer bei Einkreisung von n Stationen erhält, kann man bei einer sehr weiten Auslegung, was ein RING-Netz mit „Senden durch Ersetzen“ ist, sogar zeigen, daß (A 3) nicht allgemeingültig ist [Höck_85].

Gegenbeispiel zu (A 3): Man betrachte einen Ring mit (2k+1) Teilnehmer und einer Verbindungs-Verschlüsselung zwischen den Stationen (i mod (2k+1)) und ((i+2) mod (2k+1)). Nach dem in Abschnitt 2.6 Gesagten hat man hier, wie in Bild 40 gezeigt, auf den Schichten oberhalb von Schicht 1 eine andere Ringkonfiguration als auf Schicht 1 (Bitübertragungsschicht).

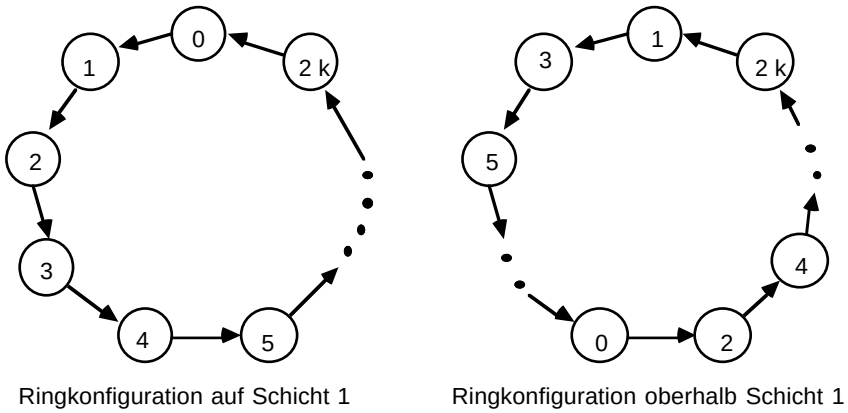


Bild 40: Andere Ringkonfiguration oberhalb von Schicht 1 als auf Schicht 1

Ein Angreifer, der auf Schicht 1 (Bitübertragungsschicht) 2 Stationen einkreist, hat bezüglich der höheren Schichten den halben Ring eingekreist, und ein Angreifer, der auf Schicht 1 (Bitübertragungsschicht) 3 Stationen einkreist, hat bezüglich der höheren Schichten nur eine Station eingekreist, kann diese also beobachten.

(A 3) ist also bei einer sehr weiten Auslegung, was ein RING-Netz mit „Senden durch Ersetzen“ ist, nicht allgemeingültig. Unter hinreichend starken Voraussetzungen sollte (A 3) jedoch gelten und bewiesen werden können. Eine starke, den Schluß von n auf n+1 unterstützende Voraussetzung wäre, daß jede der eingekreisten Stationen die Aktivität einer benachbarten noch mitübernehmen kann.

Vor. Jede Station kann das gleiche Ein-/Ausgangsverhalten aufweisen wie zwei aufeinanderfolgende Stationen.

Beh. schwach n-anonym $\Rightarrow$ schwach (n+1)-anonym

Bew. Man betrachte n+1 eingekreiste Stationen. Sei A eine beliebige der eingekreisten Stationen und B eine Nachbarstation zu A und auch eine der eingekreisten Stationen. Wegen der Voraussetzung kann das Verhalten der Stationen A und B von nur einer Station AB simuliert werden. Jetzt gibt es nur noch n eingekreiste Stationen. Wegen der schwachen n-Anonymität kann der Angreifer keiner Nachricht ihren Sender bzw. Empfänger zuordnen. Es gibt also für jede Nachricht, die von der Station AB gesendet wurde, einen alternativen Sender aus den restlichen n-1 Stationen. Also gibt es den gleichen alternativen Sender für Sendungen der Station A oder der Station B. ♦

Obige Voraussetzung ist jedoch sehr stark. Man kann nämlich sogar schon folgendes beweisen.

Beh. Obige Voraussetzung impliziert schon 2-Anonymität.

Bew. Es gibt die trivialen Alternativen, daß die erste der beiden eingekreisten Stationen alle Informationseinheiten sendet bzw. daß die zweite dies tut. ♦

Nachdem schon erste Beweise bezüglich Anonymitätseigenschaften geführt wurden, ist es zweckmäßig, die dabei verwendeten **Beweismethoden** hervorzuheben und zu verallgemeinern. Zwei Fälle sind zu unterscheiden:

1. Der Nachweis von „nicht anonym“:
   Hier muß einfach angegeben werden, wie der Angreifer eine der eingekreisten Stationen als Sender einer Nachricht identifizieren kann.
2. Der Nachweis von „anonym“:
   Hier muß gezeigt werden, daß der Angreifer nie eine der eingekreisten Stationen als Sender einer Nachricht identifizieren kann. Aber wie soll man das tun, da man dem Angreifer doch beliebig (oder zumindest sehr, aus Beweisgründen etwa polynomial) lange Beobachtungen und alle denkbaren (oder zumindest mit möglichem, aus Beweisgründen etwa polynomialem Aufwand durchführbaren) logischen Schlüsse zugestehen muß?

Einen Hinweis erhält man, wenn man die Situation von außen betrachtet. Aufgrund seiner Beobachtung glaubt der Angreifer, daß ein bestimmtes Ereignis stattgefunden hat. Man muß also nur zeigen, daß dies nicht zu stimmen braucht. Für diesen Nachweis wird das Konzept möglicher *alternativer Abläufe* (versteckte Automorphismen [Merr_83], Alternativfolgen [Waid_84]) angewandt. Es werden mögliche alternative Abläufe konstruiert, die für den Angreifer nicht unterscheidbar sind und in welchen ein vom Angreifer behauptetes Ereignis nicht auftrat. Diese alternativen Abläufe müssen sogar nicht einmal möglich sein, wenn man zeigen kann, daß der Angreifer die Unmöglichkeit nicht nachweisen kann. Dieses Vorgehen ist denkbar, wenn der Angreifer mit nur partiellem Protokollwissen modelliert wird.

Da das Gewünschte bereits in der *informationstheoretischen Modellwelt* (d. h. ohne die eingeklammerten Texte in 2.) gezeigt werden kann, und die Beweise in ihr einfacher und überzeugender sind, wird sie allen Unterabschnitten von Abschnitt 3.1.4 zugrunde gelegt.

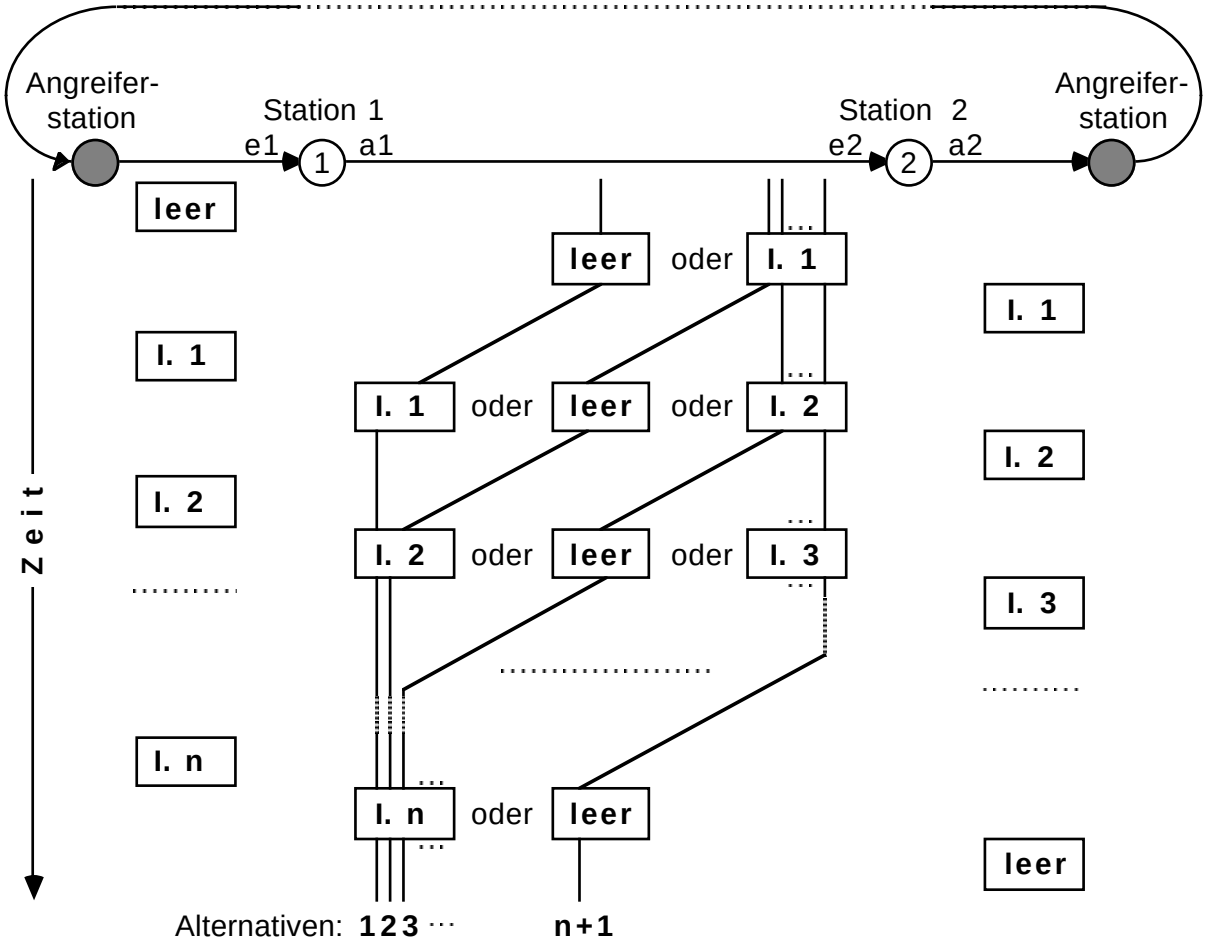
3.1.4.2 Ein effizientes 2-anonymes Ringzugriffsverfahren

Geeignet und effizient sind gewisse bekannte Verfahren (Ring mit umlaufenden Übertragungsrahmen = slotted ring, Ring mit umlaufendem Senderecht = token ring), die dahingehend abgewandelt wurden, daß Senderecht zeitlich unbefristet vergeben wird und daß jede Informationseinheit (Paket, Nachricht, Übertragungseinheit eines Kanals) einmal ganz um den Ring läuft. Ersteres bewirkt verteiltes (und wie zu zeigen ist: anonymes) Abfragen. Letzteres, d. h. daß Informationseinheiten nicht vom Empfänger, sondern erst vom Sender wieder vom Ring entfernt werden, realisiert bereits Verteilung, so daß neben dem Sender auch der Empfänger geschützt wird.

Um die Unsicherheit des Angreifers bezüglich des tatsächlichen Ablaufs zu beweisen, werden für jeden Ablauf, in dem eine Informationseinheit gesendet wird, alternative Abläufe konstruiert. Diese alternativen Abläufe sind in Bild 41 dargestellt. Damit ist der Ring mit diesen Ringzugriffsverfahren als 2-anonyme bewiesen.

Der in [HöPf_85, Höck_85] enthaltene formale Beweis auf Bitübertragungsebene entspricht völlig dem dargestellten Beweis auf Informationseinheitenebene.

Diese Beweise gelten natürlich nur für einen Angreifer, der nicht den Sender der Informationseinheiten kennt, die im alternativen Ablauf von einer anderen Station gesendet werden müssen. Diese Kenntnis könnte der Angreifer etwa dadurch erhalten, daß er selbst Empfänger einer solchen Informationseinheit ist und sich der Absender in der Informationseinheit zu erkennen gibt. Dies wird hier nicht modelliert, da es sich gemäß Abschnitt 2.6 um Einschränkungen möglicher Alternativen auf Schicht 2 durch höhere Schichten handelt.



Effiziente Ringzugriffsverfahren (token, slotted) reichen ein zeitlich unbefristetes Senderecht von Station zu Station weiter. Wenn ein Angreifer 2 Stationen umzingelt hat, die nach Erhalt des Senderechts insgesamt n Informationseinheiten (I.) senden und dann das Senderecht weiterreichen, gibt es n+1 Alternativen, welche Station welche Informationseinheit gesendet haben kann. Für jede Informationseinheit gibt es mindestens eine Alternative, bei der Station i (i=1, 2) die Informationseinheit sendet.

Das Beispiel kann auf g umzingelte Stationen verallgemeinert werden. Es gibt $\binom{n+g-1}{n}$ Alternativen und zumindest eine Alternative für jede Informationseinheit, bei der Station i (i=1, 2, ...,g) die Informationseinheit sendet.

Bild 41: Ein anonymes Zugriffsverfahren für RING-Netze garantiert: ein Angreifer, der eine Folge von Stationen umzingelt hat, kann nicht entscheiden, welche was sendet.

3.1.4.3 Effiziente Kanalvermittlung und Konferenzschaltung

Wird die Bandbreite des RING-Netzes nicht als Ganzes, sondern in Teilen verwaltet (etwa mehrere Übertragungsrahmen bei „Ringen mit umlaufenden Übertragungsrahmen“ oder mehrere Senderechtszeichen für unterschiedliche Teile bei „Ringen mit umlaufendem Senderecht“), so kann eine Station, indem sie einen (oder mehrere) Teil geeigneter Bandbreite für längere Zeit fortlaufend benutzt, mit dem in Abschnitt 3.1.4.2 beschriebenen Ringzugriffsverfahren 2-anonym (Simplex-)**Kanäle** schalten.

Bei **Duplex-Kanälen** kann sogar ohne große Anonymitätseinbußen darauf verzichtet werden, daß alle Information einmal ganz um den Ring läuft. Statt dessen nimmt der Empfänger die Information vom Ring und ersetzt sie sofort durch Information in Gegenrichtung. Dadurch ist die Übertragungskapazität des Rings doppelt so gut nutzbar.

Eine Station kann das Verhalten zweier aufeinanderfolgender Stationen simulieren, sofern der Kanal nicht zwischen diesen beiden Stationen besteht. Diesen Fall kann der Angreifer aber nur dann erkennen, wenn er weiß, daß ein Duplex-Kanal vermittelt wird. Ansonsten könnte es sich auch um einen Simplex-Kanal oder eine Folge von Nachrichten oder Paketen handeln. Weiß der Angreifer, daß auf diese Weise ein Duplex-Kanal vermittelt wird, so liegt aber immerhin noch 3-Anonymität vor:

Eine Station kann das Verhalten zweier aufeinanderfolgender Stationen bis auf den Fall simulieren, daß der Kanal zwischen den Stationen geschaltet ist und hier gibt es bei 3 eingekreisten Stationen verschiedene Möglichkeiten. Der Kanal kann zwischen Station 1 und 2, 2 und 3 und 1 und 3 bestehen. In allen 3 Fällen beobachtet der Angreifer dasselbe.

Unter einer **Konferenzschaltung** wird das gleiche verstanden wie in Abschnitt 3.1.2.6.

Anderenfalls eröffnete das RING-Netz ohne erhebliche Einschränkung der Sender- und Empfängeranonymität keine Möglichkeiten zur effizienten Nutzung, als die in Abschnitt 3.1.2.6 für jedes Verteilnetz beschriebene.

Zunächst wird eine spezielle Möglichkeit für (anonyme) Konferenzschaltungen beschrieben, die ohne zusätzliche Annahmen über die Ring-Schnittstelle auskommt, jedoch nur bei Kanalvermittlung die Bandbreite des RING-Netzes effizient nutzt. Danach wird eine effizientere beschrieben. Diese setzt jedoch voraus, daß die Ring-Schnittstelle nicht nur „Senden durch Ersetzen“, sondern auch „Senden durch Überlagern“ kann.

Bei der ersten Möglichkeit fungiert eine der Teilnehmerstationen als *Zentrale*. Zwischen ihr und allen anderen Gruppenmitgliedern jeweils einzeln kann – wie beschrieben – ein Duplex-Kanal realisiert werden. Die Zentrale bildet das Summensignal aus allen erhaltenen, entschlüsselten Signalen und ihrem eigenen, verschlüsselt es (ggf. für jeden Duplex-Kanal separat) und verteilt es. Eine (anonyme) Konferenzschaltung zwischen n Teilnehmern ist auf diese Weise in n-1 statt n Kanälen möglich. Der „Preis“ für die Einsparung eines Kanals ist, daß das Maximum der Verzögerungszeiten verdoppelt wird.

Bei der zweiten Möglichkeit kreist wie beim RING-2-f-Netz in Abschnitt 2.5.3.2.1 jedes Zeichen zweimal um den Ring. Im ersten Umlauf wird das Summensignal durch Überlagerung „*dezentral*“ gebildet, im zweiten Umlauf wird es verteilt. Die Zeichenanzahl des zur Überlagerung verwendeten Alphabetes muß mindestens so groß wie die Anzahl der Quantisierungsschritte des Konferenzsignals sein. Soll eine Ende-zu-Ende-Verschlüsselung möglich sein, so muß dem Signalwert 0 das 0 entsprechende Zeichen zugeordnet werden und die Signalcodierung muß linear erfolgen. Dann können die Signalcodes wie beim überlagernden Senden (vgl. Abschnitt 3.1.2.6) in linearer Weise (Ende-zu-Ende-)verschlüsselt werden. Dies kann beispielsweise in der Form erfolgen, daß jede der Teilnehmerstationen ihren Signalcode mit einem den anderen bekannten Schlüssel überlagert und alle Teilnehmerstationen diese Schlüssel vom globalen Überlagerungsergebnis subtrahieren und so den Signalcode des Summensignals erhalten. Möchten die Teilnehmer ihr eigenes „Echo“ nicht wahrnehmen, so brauchen ihre Teilnehmerstationen nur vom Signalcode des Summensignals ihren Signalcode zu subtrahieren. Werden

beispielsweise Kanäle geschaltet, so ist eine (anonyme) Konferenzschaltung zwischen *n* Teilnehmern auf diese Weise in zwei statt *n* Kanälen möglich. Es kann sinnvoll sein, diese zwei (Summen-)Kanäle mit einem etwas größeren Amplitudenbereich des Signals und bei linearer Signalcodierung auch entsprechend größerer Bandbreite vorzusehen. Dann können auch wenige Signale großer Amplitude störungsfrei überlagert werden – anderenfalls ergäbe beispielsweise die Summe aus einem maximal und einem minimal positiven Signalwert den betragsmässig maximal negativen Signalwert. Allerdings wird zumindest für größere *n* im (Summen-)Kanal nicht die *n*-fache Bandbreite benötigt, da etwa bei drei gleichlaut Redenden der Zuhörer sowieso nichts mehr versteht.

3.1.4.4 Unkoordinierter Zugriff während des ersten und koordinierter Nichtzugriff während des zweiten Umlaufs

Die in Abschnitt 3.1.4.2 bzw. 3.1.4.3 als 2- oder 3-anonym bewiesenen Zugriffsprotokolle nutzen durch verteiltes und anonymes Abfragen nicht nur den Verteil-Kanal „Ring“ sehr effizient, sondern stellen – abgesehen von Fehlern, die in Kapitel 5 behandelt werden – auch eine konsistente Sicht von Sender und Empfänger über die Tatsache und den genauen Zeitpunkt des Empfangs her, vgl. Abschnitt 2.5.3.2.1. Wie dort schon erwähnt sowie durch die Beschreibung aller Alternativen durch Bild 41 verdeutlicht, schränkt das verteilte und anonyme Abfragen insbesondere bei Mehrfachnutzung des Senderechts die Menge aller Alternativen erheblich ein. Wie erwähnt, kann dies besonders dann die Senderanonymität untergraben, wenn der Angreifer den Sender mancher Informationseinheiten kennt, weil dieser sich ihm gegenüber als der Sender zu erkennen gibt.

Das folgende Zugriffsprotokoll vermeidet diese Einschränkung der Alternativen durch verteiltes und anonymes Abfragen. Es kann dadurch den Verteil-Kanal „Ring“ nicht so effizient nutzen, erhält jedoch die Eigenschaft, daß Sender und Empfänger über die Tatsache und den genauen Zeitpunkt des Empfangs eine konsistente Sicht haben. Dies wird dadurch erreicht, daß während des ersten Umlaufs alle Stationen unkoordiniert zugreifen, d. h. senden, dürfen, während während des zweiten Umlaufs, der nur stattfinden kann, falls der erste vollständig gelang, keine Station zugreifen, d. h. senden, darf. Da im Gegensatz zum RING-2-f-Netz die Umläufe bei einer nur dynamisch, nämlich durch ihr Senden ausgezeichneten Station beginnen und diese Station natürlich nicht global bekannt sein darf, müssen alle Stationen auch während des ersten Umlaufs die Informationseinheiten registrieren, um, sofern sie genau eine Umlaufzeit später, also bei ihrem zweiten Umlauf, nochmals vorbeikommen, sie unverändert weiterzureichen. Empfangen, d. h. an die höheren Schichten des Kommunikationssystems zur Weiterbearbeitung übergeben, werden Informationseinheiten ausschließlich während des zweiten Umlaufs. Nach dem zweiten Umlauf ersetzt der Sender die Informationseinheit durch 0 oder durch eine neue Informationseinheit, die in ihrem ersten Umlauf möglicherweise von einer anderen Station überschrieben wird.

Um die Protokolle, die das Sende- und in diesem Fall erstmals das nichttriviale Empfangsverhalten beschreiben, in der in [HöPf_85, Höck_85] üblichen, an die Syntax der Programmiersprache Ada [REFE_83] angelehnten Notation aufzuschreiben, muß diese etwas erweitert

werden: e_t und a_t bezeichne die Informationseinheit am Ein- bzw. Ausgang zum Zeitpunkt *t*, wobei die Zeitskalierung so erfolgen soll, daß *t*-1 den entsprechenden Zeitpunkt beim vorherigen Umlauf bezeichnet. *empfange* bezeichne die Weitergabe der am Eingang anliegenden Informationseinheit an die höheren Kommunikationsschichten. Dann lauten die Protokolle für ein RING-Netz mit 2 Umläufen, die bei einer beliebigen Station beginnen:

2-anonymes RING-2-b-Sendeprotokoll:

```
if   e_t = 0 or e_t-1 ≠ e_t then  select  a_t := e_t;
                                          or      a_t := I(i);      -- unkoordinierter Zugriff
                                  end select;
elsif  a_t-2 = e_t-1 = e_t  then  select  a_t := 0;         -- Übertragung fertig
                                  or      a_t := I(i);      -- Überschreiben mit neuer Sendung
                                  end select;
else   a_t := e_t;
end if;
```

RING-2-b-Empfangsprotokoll:

```
if  e_t ≠ 0 and e_t-1 = e_t       then    empfange;
end if;
```

Die bei diesem RING-2-b-Sendeprotokoll möglichen Abläufe sind in Bild 42 angegeben. *e*1 ist der Eingang von Station 1, *a*1, *a*2, *ar* die Ausgänge der Stationen 1, 2 und *r*. Der Attributwert *x.y* bedeutet, daß Station *x* (*x* = 1, 2) oder eine uninteressante andere Station (*x* = *u*) die Informationseinheit gesendet hat und sie sich im Umlauf *y* befindet.

Es sei hervorgehoben, daß der Sender einer Informationseinheit sie überschreiben darf, wenn sie nach dem 1. Umlauf unverändert zu ihm zurückkommt. Dies ist aus der Sicht der erzielbaren Nutzleistung zwar unsinnig, für die 2-Anonymität aber notwendig, wie die Untersuchung des folgenden 2-identifizierbaren RING-2-b-Sendeprotokolls zeigen wird.

Da jede der Stationen das gleiche Ein-/Ausgangsverhalten aufweisen kann wie zwei aufeinanderfolgende, ist das obige RING-2-b-Sendeprotokoll nach dem in Abschnitt 3.1.4.1 Bewiesenen 2-anonym.

Da im 1. Umlauf die Sendemöglichkeit auch gegen die Übertragungsrichtung des Ringes wandern kann und dies innerhalb einer vom Angreifer eingekreisten Gruppe von Stationen vom Angreifer nicht beobachtbar ist, ist obiges RING-2-b-Sendeprotokoll anonymer (bzw. genauer: unverkettender) als die im Abschnitt 3.1.4.2 als 2-anonym bewiesenen Zugriffsprotokolle mittels verteiltem und anonymem Abfragen. (Ein weiterführender, quantitativen Ansatz zur Bewertung der Anonymitäts- und Unverkettbarkeitserhaltung von Ringzugriffsprotokollen ist in [Höck_85 Seite 60ff] nachzulesen.)

Leider wird dieser Anonymitäts- bzw. Unverkettbarkeitsgewinn mit einem – meiner Meinung nach für fast alle Anwendungen – unverhältnismäßigen Absinken der Nutzleistung erkauft:

- Wird die Bandbreite des Ringes nur zu einem kleinen Teil genutzt, ist es selten, daß bei Zugriffsprotokollen mit verteiltem und anonymem Abfragen das Senderecht beim Durchlaufen der vom Angreifer eingekreisten Stationen insgesamt mehr als einmal genutzt wird. Wird es aber höchstens einmal pro Durchlauf genutzt, so sind die Zugriffsprotokolle mit verteiltem und anonymem Abfragen genauso anonym und insbesondere

unverkettend wie das gerade beschriebene 2-anonyme RING-2-b-Sendeprotokoll. Wird bei den Zugriffsprotokollen mit verteiltem und anonymem Abfragen pro Durchlauf das Senderecht insgesamt oft genutzt, so kann das 2-anonyme RING-2-b-Sendeprotokoll die geforderte Nutzleistung (genauer: den geforderten Durchsatz) gar nicht mehr erbringen, ist also sowieso nicht einsetzbar.

- Die Einhaltung des Zugriffsprotokolls ist nur möglich, wenn die Anzahl der Bitverzögerungen pro Station so groß ist, daß eine Informationseinheit mit gespeicherten verglichen werden kann, bevor die entsprechende Ausgabe erfolgt. Zwar kann bei sehr langen Informationseinheiten der Vergleich auf beispielsweise die ersten 50 Bit beschränkt werden, jedoch stellt diese Zahl dann jeweils eine untere Schranke für die mögliche Verzögerung dar, während diese Zahl bei den Zugriffsprotokollen mittels verteiltem und anonymem Abfragen die bereits durch die digitale Signalregenerierung erzwungene Zahl ist. Diese Zahl ist bei ökonomischer Dimensionierung sicher größer als 1/2, da erst in der „Mitte“ eines Bits dessen Wert feststeht (anderenfalls könnte die Bitrate ohne Probleme erhöht werden) und erst danach mit der Übertragung dieses Bitwertes begonnen werden kann. Praktische Implementierungen erreichen für diese Zahl etwa den Wert 1.
  Die in manchen Ringbeschreibungen explizit [Tane_81 Seite 308] oder implizit gemachte Aussage, daß diese Zahl durch das Ringzugriffsverfahren erzwungen wird, ist für binäre Ringe falsch: Bei Übertragungsrahmen genügt es, das Reservierungsbit ganz am Anfang des Übertragungsrahmen zu setzen, *bevor* es gelesen werden kann. Wird es dann als gesetzt gelesen, hat es die Station bereits richtig weitergeleitet und darf natürlich nicht senden. Wird es jedoch danach als nicht gesetzt gelesen, sendet die Station ihre Informationseinheit. Ebenso kann das letzte Bit eines Senderechtszeichens invertiert ausgegeben werden, bevor es gelesen wird. Erhält es die Station danach nicht, darf sie natürlich nicht senden, hat es aber bereits richtig weitergeleitet. Erhält sie es, hat sie es ebenfalls richtig invertiert und sendet.
  Da die Verzögerungszeit pro Station proportional zur Anzahl der Bitverzögerungen ist, wird sie durch das RING-2-b-Sendeprotokoll erhöht. Dies geschieht natürlich in jeder Ringstation, so daß die globale Verzögerungszeit zumindest bei großen Ringen mit einer Bandbreite von nur wenigen hundert Mbit/s stark ansteigt und damit für viele Anwendungen zu groß wird.

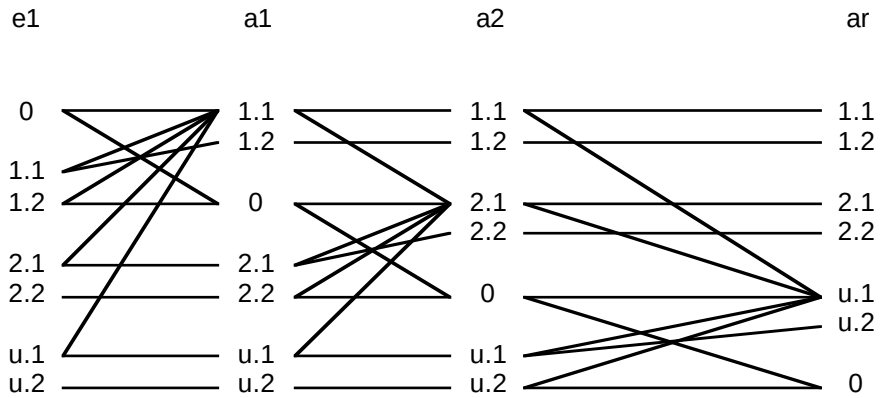


Bild 42: 2-anonymes RING-2-b-Sendeprotokoll

Wird das obige RING-2-b-Sendeprotokoll zum unten angegebenen eingeschränkt, indem verboten wird, daß Stationen Informationseinheiten, die sie im vorherigen ersten Umlauf gesendet haben und die unverändert zu ihnen zurückkommen, selbst überschreiben, so ist nicht nur der Beweis von Abschnitt 3.1.4.1 nicht anwendbar, da nun nicht mehr jede Station das gleiche Ein-/Ausgangsverhalten aufweisen kann wie zwei aufeinanderfolgende, sondern das RING-2-b-Sendeprotokoll wird sogar 2-identifizierbar:

Ein Angreifer habe eine Gruppe von 2 aneinandergrenzenden Stationen eingekreist. Beobachtet er eingangsseitig 0 und danach ausgangsseitig 2 mal hintereinander verschiedene Informationseinheiten, deren erste von den nicht eingekreisten Stationen jeweils nicht verändert wird, so wurde die erste der beiden Informationseinheiten von der letzten der eingekreisten Stationen gesendet. Anderenfalls hätte die erste der eingekreisten Stationen sie gesendet, wobei dann nach dem unten angegebenen RING-2-b-Sendeprotokoll keine der beiden Stationen sie hätte überschreiben dürfen.

Gegenüber dem 2-anonymen Sendeprotokoll wird nur $e_{t\text{-}1}$ in der ersten Bedingung durch $a_{t\text{-}1}$ ersetzt.

2-identifizierbares RING-2-b-Sendeprotokoll:

```
if   e_t = 0 or a_t-1 ≠ e_t then  select  a_t := e_t;
                                          or      a_t := I(i);      -- unkoordinierter Zugriff
                                  end select;
elsif  a_t-2 = e_t-1 = e_t  then  select  a_t := 0;       -- Übertragung fertig
                                  or      a_t := I(i);    -- Überschreiben mit neuer Sendung
                                  end select;
else   a_t := e_t;
end if;
```

Die bei diesem RING-2-b-Sendeprotokoll noch möglichen Abläufe sind in Bild 43 angegeben.

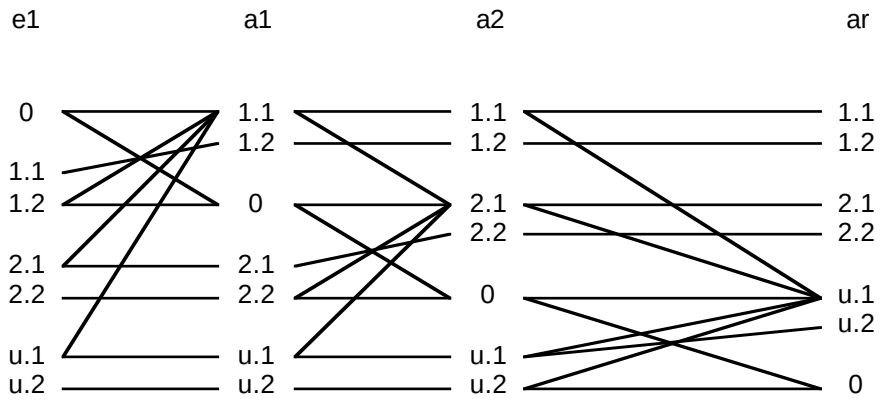


Bild 43: 2-identifizierbares RING-2-b-Sendeprotokoll

3.1.4.5 Klassifikation und Anonymitätseigenschaften der Ringzugriffsverfahren

Alle mit diesen Beweismethoden bisher untersuchten Zugriffsverfahren für Ringe mit „Senden durch Ersetzen“ sind in Bild 44 klassifiziert.

Ihre Anonymitätseigenschaften sind jeweils angegeben. Soweit die Anonymitätseigenschaften in dieser Arbeit noch nicht gezeigt wurden, geschieht dies direkt nach Bild 44 bzw. in bis auf die Bitübertragungsebene formalisierten Beweisen in [HöPf_85, Höck_85].

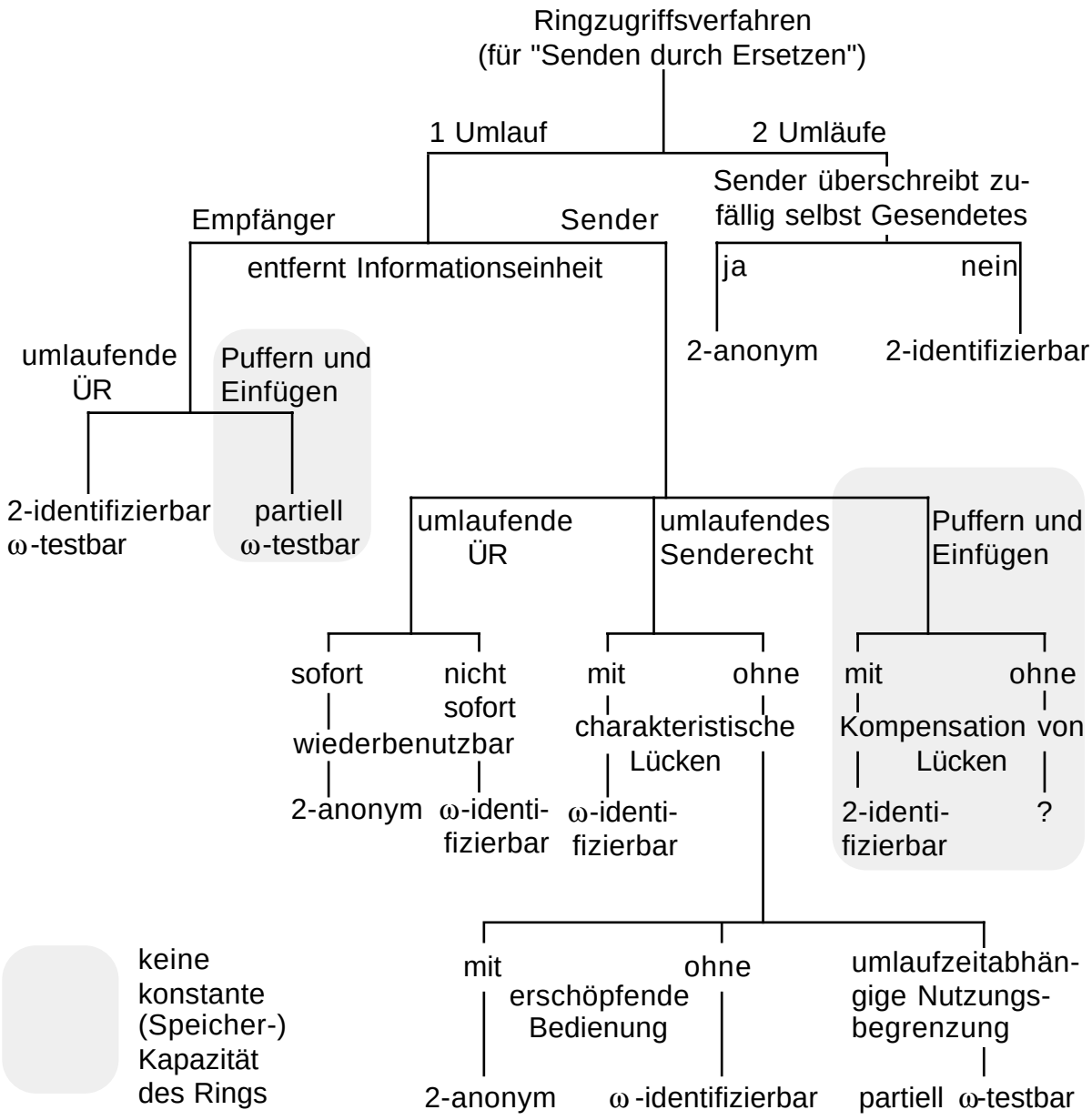


Bild 44: Übersicht der Anonymitätseigenschaften von Ringzugriffsverfahren

Um bei einem „Ring mit umlaufendem Senderecht“ Prioritäten zwischen verschiedenen Verkehrsklassen zu realisieren, werden die obigen Regeln um eine Zusatzregel **Senderechtszeichen mit umlaufzeitabhängiger Nutzungsbegrenzung** (timed token access, timed token rotation protocol) erweitert:

Eine Station darf nach Erhalt des Senderechtszeichens das Senderecht nur nutzen, wenn eine, von der Priorität der zur Sendung anstehenden Informationseinheit (üblicherweise der momentan höchstprioren dieser Station) abhängige Zeitdauer seit dem letzten Erhalt des Senderechtszeichen noch nicht abgelaufen ist. Diese Zeitdauer kann direkt nach Erhalt des Senderechtszeichen ausgewertet werden [Josh_85 Seite 69, Ross_86 Seite 14, ZaNi_87 Seite 432] oder aber – was mir vernünftiger erschiene – das späteste Ende einer Übertragung dieser Station festlegen.

Kennt ein Angreifer die Priorität von Informationseinheiten nicht (was, da verschiedene Prioritäten üblicherweise für verschiedene Verkehrsklassen mit unterschiedlichen Verkehrscharakteristika verwendet werden, eine sehr wenig plausible Annahme ist) und wird die Zusatzregel auf die höchstprioren Informationseinheiten nicht angewendet, etwa indem für sie Zeitdauer auf „unendlich“ gesetzt wird, so sind die entstehenden Ringzugriffsprotokolle mit Prioritäten genauso anonym bzw. identifizierbar wie die zugrundegelegten ohne Prioritäten: Sie sind nicht weniger anonym bzw. mehr identifizierbar, da man bei Unterstellung der höchsten Priorität für alle Informationseinheiten dieselben Alternativfolgen konstruieren kann. Sie sind nicht anonymer bzw. weniger identifizierbar, da die Zusatzregel die Sendemöglichkeiten einer Station nur einschränkt aber nicht erweitert, ansonsten aber alle Abläufe um die Station herum mittels höchstpriorer Informationseinheiten möglich bleiben. An dieser Stelle muß allerdings daran erinnert werden, daß die Begriffe anonym und identifizierbar in dem in Abschnitt 3.1.4.1 definierten Sinne gebraucht wurden. Bei einer quantitativen Bewertung der Anonymitätserhaltung [Höck_85 Seite 60ff] würde erfaßt, daß die Alternativfolgen unwahrscheinlicher würden, die Anonymität also sinken und die Identifizierbarkeit steigen würde.

Kennt ein Angreifer die Priorität von Informationseinheiten, so kann er bei Auswertung der Zeitdauer direkt nach Erhalt des Senderechtszeichens mittels Kontrolle einer Station nach dem Senden einer Informationseinheit für die der diese Informationseinheit sendenden Station folgenden Stationen sukzessiv eine Sendegelegenheit gewünschter Priorität herbeiführen: Der Angreifer verzögert das Senderecht jeweils solange, daß es erst mit Ablauf der festgelegten Zeitdauer bei der nächsten Station eintrifft, diese also (mit der betrachteten Priorität) nicht senden darf. Dies gilt für alle Stationen bis zu der hinter der Station, die die Informationseinheit im vorherigen Senderechtszeichenumlauf gesendet hat, da diese das Senderechtszeichen um die Sendedauer der Informationseinheit später erhielt, also (genau wie alle folgenden) senden darf. Wurde nun die erste Informationseinheit von der ersten Station hinter der des Angreifers gesendet und nutzen alle folgenden Stationen jeweils ihr Senderecht für jeweils mindestens eine Informationseinheit, so kann der Angreifer dies feststellen und damit allen betrachteten Informationseinheiten ihren Sender zuordnen. Dieses Ringzugriffsprotokoll ist also für einen Angreifer, der die Priorität von Informationseinheiten kennt, partiell ω-testbar.

Der geschilderte Angriff gelingt auch, wenn die Zeitdauer das späteste Ende einer Übertragung der Station festlegt. Der Angreifer verzögert in diesem Fall das Senderecht jeweils solange, daß es der nächsten Station das Senden der kleinstmöglichen Informationseinheit nicht mehr erlaubt. Dann kann alles wie oben geschildert ablaufen, nur daß das von einzelnen Stationen ge-

sendete von Station zu Station höchstens um etwas weniger als die kleinstmögliche Informationseinheit länger werden kann, während dies oben nicht der Fall zu sein braucht. Auch dieses Ringzugriffsprotokoll ist also für einen Angreifer, der die Priorität von Informationseinheiten kennt, partiell ω-testbar.

Da man dies, wie oben begründet, unterstellen muß, sind „Ringe mit umlaufendem Senderecht“ und umlaufzeitabhängiger Nutzungsbegrenzung des Senderechtszeichen für Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz nicht geeignet.

3.2 Anonymität schaffende Schichten

In diesem Abschnitt wird die effiziente Realisierung der (Teil)Schichten beschrieben, die (innerhalb des Kommunikationsnetzes) Anonymität und Unverkettbarkeit schaffen. Wie schon in Abschnitt 2.6 erwähnt, bezieht sich der Terminus „schaffen“ nicht auf eine globale, d. h. auch Information außerhalb des Kommunikationsnetzes einschließende Sicht, da dem Angreifer durch die Gestaltung des Kommunikationsnetzes keine Information außerhalb dessen weggenommen werden kann.

3.2.1 Kanäle bei Verteilung

Wie in den Abschnitten 2.6 und 3.1.1 schon erwähnt, wird in diesem Abschnitt eine effiziente Realisierung der in Bild 30 eingezeichneten Kanalselektion behandelt.

Während heutzutage bei der breitbandigsten Übertragungsleitung, der Monomode-Glasfaser, meistens nur ein Bitstrom mittels über einen relativ großen Frequenzbereich verschmierter Energieimpulse übertragen wird, oder allenfalls einige wenige solcher Bitströme mittels Wellenlängenmultiplex (wavelength division multiplexing = WDM, [Unge_84]), wird es die *kohärente optische Nachrichtentechnik* (coherent optical fiber transmission) in wenigen Jahren erlauben, sehr preiswert sehr viele sehr breitbandige Bitströme über eine Monomode-Glasfaser zu übertragen. Der für den Schutz des Empfängers mittels Verteilung wichtige Punkt ist, daß der Empfänger mittels *optischem Überlagerungsempfang* (coherent detection [BaBr_85, Stan_85, Baac_85, LiHe_87]) einen (oder mehrere) der Bitströme auswählen kann [Pfi1_85 Seite 58]. Diese Auswahl erlaubt eine sehr effiziente Implementierung der K- und V-Kanäle von Abschnitt 3.1.1, indem eine Station ihre optischen Überlagerungsempfänger genau auf die Kanäle einstellt, die ihr in einem immer empfangenen I-Kanal (oder bei Massenkommunikationsdiensten [Kais_82] von ihrem Eigentümer direkt) als diejenigen mitgeteilt wurden, in denen etwas an sie gesendet wird. Diese Auswahl mittels optischem Überlagerungsempfang hält den Teil des Kommunikationsnetzes, der mit allerhöchsten Frequenzen und Bitraten arbeiten muß und deshalb aufwendig ist, minimal klein. Sie ist deshalb weit billiger und leistungsfähiger als eine Realisierung der Kanalauswahl mittels Zeitmultiplex (time division multiplexing = TDM) oder Wellenlängenmultiplex. Letzteres deshalb, weil optische Überlagerungsempfänger aus einem weiten Frequenzspektrum beliebige Kanäle selektieren können, während bei Wellenlängen-

multiplex für jede Wellenlänge ein eigener Empfänger benötigt wird und die Frequenzauflösung zudem gröber ist.

Da ein optischer Überlagerungsempfänger zudem mit einem sehr kleinen Bruchteil der Lichtenergie auskommt, die ein konventioneller optischer (Direkt-)Empfänger (direct detection) benötigt, kann die Lichtenergie jedes in einem bestimmten Frequenzbereich sendenden Senders auf sehr viel mehr Empfänger aufgeteilt werden, so daß auch der senderseitige Aufwand gering ist. Dadurch wird das von mir aus Gründen des überprüfbaren Datenschutzes in Frage gestellte Konzept der „Verteilvermittlung“ von BIGFON bzw. des IBFN (vgl. Abschnitt 1.1) auch bezüglich seiner technischen Effizienz in Frage gestellt [Pfi1_85 Seite 59].

3.2.2 MIX-Netz

Bezüglich der Realisierung der (Teil)Schichten, die innerhalb eines MIX-Netzes Anonymität und Unverkettbarkeit schaffen, verdienen vier Gruppen von Fragen vertiefte Beantwortung:

- Wie können auch Kommunikationsdienste mit Realzeitanforderungen, insbesondere nach kurzer Verzögerungszeit, abgewickelt werden? Läßt sich durch Schalten von Kanälen Aufwand sparen?
- Wie wächst die Länge von Nachrichten und Paketen einerseits bzw. Kanälen andererseits mit der Zahl der pro Kommunikationsbeziehung benutzten MIXe?
- Gibt es zu beliebig vorgegebenen asymmetrischen Konzelationssystemen ein minimal längenexpandierendes und zusätzlich noch längentreues Umcodierungsschema?
- Wieviele MIXe können pro Kommunikationsbeziehung benutzt werden? Wie groß ist der mögliche Anteil der MIXe an der Gesamtheit aller Stationen?

Jede Gruppe von Fragen wird in einem eigenen Unterabschnitt behandelt.

3.2.2.1 Schalten von Kanälen beim MIX-Netz

So wie das Verfahren der umcodierenden MIXe ursprünglich in [Chau_81, Cha1_84] und in verallgemeinerter Form in Abschnitt 2.5.2 beschrieben wurde, kann es manche Realzeitforderungen, etwa die Forderung nach kurzer Verzögerungszeit beim Telefonverkehr, nicht erfüllen. Dies liegt im wesentlichen daran, daß jeder MIX alle Bits eines langen Blocks abwarten muß, bevor er mit seiner Entschlüsselung beginnen und danach die Bits des entschlüsselten Blocks zum nächsten MIX senden kann.

Dies kann vermieden werden, wenn eine einzelne, wie in Abschnitt 2.5.2 beschrieben gebildete Nachricht zum Aufbau einer (längere Zeit bestehen bleibenden) Verbindung verwendet wird. Für büschelweise auftretenden Verkehr (bursty traffic), der nur eine kurze Verzögerungszeit erlaubt, kann diese Verbindung ein virtueller Kanal (virtual circuit [Tane_81 Seite 188]) sein, oder ein (realer) Kanal für einen kontinuierlichen Informationsstrom. Die die Verbindung aufbauende, notwendigerweise meistenteils mit einem asymmetrischen Kryptosystem verschlüsselte Nachricht teilt jedem an ihr beteiligten MIX einen Schlüssel eines schnelleren symmetrischen Kryptosystems (vgl. Abschnitt 2.2) mit, den dieser dann als Stromchiffre verwendet (vgl. Abschnitt 2.2.2.1).

Mit diesen Schlüsseln verschlüsselt der Sender und entschlüsseln die MIXe die folgenden Bits der aufgebauten Verbindung genauso, wie die öffentlich bekannten Chiffrierschlüssel beim direkten Umcodierungsschema für Senderanonymität vom Sender dazu verwendet werden zu ver- und die entsprechenden geheimgehaltenen Dechiffrierschlüssel von den MIXen dazu verwendet werden zu entschlüsseln. Wie beim indirekten Umcodierungsschema für Empfängeranonymität ist auch hier selbst bei Verwendung von deterministischen Kryptosystemen eine Mitverschlüsselung von zufälligen Bitketten nicht nötig, da jedem Angreifer bezüglich mit ihm unbekannten Schlüsseln umcodierter Informationseinheiten kein Testen möglich ist. Ebenso braucht auch hier nur bei der Nachricht zum Verbindungsaufbau darauf geachtet zu werden, daß sie mit jedem Schlüssel höchstens einmal umcodiert wird, während sich die Bitfolgen des stromverschlüsselten Kanals – sofern eine synchrone Stromchiffre verwendet wird – beliebig wiederholen dürfen. Bei einer selbstsynchronisierenden Stromchiffre oder einer Blockchiffre besteht die Gefahr, daß ein aktiver Angreifer ein genügend langes Stromstück oder einen Block zweimal mixen läßt, vgl. Abschnitt 2.5.2.5.

Letzteres, die größere Effizienz symmetrischer Kryptosysteme und die Einsparung an Adressieraufwand können Gründe sein, Verbindungen auch dann aufzubauen, wenn keine anderenfalls nicht erfüllbaren Realzeitanforderungen seitens des zu erbringenden Kommunikationsdienstes bestehen. Allerdings sind natürlich alle Informationseinheiten, die eine Verbindung benutzen, auch für das Kommunikationsnetz verkettbar.

Auf den tieferen Schichten des Kommunikationsnetzes müssen dann zwischen Teilnehmerstationen und MIXen sowie zwischen MIXen ebenfalls Verbindungen geschaltet werden, damit erkennbar ist, welche Bits zu welcher Verbindung gehören und ggf. kurze Verzögerungszeiten und/oder gleichmäßiger Informationsfluß garantiert werden können.

Um die Beziehung zwischen Verbindungen zu und von einem bestimmten MIX zu verbergen, muß der MIX auch hier mehrere gleichartige, d. h. für äußere Angreifer nicht in verschiedene Verkehrs-Klassen einteilbare (partitionierbare) Ereignisse abwarten, bevor er sie bearbeitet. In allen drei Regeln bedeutet „zusammen“ im wesentlichen „gleichzeitig“.

R1 Bevor ein MIX eine Verbindung aufbaut, muß er mehrere gleichartige Verbindungsaufbauwünsche abwarten (oder ggf. generieren). Gleichartige, zusammen aufgebaute Verbindungen sollten auch zusammen abgebaut werden. Zumindest müssen jeweils mehrere gleichartige, zusammen aufgebaute Verbindungen zusammen abgebaut werden.

R2 Das (Umcodieren und) Ausgeben kontinuierlicher Informationsströme gleichartiger, zusammen aufgebauter Verbindungen muß zusammen beginnen und sollte zusammen enden. Zumindest müssen jeweils mehrere Informationsströme gleichartiger, zusammen aufgebauter Verbindungen zusammen enden.

R3 Nachrichten oder Pakete von Verbindungen dürfen nur umcodiert werden, wenn von allen gleichartigen, zusammen aufgebauten Verbindungen jeweils gleichviele umcodiert werden können.

Wird auch nur eine dieser drei Regeln verletzt, ist das Umcodieren des sie verletzenden MIXes bezüglich Anonymität der Kommunikationsbeziehung wertlos, wenn die MIXe, über

die der Verbindungswunsch ankam und die MIXe, zu denen der Verbindungswunsch weitergeht, als Angreifer zusammenarbeiten.

Werden bezüglich R1 bzw. R2 nicht alle gleichartigen, zusammen aufgebauten Verbindungen zusammen abgebaut bzw. alle zusammen begonnenen Informationsströme zusammen beendet, werden bezüglich des gerade diskutierten Angreifers die von ihm nicht unterscheidbaren Verbindungsmöglichkeiten in so viele Verkehrs-Klassen eingeteilt, wie Gruppen von Verbindungen zusammen abgebaut werden bzw. wie Informationsströme gleichzeitig enden.

R2 verursacht großen zusätzlichen Übertragungsaufwand, wenn die Varianz der Nutzungszeit (realer) Kanäle groß ist. Allerdings ist dies nicht vom Verbindungsaufbau verursacht, sondern liegt in der Natur des Kommunikationsdienstes: werden kontinuierliche Informationsströme, die kurze Übertragungszeiten fordert, mittels „unabhängiger“ Pakete oder Nachrichten übertragen, und beginnen und enden die Informationsströme zu verschiedenen Zeiten, so kann ein Angreifer durch eine statistische Analyse der Paket- oder Nachrichtenraten zwischen Sender bzw. Empfänger und MIXen als auch, wenn alle Pakete oder Nachrichten dieselbe Route verwenden, zwischen MIXen dasselbe herausfinden. Bedeutungslose Nachrichten, Pakete oder Informationsströme sind also bei solchen Kommunikationsdiensten in jedem Fall nötig.

R3 schränkt die Anwendbarkeit von virtuellen Kanälen drastisch ein.

Nachdem nun die notwendigen und hinreichenden Regeln für das Schalten von Kanälen beim MIX-Netz diskutiert wurden, sind entsprechende Implementierungen zu skizzieren. Zunächst werden Simplex-Kanäle (simplex channel) betrachtet, danach Duplex-Kanäle (duplex channel).

Zunächst wird die Nachricht zum Verbindungsaufbau etwas formaler beschrieben.

Wie in Abschnitt 2.5.2 sei $A_1,...,A_n$ die Folge der Adressen und $c_1,...,c_n$ die Folge der öffentlich bekannten Chiffrierschlüssel der vom Sender gewählten MIX-Folge $MIX_1,...,MIX_n$, wobei c_1 auch ein geheimer Schlüssel eines symmetrischen Kryptosystems sein kann. Sei A_{n+1} die Adresse des Empfängers, der zur Vereinfachung der Notation MIX_{n+1} genannt wird, und c_{n+1} sein Chiffrierschlüssel. Bedeute K „Bitte schalte einen Kanal“ und seien $k_1,...,k_n$ die den MIXen $MIX_1,...,MIX_n$ mitzuteilenden Schlüssel eines symmetrischen Kryptosystems. Damit lautet die Nachricht zum Verbindungsaufbau

$$A_1,c_1(\mathrm{K},k_1,A_2,c_2(\mathrm{K},k_2,A_3,c_3(...,A_{n+1},c_{n+1}(\mathrm{K},k_{n+1})...))).$$

Wo immer zwischen MIXen ein Verteil-Netz benutzt wird, können statt expliziten Adressen auch implizite verwendet werden.

Nach der Nachricht zum Verbindungsaufbau verschlüsselt der Sender die zu sendende Information I als $k_1(k_2(k_3(...k_{n+1}(I)...)))$.

Wenn im Falle eines (realen) Kanals der Sender sofort nach der Nachricht zum Verbindungsaufbau einen kontinuierlichen Informationsstrom sendet und ein MIX nicht sofort einen Kanal vermitteln kann (was meistens der Fall sein wird, da er auf andere Wünsche zur Vermittlung eines Kanals gleicher Bandbreite warten wird), muß dieser MIX den Informationsstrom puffern. Dies ist aufwendig und erhöht die Verzögerungszeit des Kanals, sollte also vermieden werden. Allerdings sollten die Informationsströme auf Kanälen, die von ein und demselben MIX zusammen aufgebaut werden, alle gemäß R2 zusammen beginnen und enden.

Wenn die Stromchiffre selbstsynchronisierend ist, was für jede Blockchiffre mit den in Abschnitt 2.2.2.1 beschriebenen Techniken leicht erreicht werden kann, kann folgendes Verfahren verwendet werden [Pfi1_85]:

Der Sender beginnt seinen kontinuierlichen Informationsstrom sofort. Dieser Bitstrom besteht anfangs aus zufälligen (und damit natürlich auch völlig bedeutungslosen) Bitketten, geht dann aber, angezeigt durch eine spezielle Anfangs-Bitkette (beispielsweise durch hundert Einsen gefolgt von einer Null), deren Auftrittswahrscheinlichkeit bezüglich zufälligen Auftretens gering genug sein muß, in den bedeutungstragenden Bitstrom über. Genügend früh (bezüglich der zur Selbstsynchronisation nötigen Zeichenzahl und der Anzahl der zu durchlaufenden MIXe und damit der nötigen, kaskadierten Selbstsynchronisationen) vor der ersten der hundert Einsen verschlüsselt der Sender den Informationsstrom wie oben angegeben, so daß nur der Empfänger die hundert Einsen und folgenden Zeichen erhält und verstehen kann. Die MIXe entschlüsseln den eintreffenden Bitstrom kontinuierlich ab dem Zeitpunkt, an dem er bei ihnen eintrifft, und übertragen den entschlüsselten Bitstrom ohne Pufferung zum nächsten MIX, sobald mehrere gleichartige Informationsströme zusammen beginnen können. Können hin und wieder Informationsströme nicht schnell genug sukzessiv über alle Teilstrecken durchgeschaltet werden, erhält der Empfänger den Anfang des bedeutungstragenden Bitstroms auch nicht. Dies kann mit den in Abschnitt 5.3 beschriebenen Fehlerbehandlungsverfahren für MIX-Netze toleriert werden.

Eine Alternative wäre, daß der Empfänger den Sender mittels einer Nachricht oder eines Paketes informiert, wenn der Kanal bis zu ihm durchgeschaltet ist, so daß der Sender erst danach von zufälligen Bitketten auf bedeutungstragende übergeht.

Um einen Simplex-Kanal abzubauen, kann ein ähnliches Verfahren wie oben beschrieben verwendet werden:

Nach dem letzten zu übertragenden Nutzbit beendet der Sender die Verschlüsselung mit k_{n+1}. Er verschlüsselt eine spezielle Ende-Bitkette (beispielsweise eine Eins gefolgt von hundert Nullen) mit k_n, k_{n-1}, ..., k_3, k_2, k_1, so daß der Empfänger sie in dieser Form (vor seiner Entschlüsselung mit k_{n+1}) erhält. Dies zeigt dem Empfänger das Ende der Nutzbitfolge an. Die Wahrscheinlichkeit, daß eine Ende-Bitkette zufällig auftritt ist, da es sich um einen mit einer Stromchiffre verschlüsselten Bitstrom handelt, exponentiell klein in der Länge der Ende-Bitkette. Nach Erkennen der Ende-Bitkette weiß der Empfänger, daß diese und alle folgenden Bits bedeutungslos sind und folglich weder entschlüsselt noch beachtet werden müssen.

Nachdem der Sender die Ende-Bitkette, wie gerade beschrieben, an den Empfänger gesendet hat, beendet er auch die Verschlüsselung mit den Schlüsseln k_n, k_{n-1}, ..., k_3, k_2, k_1, und sendet eine spezielle Ende-Bitkette (beispielsweise eine Eins gefolgt von hundert Nullen) an den ersten MIX und hört anschließend auf, auf diesem Kanal zu senden. Nachdem der erste MIX die spezielle Ende-Bitfolge erhalten hat, weiß er, daß der Kanal abgebaut werden kann, sendet aber noch solange bedeutungslose Bitfolgen, bis er mindestens zwei gleichartige, zusammen aufgebaute Kanäle zusammen abbauen kann. Um dies zu tun, beendet er spätestens jetzt sein Entschlüsseln und sendet die spezielle Ende-Bitkette an den nächsten MIX. Dieser verfährt genauso bis schlußendlich der Empfänger ein zweites Mal eine Ende-Bitkette erhält.

Da jeder MIX lokal vollständig kontrollieren kann, welche der gleichartigen, zusammen aufgebauten Kanäle er zusammen abbaut, können alle Kanäle so abgebaut werden. Da sich der Abbau von Kanälen nur dann gegenseitig blockieren kann, wenn sie zusammen aufgebaut wurden,

verhindert die zeitliche Abfolge Verklemmungen. Präziser gesagt: Ein Teil eines Simplex-Kanals kann spätestens dann abgebaut werden, wenn die Sender aller gleichartigen Kanäle, bei denen der Verbindungswunsch vor Beginn dieses Teiles des Simplex-Kanal geäußert wurde, das Kanalende signalisiert haben.

Um einen Duplex-Kanal (duplex channel) zu schalten, gibt es zwei Möglichkeiten:

1. Zuerst wird ein Simplex-Kanal vom Initiator des Duplex-Kanals (Sender 1) zur gerufenen Partei (Empfänger 1) geschaltet und danach beispielsweise mittels einer anonymen Rückadresse (vgl. Abschnitt 2.5.2.3) über möglicherweise andere MIXe ein Simplex-Kanal zwischen gerufener Partei (Sender 2) und Initiator des Duplex-Kanals (Empfänger 2).
   Der erste Nachteil dieser Möglichkeit ist, daß die Zeit zum Kanalaufbau zweimal benötigt wird, bevor der Duplex-Kanal benutzt werden kann. Der zweite Nachteil ist, daß der kausale Zusammenhang zwischen den zwei Simplex-Kanälen und seine beobachtbare Auswirkung, nämlich zeitliche Korrelation, die Anonymität der Kommunikationsbeziehung gefährden kann.
2. Zuerst wird ein Duplex-Kanal zwischen Initiator des Duplex-Kanals und MIX_1 geschaltet, danach zwischen MIX_1 und MIX_2, ..., danach zwischen MIX_n und der gerufenen Partei. Hierbei kann dieselbe Art von Nachricht zum Verbindungsaufbau wie für Simplex-Kanäle verwendet werden. Auf diesen Teilstücken des Duplex-Kanals beginnt nicht nur der Initiator des Duplex-Kanals, sondern auch alle MIXe beginnen jeweils sofort damit, zufällige Bitströme zu senden. Wenn die anderen im Kontext von Simplex-Kanälen besprochenen Regeln eingehalten werden, ist die Anonymität der Kommunikationsbeziehung bezüglich der in Abschnitt 2.5.2 „erlaubten“ Angreifer garantiert.
   Es sollte hervorgehoben werden, daß auch bei Duplex-Kanälen, bei denen Initiator oder gerufene Partei den Kanalabbau veranlassen können, der Duplex-Kanal abschnittsweise immer vom Initiator über die MIXe zur gerufenen Partei abgebaut werden kann. Wenn die gerufene Partei den Kanalabbau veranlaßt, wird dies von ihr dem Initiator signalisiert, der dann den abschnittsweisen Kanalabbau beginnt.

Wie in Abschnitt 2.5.2.5 bereits skizziert, hat die für diese Kanalauf- und Abbauverfahren nötige Verwendung *selbstsynchronisierender Stromchiffren* den großen Nachteil, daß jeder durchlaufene MIX Maßnahmen gegen einen aktiven Angriff durch Wiederholung genügend langer Zeichenfolgen ergreifen muß. Deshalb ist es schon aus Aufwandsgründen, und nicht erst aus Gründen der Erhöhung der Unbeobachtbarkeit der Teilnehmer und Einsparung von Bandbreite im Teilnehmeranschlußbereich sinnvoll, eine *synchrone Stromchiffre* zu verwenden und Kanäle synchron zu schalten, wie dies in Abschnitt 6.2 erklärt wird.

3.2.2.2 Längenwachstum der bisherigen Umcodierungsschemata

In diesem Abschnitt wird untersucht, wie die Länge von Nachrichten und Paketen einerseits bzw. Kanälen andererseits mit der Zahl der pro Kommunikationsbeziehung benutzten MIXe wächst. Dies ist für die in den Abschnitten 2.5.2 und 3.2.2.1 angegeben Umcodierungsschemata sowie verschiedene Kryptosysteme gravierend unterschiedlich.

Die Länge jeder Informationseinheit wächst mindestens proportional zur Zahl der pro Kommunikationsbeziehung benutzten MIXe – wobei nur von anderen unabhängige Informationseinheiten als solche bezeichnet werden. Ein Teil der auf einem Kanal übertragenen Bitfolge etwa ist keine vom Rest unabhängige Informationseinheit, so daß es asymptotisch irrelevant ist, daß sie nicht wächst, da die Nachricht zum Verbindungsaufbau und damit auch die Länge des Kanals insgesamt wächst. Die Länge aller möglichen Umcodierungsschemata wächst deshalb mindestens proportional zur Zahl der pro Kommunikationsbeziehung benutzten MIXe, da – wie in Abschnitt 2.5.2 begründet – Sender bzw. Empfänger und „mittlere“ MIXe keinen geheimen Schlüssel gemeinsam kennen können und deshalb alle „mittleren“ MIXe zumindest einen Teil der Informationseinheit, der mit ihrem öffentlich bekannten Chiffrierschlüssel verschlüsselt wurde, mit ihrem geheimgehaltenen Dechiffrierschlüssel entschlüsseln müssen, und von diesem Teil zumindest etwa 100 Bits, deren Werte zufällig gewählt worden sein müssen, vom jeweiligen MIX nicht ausgegeben werden dürfen. Hierbei ist es natürlich irrelevant, ob diese etwa 100 Bit bei Verwendung eines deterministischen asymmetrischen Konzelationssystems explizit durch das Umcodierungsschema vorgeschrieben oder bei Verwendung eines indeterministischen asymmetrischen Konzelationssystems (vgl. Abschnitt 2.2.1.2.1) von diesem automatisch hinzugefügt werden.

Wird das *direkte Umcodierungsschema für Senderanonymität* (Abschnitt 2.5.2.2) mit einem asymmetrischen Konzelationssystem fester Blocklänge, kurz einer asymmetrischen Blockchiffre, benutzt, wächst die Länge jeder Informationseinheit sogar exponentiell mit der Zahl der pro Kommunikationsbeziehung benutzten MIXe: Da jeder Block unabhängig von allen anderen ver- und entschlüsselt wird, muß jeder Block etwa 100 Bits, deren Werte zufällig gewählt wurden, enthalten, so daß von der Blocklänge b (in Bits) noch b-100 Bits für die Nutzinformation übrigbleiben. Folglich wächst die Länge der Informationseinheit mit jedem MIX um mindestens den Faktor $b/(b\text{-}100)$, wobei b typischerweise Werte um 1000 annimmt. Gleiches gilt beim indirekten Umcodierungsschema für Empfängeranonymität für den direkt mit dem asymmetrischen Konzelationssystem fester Blocklänge verschlüsselten Rückadreßteil.

Da beim *indirekten längentreuen Umcodierungsschema* in Abschnitt 2.5.2.5 (und den in Abschnitt 5.3.2.3 enthaltenen fehlertoleranten Umcodierungsschemata) kein Teil immer wieder mit dem asymmetrischen Konzelationssystem verschlüsselt wird, tritt bei ihm (ihnen) kein exponentielles, sondern nur lineares Längenwachstum auf. Allerdings ist dies beim in [Chau_81 Seite 87] und leicht verbessert in Abschnitt 2.5.2.5 angegebenen indirekten längentreuen Umcodierungsschema nicht unbedingt ein lineares Wachstum um die minimalen etwa 100 Bits (+ einigen Bits für die Adressierung), sondern ein lineares Wachstum um die die minimale Blocklänge bestimmende minimale Länge einer mit dem asymmetrischen Konzelationssystem noch sicher verschlüsselbaren Informationseinheit, also eher einigen 100 Bits.

Wie in Abschnitt 3.2.2.3 genauer beschrieben wird, kann dies vermieden werden, indem „überflüssige“ Bits im mit dem asymmetrischen Konzelationssystem verschlüsselten Block vom Verschlüsseler mit Nutzinformation belegt werden.

3.2.2.3 Minimal längenexpandierendes längentreues Umcodierungsschema

Der Kommunikations- und Verschlüsselungsaufwand pro Nachricht, Paket bzw. Kanal ist direkt proportional zum Produkt aus der jeweiligen Länge der Informationseinheit und der Zahl der pro Kommunikationsbeziehung benutzten MIXe, da die Informationseinheit natürlich zwischen MIXen jeweils übertragen und von ihnen jeweils umcodiert werden muß.

Deshalb wird ein bei vorgegebenem asymmetrischem Konzelationssystem minimal längenexpandierendes und zusätzlich noch längentreues Umcodierungsschema angegeben.

Der Einfachheit halber wird das minimal längenexpandierende Umcodierungsschema aus dem in Abschnitt 2.5.2.5 für symmetrische Kryptosysteme mit den Eigenschaften $k^{-1}(k(x)) = x$ und $k(k^{-1}(x)) = x$, d. h. nicht nur Ver- und Entschlüsselung, sondern auch Ent- und Verschlüsselung sind zueinander invers, angegebenen entwickelt, vgl. Bild 25.

„Überflüssige“ Bits im mit dem asymmetrischen Konzelationssystem verschlüsselten ersten Block werden vom Verschlüsseler mit Nutzinformation belegt und vom entschlüsselnden MIX *vor* den mit einer symmetrischen Stromchiffre entschlüsselten Rest der Nachricht gehängt. *An* den Rest der Nachricht wird dann entsprechend viel (genauer: wenig) „zufälliger Inhalt“ angehängt, wodurch die Umcodierung längentreu wird.

Voraussetzung für minimale Längenexpansion des Umcodierungsschemas ist, daß die Stromchiffre beliebig lange Informationseinheiten ohne Längenexpansion ver- und entschlüsseln kann. Dies ist etwa für Ergebnisrückführung (vgl. Abschnitt 2.2.2.1) unter Verwendung von (verallgemeinertem) DES (vgl. Abschnitte 2.2.2.2 und 2.2.2.3 sowie den Anhang) ebenso der Fall wie $k^{-1}(k(x)) = x$ und $k(k^{-1}(x)) = x$.

Jede Nachricht N_j besteht aus b Bits und wird von MIX_{j-1} gebildet.

Wie in Bild 45 gezeigt, entschlüsselt jeder MIX_j die ersten b_j Bits der Nachricht N_j mit seinem geheimgehaltenen Dechiffrierschlüssel d_j und findet als Ergebnis dieser Entschlüsselung

1. einen Schlüssel k_j einer symmetrischen, beliebig lange Informationseinheiten verschlüsselnden Stromchiffre (zum Umcodieren der restlichen b-b_j Bits der Nachricht),
2. die Adresse A_{j+1} des nächsten MIXes (oder Empfängers) und
3. n_j mit chiffrierter Nutzinformation belegte Bits C_j.

Mit k_j verschlüsselt MIX_j die restlichen b-b_j Bits der Nachricht und erhält so den Mittelteil M_j der auszugebenden Nachricht N_{j+1}. Danach hängt er vor M_j die n_j mit Nutzinformation belegten Bits C_j, hinter M_j hängt er, um die Länge der Nachricht nicht zu ändern, b_j-n_j Bits zufälligen Inhalts Z_j. Danach sendet MIX_j die Nachricht $N_{j+1} = C_j,M_j,Z_j$ an die Station mit Adresse A_{j+1}.

Mit den in Abschnitt 2.5.2.5 verwendeten Bezeichnungen besteht jede Nachricht N_j aus dem (Rück-)Adreßteil R_j und dem Nachrichteninhaltsteil I_j. N_1 wird vom Sender (auch MIX_0 genannt) entsprechend den in Abschnitt 2.5.2.5 angegebenen rekursiven Schemata gebildet. Um zu verdeutlichen, wie dies geschieht, wird hier das Bildungsschema für den (Rück-)Adreßteil R_1 explizit angegeben. Im folgenden bedeute $[R_j]_{\leq y}$ die Bits an den Positionen $\leq y$ von R_j, $[R_j]_{>y}$ die Bits an den Positionen $>y$.

$R_{m+1} = e$
$R_j = c_j(k_j, A_{j+1}, [R_{j+1}]_{\leq n_j}), k_j^{-1}([R_{j+1}]_{>n_j})$ für $j = m,\ldots,1$

Da die Instanz, die k_j generiert, nämlich Sender bzw. Empfänger, jeweils $k_j^{-1}([R_{j+1}]_{>n_j})$ kennt, kann sie den, wie in Abschnitt 2.5.2.5 gebildeten, Nachrichteninhaltsteil I_j jeweils mit der synchronen Stromchiffre passend vor dem Senden bzw. nach dem Empfangen entschlüsseln.

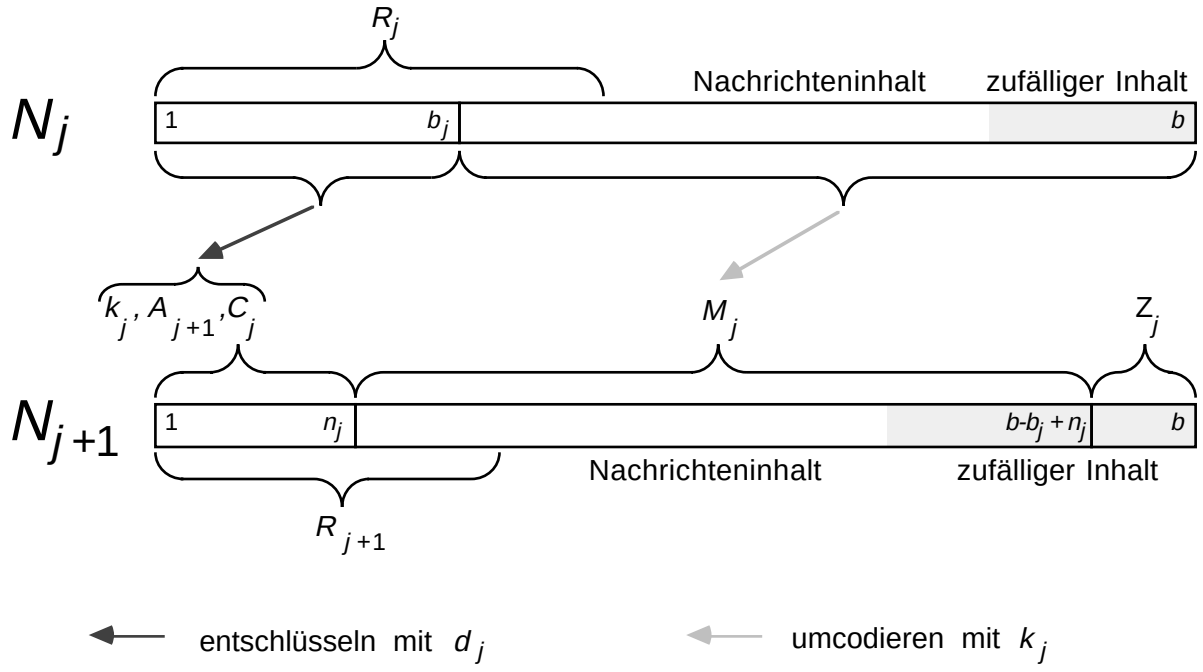


Bild 45: Minimal längenexpandierendes längentreues Umcodierungsschema

3.2.2.4 Anzahl der pro Kommunikationsbeziehung benutzbaren MIXe und ihr möglicher Anteil an der Gesamtheit aller Stationen

In diesem Abschnitt wird anhand eines einfachen Kommunikationsnetzmodells der Frage nachgegangen, wieviele MIXe pro Kommunikationsbeziehung bei günstiger Wahl des Verschlüsselungsschemas und Kryptosystems benutzt werden können. Hieraus ergibt sich – sollen bedeutungslose Informationseinheiten weitgehend vermieden werden – der mögliche Anteil der MIXe an der Gesamtheit aller Stationen.

Die bisherigen drei Unterabschnitte zeigten, daß auch für minimal längenexpandierende Umcodierungsschemata der Übertragungsaufwand im Kommunikationsnetz für jede Nachricht, jedes Paket und auch jeden Kanal mindestens quadratisch mit der Zahl der pro Kommunikationsbeziehung benutzten MIXe wächst, denn es werden mindestens linear wachsende Informationseinheiten linear oft übertragen. Folglich darf die Zahl der pro Kommunikationsbeziehung

benutzten MIXe nicht zu groß sein, insbesondere können nicht alle Stationen eines großen Kommunikationsnetzes alle Nachrichten, Pakete oder Kanäle mixen.

Glücklicherweise tritt das Längenwachstum bezüglich des Inhalts geschalteter Kanäle nicht auf, da eine konventionelle Stromchiffre verwendet werden kann. Da aber die Verzögerungszeit (und auch der Umcodierungs- und Übertragungsaufwand) mindestens proportional zur Zahl der pro Kommunikationsbeziehung benutzten MIXe ist, darf auch hier diese Zahl nicht zu groß sein.

Um für Dienste mit harten Realzeitbedingungen kurze Verzögerungszeiten erreichen zu können, muß der Durchsatz einer Station, die als MIX agiert, sehr groß sein, da sie immer genug Nachrichten, Pakete bzw. Kanäle zu mixen haben muß. Diese müssen auf Wiederholungen getestet, umcodiert, umsortiert und weitergeleitet werden, weswegen ein MIX extrem leistungsfähig sein muß und deshalb ziemlich komplex und nicht billig sein dürfte. Folglich kann man sich in einem MIX-Netz nur eine beschränkte Zahl MIXe leisten.

Wenn das MIX-Netz implementiert wird, indem einige Teilnehmerstationen eines existierenden (physischen) Kommunikationsnetzes als MIXe verwendet werden, muß jede Informationseinheit mehrmals über das Kommunikationsnetz übertragen werden, was zur Verzögerungszeit in den MIXen weitere hinzufügt. Einfach die Vermittlungseinrichtungen des (physischen) Kommunikationsnetzes als MIXe zu verwenden, kann aus den in Abschnitt 2.1.2 diskutierten Gründen auch nicht empfohlen werden, da die Gefahr ihrer Zusammenarbeit generell viel zu groß und in Staaten mit einem – auch nur die Übertragungsdienste betreffenden – Fernmeldemonopol wie der Bundesrepublik Deutschland völlig absurd ist.

Um ein besseres Verständnis der Zusammenhänge der Entwurfsentscheidungen zu gewinnen, wird im folgenden das in [Pfi1_85] entworfene, einfache Kommunikationsnetzmodell betrachtet. Zunächst wird das zugrundegelegte Kommunikationsnetz beschrieben, danach seine Verkehrslast und meine Annahmen. Danach werden einige Leistungskenngrößen mittels geschlossener Formeln berechnet, was zu oberen Schranken für die Zahl der pro Nachricht, Paket bzw. Kanal sowie insgesamt benutzbaren MIXe führt. Die Formeln werden auf einige Nutzleistungs-Szenarios angewandt. Entsprechende Szenarios für andere Nutzleistungsforderungen können leicht entwickelt werden.

Notation des Kommunikationsnetzmodells

Sei

N — die Zahl der Teilnehmer,

M — die Zahl der MIXe, wobei $M \leq N$ gelte,

U [bit] — die Länge der kleinsten, mit dem verwendeten Kryptosystem sicher verschlüsselbaren Informationseinheit (unit) nach ihrer Verschlüsselung,
(Da, wie schon häufig erwähnt, bei Verwendung eines asymmetrischen Konzelationssystems bei MIXen jede Informationseinheit, die mit einem öffentlich bekannten Chiffierschlüssel des MIXes verschlüsselt wird, etwa 100 bit lange zufällige Bitketten bei Verwendung eines deterministischen Kryptosystems explizit enthalten muß und bei Verwendung eines indeterministischen implizit enthält, gilt für alle hier verwendbaren asymmetrischen Konzelationssysteme $U \geq 100$.
Für das einzige bekannte, für MIXe verwendbare asymmetrische Konzelationssystem RSA gilt $U \geq 500$.

Für übliche symmetrische Stromchiffren, die beliebig lange Informationseinheiten verschlüsseln können, beispielsweise (verallgemeinertes) DES und Schlüsseltextrückführung, gilt $1 \le U \le 64$.)

T [s] die Zeit, die zur Ver- bzw. Entschlüsselung einer Informationseinheit des verwendeten Kryptosystems benötigt wird,
(z. B. T = 1/128 s für das Kryptosystem RSA [SeGo_86] oder 1 ns ≤ T ≤ 4,5 µs für eine Stromchiffre, wobei die obere Grenze mittels der Verschlüsselungsleistung des leistungsfähigsten DES-Chips berechnet wurde: 64 bit / 14000000 bit/s)

D_{MtM} [s] die MIX-zu-MIX Übermittlungszeit (MIX-to-MIX delay), d. h. die Zeit pro MIX, die (ohne Umcodieren) für die Informationsübertragung und ggf. Vermittlung benötigt würde,
(beispielsweise 0,001 s = 200 km / 200000 km/s, was bedeuten würde, daß MIXe höchstens 200 km voneinander entfernt sein könnten, da die Signalausbreitungsgeschwindigkeit in Kupfer- und Glasfaserkabeln in etwa 200000 km/s beträgt)

D_{tra} [s] die maximale Übermittlungszeit (transmission delay) im Kommunikationsnetz ohne MIXe (in einer Richtung), so daß immer gilt $D_{tra} \ge$ Durchmesser des Kommunikationsnetzes / Signalausbreitungsgeschwindigkeit. Für ein weltweites Kommunikationsnetz gilt also $D_{tra} \ge 20037$ km / 200000 km/s $\ge 0{,}1$ s.

Annahmen und Notation bezüglich der Verkehrslast

- Der Informationsaustausch zwischen Teilnehmern sei gleichverteilt.
- Der Informationsaustausch durch MIXe sei gleichverteilt.
  Anderenfalls wird die Situation für MIXe, durch die weniger Information ausgetauscht wird, und damit auch die Situation für die Teilnehmer, die diese MIXe benutzen, schlimmer.
- Für jede Nachricht, jedes Paket und jede Verbindung werde dieselbe Zahl MIXe verwendet.
- Wenn bedeutungslose Informationseinheiten gesendet werden, geschieht dies Ende-zu-Ende zwischen Teilnehmerstationen, so daß bedeutungslose Informationseinheiten als Erhöhung der normalen Senderate behandelt werden können.
- Jeder MIX gibt Nachrichten oder Pakete in festen Zeitintervallen aus. Ebenso errichtet er Verbindungen nur in, möglicherweise anderen, festen Zeitintervallen.

Sei also

r_{ev} [1/s] die Rate des betrachteten Ereignisses (event), beispielsweise gilt typischerweise
für das Beginnen einer Verbindung $0{,}01 \ge r_{ev} \ge 10^{-6}$ (1986 wurden in der Bundesrepublik Deutschland im Mittel 1066 Telefongespräche pro Hauptanschluß begonnen [SIEM_87]. Dies ergibt $r_{ev} = 3{,}38 \cdot 10^{-5}$.),
für das Senden einer Nachricht $r_{ev} = 0{,}0001$ und
für das Senden eines Paketes $r_{ev} = 0{,}01$,

a [s] die akzeptable Verzögerungszeit, beispielsweise gilt typischerweise
Verbindungsaufbauzeit für (Bild-)Telefongespräche: 10 s
Übermittlungszeit (in einer Richtung) für
(Bild-)Telefongespräche: 0,2 s (CCITT erlaubt maximal 0,4 s [Bock_86 Seite 197])
Bildschirmtext (interactive videotex): 10 s
Elektronische Post (electronic mail): 1000 s

r_{tra} [bit/s] die Bitrate der Übertragung (transmission) im Kommunikationsnetz

r_{sen} [bit/s] die Bitrate des Dienstes beim Sender, beispielsweise

Telefongespräche: 64 kbit/s

Bildtelefongespräche: 34 Mbit/s

u [bit] die Länge der Informationseinheiten des Dienstes, beispielsweise die Zahl der Nutzinformationsbits in jeder verschlüsselten Informationseinheit. Es gilt immer $u \leq U$ und typischerweise u=U für eine symmetrische Stromchiffre und u = U-100 für ein zur Umcodierung durch MIXe passend gewähltes asymmetrisches Konzelationssystem. Die Wahl eines kleineren u kann die Übermittlungszeit verkürzen, verursacht aber größeren Übermittlungsaufwand.

m die Zahl der pro Nachricht, Paket bzw. Verbindung benutzten MIXe.

t [s] die Länge des Zeitintervalls zwischen den schubweisen, d. h. jeweils zusammen umcodierte Informationseinheiten oder zusammen durchgeschaltete Verbindungen umfassenden Ausgaben der MIXe.

Weiterhin wird angenommen, daß im Falle von Paketvermittlung die Paketlänge die Länge der Verschlüsselungseinheit U teilt, so daß beim Paketieren und Depaketieren von Verschlüsselungseinheiten keine zusätzliche Verzögerungszeit entstehen muß. In der Realität können diese Paketlängen ziemlich groß sein, beispielsweise mindestens 80•20•8 bit = 12800 bit bei Bildschirmtext, sofern ganze Seiten als ein „Paket“ übertragen werden, oder etwa 100000 bit für Elektronische Post, wenn Briefe durchschnittlicher Länge als ein „Paket“ übertragen werden. Solch große Paketlängen könnten U natürlich nicht teilen.

Weiterhin wird das durch die 100 zufällig gewählten Bits verursachte Längenwachstum der Informationseinheiten bei Verwendung eines asymmetrischen Konzelationssystems mit öffentlich bekannten Chiffrierschlüsseln ignoriert.

Beides sind konservative Annahmen bezüglich der Herleitung oberer Schranken für die Zahlen m und M.

Formeln

Zu berechnen sind

v, die (erwartete) Zahl von Ereignissen (vgl. r_{ev}) pro MIX und schubweiser Ausgabe und

D [s], die maximale Verzögerungszeit von Informationseinheiten.

Die minimalen Forderungen sind

$$v \geq 2 \quad (1)$$

$$D \leq a \quad (2)$$

Es gilt

$$v = (N \cdot r_{ev} \cdot t \cdot m) / M.$$

D kann berechnet werden als

$$D = D_{sen} + D_{tra} + D_{MIX},$$

wobei D_{sen} die maximale Verzögerungszeit (delay) beim Sender und D_{MIX} die bei den m MIXen bezeichnet. D_{tra} ist die (bereits definierte) maximale Übermittlungszeit im Kommunikationsnetz ohne MIXe, wobei, wenn jeder Teilnehmer für seine Informationseinheiten m unabhängig wählt, diejenigen, die wissen, wo der Empfänger ist, mit der tatsächlichen Übermittlungszeit statt mit D_{tra} arbeiten könnten.

Es gilt

$D_{sen} = u / r_{sen} + m \cdot T,$

da u Bits abgewartet und dann m mal verschlüsselt werden müssen.
D_{MIX} hängt davon ab, wie die Zeiten koordiniert sind, zu denen MIXe Nachrichten oder Pakete ausgeben bzw. Verbindungen aufbauen. In jedem Fall gilt

$D_{MIX} \geq m \cdot (D_{MtM} + D_{cry}),$

wobei D_{cry} die durch Umcodieren (decryption) bei jedem MIX verursachte Verzögerungszeit (delay) bezeichnet. Es gilt

$D_{cry} = U / r_{tra} + T.$

Wenn die MIXe bezüglich der Zeiten, zu denen sie Nachrichten oder Pakete ausgeben bzw. Verbindungen aufbauen, vollkommen unkoordiniert sind, muß

$D_{MIX} = m \cdot (D_{MtM} + D_{cry} + t)$

angenommen werden, da es bei jedem MIX passieren kann, daß die Nachricht, das Paket oder der Verbindungswunsch gerade ein bißchen zu spät ankommt, um in einem Zeitintervall berücksichtigt zu werden, und deshalb zusätzlich zur zum Umcodieren benötigten Zeit die Zeit t fast vollständig warten muß.
Wenn es genügt, daß die Verzögerungszeit mit großer Wahrscheinlichkeit akzeptabel ist, kann

$D_{MIX} = m \cdot (D_{MtM} + D_{cry} + c \cdot t)$

mit einer Konstante c mit $0{,}5 < c < 1$ gewählt werden, da $0{,}5 \cdot t$ der Erwartungswert der Wartezeit bei jedem MIX ist.
Wenn die Zeitintervalle aller MIXe synchronisiert sind, gilt

$D_{MIX} = m \cdot \max \{D_{MtM} + D_{cry}, t\}.$

(Wenn $t < D_{MtM} + D_{cry}$ ist, dann ist D_{MIX} präziser m mal das kleinste Vielfache von t größer als $D_{MtM} + D_{cry}$. Es macht aber in diesem Fall keinen Sinn, t kleiner als $D_{MtM} + D_{cry}$ zu machen, da die von anderen MIXen kommenden Informationseinheiten zu dieser Zeit noch gar nicht ausgegeben werden können. Außerdem muß beim ersten MIX die Informationseinheit immer möglicherweise die gesamte Zeit t warten.)
Solange die Teilnehmer beliebige Folgen von MIXen wählen können, ist dies nicht wesentlich verbesserbar. Für $D_{MtM} + D_{cry} < (M\text{-}1)/m \cdot t$ ist das Bestmögliche, daß die M MIXe Nachrichten oder Pakete bzw. Verbindungen in Zeitintervallen der Länge t/M ausgeben bzw. errichten. Dann gilt (deterministisch)

$D_{MIX} = m \cdot (M\text{-}1)/M \cdot t = m \cdot \max \{D_{MtM} + D_{cry}, (M\text{-}1)/M \cdot t\}.$

Wenn die Freiheit der Teilnehmer, beliebige Folgen von MIXen zu wählen, beschränkt wird, kann für große t eine erhebliche Verbesserung erreicht werden, indem die MIXe in Klassen eingeteilt werden und jede Klasse die Informationseinheiten $D_{MtM} + D_{cry}$ Sekunden nach der vorherigen ausgibt. Wenn die Teilnehmer für ihre Informationseinheiten jeweils MIXe aufeinanderfolgender Klassen wählen, muß die Informationseinheit nur jeweils beim ersten MIX warten, so daß

$D_{MIX} = t + m \cdot (D_{MtM} + D_{cry}).$

In jedem Fall lauten die Forderungen (1) und (2)

$M \leq 0{,}5 \cdot m \cdot t \cdot r_{ev} \cdot N$ (1)

$$u / r_{sen} + m \bullet T + D_{tra} + D_{MIX} \leq a \qquad (2)$$

Für den Fall beliebig gewählter Folgen von MIXen und synchronisierter Zeitintervalle gilt

$$(2) \Leftrightarrow (2'): \quad m \bullet \max \{D_{MtM} + U / r_{tra} + 2 \bullet T, t + T\} \leq a - D_{tra} - u / r_{sen}$$

und für den Fall einer Klasseneinteilung von MIXen, Synchronisation zwischen den Klassen und klassenkompatibler Folgen von MIXen gilt

$$(2) \Leftrightarrow (2''): \quad t + m \bullet (D_{MtM} + U / r_{tra} + 2 \bullet T) \leq a - D_{tra} - u / r_{sen}$$

Von nun an werden nur noch diese zwei Fälle behandelt.

Üblicherweise müssen m, t und M gewählt werden, während der Rest der Parameter fest ist. Für letztere nehme ich für die Szenarios die Beispiele, die bei Einführung der Notation erwähnt wurden.

In allen Szenarios werden zunächst (2') und (2'') in konservativer Weise abgeschätzt, um zu einfacheren Formeln zu gelangen. Beispielsweise ist u / r_{sen} immer klein verglichen mit a und wird deshalb generell weggelassen. (Auch $a - D_{tra}$ wird in der gleichen Größenordnung wie a liegen, anderenfalls war a überspezifiziert.)

Außerdem sind in den meisten Situationen zwei der drei Summanden der Summe $D_{MtM} + U / r_{tra} + 2 \bullet T$ klein verglichen mit dem dritten und werden deshalb weggelassen. Zusätzlich wird in (2') der Summand T in der Summe $t + T$ ignoriert.

Wenn die Gleichungen (1), (2), (2') bzw. (2'') mit dem speziellen Parameter x eines Szenarios als (1.x), (2.x), (2'.x) bzw. (2''.x) bezeichnet werden, führen diese Abschätzungen zu den Gleichungen (3'.x) bzw. (3''.x) als Folgerungen aus (2'.x) bzw. (2''.x). Sie haben die Form

$$m \bullet \max \{k, t\} \leq b \qquad (3'.x)$$

$$t + m \bullet k \leq a \qquad (3''.x)$$

Von beiden kann dieselbe obere Grenze

$$m \leq b / k \qquad (4.x)$$

für die Zahl der MIXe, die in Szenario x pro Informationseinheit verwendet werden können, hergeleitet werden.

Um eine obere Grenze für M, die Zahl aller MIXe, von (1) herleiten zu können, muß zuerst eine für m•t aus Gleichung (3'.x) oder (3''.x) hergeleitet werden.

Von Gleichung (3'.x) wird $m \bullet t \leq b$ verwendet, so daß sich zusammen mit Gleichung (1) die Gleichung

$$M \leq 0{,}5 \bullet b \bullet r_{ev} \bullet N \qquad (5'.x)$$

ergibt, bei der die Werte von b und r_{ev} gegeben sind.

Im Falle einer Klasseneinteilung von MIXen, Synchronisation zwischen den Klassen und klassenkompatibler Folgen von MIXen, bei dem Forderung (3''.x) besteht, ist m•t maximal wenn $t + m \bullet k = b$ ist, woraus $m \bullet t = m \bullet (b - m \bullet k)$ folgt. Diese Funktion in m hat ihr Maximum bei $m = b/(2 \bullet k)$. Deshalb ist m•t maximal für $m = b/(2 \bullet k)$ und $t = b - m \bullet k$, woraus $t = b/2$ folgt. Diese Gleichungen implizieren

$$m \bullet t \leq b^2 / (4 \bullet k).$$

Daher führen (1) und (3''.x) zusammen zu

$$M \leq 0{,}5 \bullet b^2 / (4 \bullet k) \bullet r_{ev} \bullet N \qquad (5''.x)$$

Szenario 1: Elektronische Post

Hier gilt a = 1000, so daß D_{tra} ignoriert und

b = 1000

gesetzt werden kann. Da es sich hier um ein verbindungsloses MIX-Schema handelt und die Verwendung des Kryptosystems RSA unterstellt wird, sind D_{MtM} und U/r_{tra} klein verglichen mit 2•T = 1/64. Deshalb wird

k = 1/64

gewählt. Dies ergibt

$$m \leq 64000 \qquad (4.1)$$

$$M \leq 0{,}5 \cdot 1000 \cdot 10^{-4} \cdot N = 0{,}05 \cdot N \qquad (5'.1)$$

$$M \leq 0{,}5 \cdot 1000^2 \cdot 64/4 \cdot 10^{-4} \cdot N = 800 \cdot N \qquad (5''.1)$$

Also können höchstens 64000 MIXe pro „Elektronischem Brief“ benutzt werden. Wenn die Teilnehmer beliebige Folgen von MIXen wählen, können nach (5'.1) höchstens 5% der Teilnehmerstationen als MIXe fungieren. Gleichung (5".1) liefert eine Bedingung, die schwächer als M≤N ist, so daß in diesem Fall alle Teilnehmerstationen als MIXe fungieren könnten, vgl. Abschnitt 2.5.2.7.

Diese Zahlen erwecken einen sehr positiven Eindruck. Aber bevor versucht wird, tatsächlich 64000 MIXe pro „Elektronischem Brief“ zu benutzen, sollte auch noch das früher diskutierte, bei den Formeln aber vernachlässigte Längenwachstum der „Elektronischem Briefe“ mit analysiert werden. Außerdem ist zu bedenken, wie leistungsfähig und folglich komplex die MIXe sein müßten – bisher wurde immer nur eine einzelne Informationseinheit betrachtet, wodurch implizit unterstellt wurde, daß Informationseinheiten parallel umcodiert werden.

Im folgenden werden Szenarios mit härteren Leistungsanforderungen der Kommunikationsdienste entwickelt.

Szenario 2: Telefongespräche mit Kanalvermittlung

Dies ist eigentlich eine Gruppe von Szenarios, da zwei Sorten von Ereignissen zu betrachten sind, nämlich Kanalaufbau und eigentlicher Informationsaustausch. Wenn Formeln nur für eine Sorte gelten, werden sie durch die Endungen „con“ für Verbindungsaufbau (connection set up) und „tra“ für Informationsaustausch (transmission) unterschieden.

Für den Verbindungsaufbau müssen – wie üblich – die Forderungen (1) und (2) erfüllt werden, d. h.

es müssen genug Kanäle gleichzeitig vermittelt werden (1.2con)

die Verzögerungszeit des Kanalaufbaus muß akzeptabel sein (2.2con)

Da es sich beim Kanalaufbau um ein verbindungsloses MIX-Schema handelt und die Verwendung des Kryptosystems RSA unterstellt wird, wird wie bei Szenario 1

k = 1/64

und hier

b = a = 10

gewählt. Damit ergibt sich für einen „mittleren“ Wert von $r_{ev} = 10^{-4}$

$$m \leq 640 \qquad (4.2con)$$

$$M \leq 0{,}5 \cdot 10 \cdot 10^{-4} \cdot N = 0{,}0005 \cdot N \qquad (5'.2con)$$

$$M \leq 0{,}5 \cdot 10^{2} \cdot 32/4 \cdot 10^{-4} \cdot N = 0{,}04 \cdot N \qquad (5''.2con)$$

Dies bedeutet, daß höchstens 0,05% bzw. 4% aller Teilnehmerstationen als MIXe fungieren können.

Die Forderungen bezüglich des eigentlichen Informationsaustausches sind schwächer als im verbindungslosen Fall: Wenn (1.2con) erfüllt ist, gibt es keine zusätzliche Forderung bezüglich des eigentlichen Informationsaustausches, da jeder MIX immer die einander entsprechenden Bits der zusammen vermittelten Kanäle, sobald sie eintreffen, umcodieren und ausgeben kann. Deshalb brauchen hierfür keine Zeitintervalle festgelegt und ggf. synchronisiert zu werden. So muß in diesem Fall nur die Forderung

$$m \cdot k \leq b \qquad (2.2tra)$$

erfüllt werden, wobei k und b ihre übliche Bedeutung haben.

Um k und b zu wählen, muß nun zwischen Kommunikationsnetzen verschiedener räumlicher Ausdehnung unterschieden werden, da die Übermittlungszeit bei Verwendung einer Stromchiffre statt RSA stärker ins Gewicht fällt.

Szenario 2A: Weltweites Kommunikationsnetz

Hier ist $D_{tra} = 0{,}1$ und $D_{MtM} = 0{,}001$. U / r_{tra} und T sind klein verglichen mit D_{MtM}. Deshalb wird

$$k = D_{MtM} = 0{,}001$$

und

$$b = a - D_{tra} = 0{,}1$$

gewählt. Damit ergibt sich

$$m \leq 100 \qquad (4.2Atra)$$

Diese Forderung ist stärker als die vom Verbindungsaufbau hergeleiteten. Sie bedeutet, daß jedes Telefongespräch höchstens 100 MIXe durchlaufen kann.

Szenario 2B: Lokales Kommunikationsnetz (Ortsbereich)

Hier sind D_{tra} und D_{MtM} kleiner als in Szenario 2A. Da $b \geq 0{,}1$ und auch im Ortsbereich bei über das Ortsnetz verstreuten MIXen sicherlich $k \leq 10^{-4}$ ist, ergibt dies keine stärkere Forderung als (4.2con), so daß höchstens 640 MIXe pro Ortsgespräch benutzt werden können.

Szenario 2C: Zusätzliches Vermitteln bedeutungsloser Kanäle

Wenn ein höherer Prozentsatz der Teilnehmerstationen als MIXe verwendet werden soll, kann dies durch zusätzliches Vermitteln bedeutungsloser, d. h. anderenfalls gar nicht benötigter Kanäle zwischen Teilnehmerstationen geschehen.

Formel (1) und folglich auch die Formeln (5'.x) und (5".x) zeigen, daß, um um den Faktor f mehr MIXe verwenden zu können, die Rate des betrachteten Ereignisses um den Faktor f erhöht werden muß.

Insbesondere muß, wenn alle Teilnehmerstationen als MIXe für einige Telefongespräche verwendet werden sollen und die Teilnehmer beliebige Folgen von MIXen wählen können sollen, die Vermittlungsrate von Kanälen mindestens um den Faktor 2000 erhöht werden.

Szenario 3: Telefongespräche mit Paketvermittlung

Hier werden die Umcodierungsschemata von Abschnitt 2.5.2 nicht nur wie in Szenario 2 für den Verbindungsaufbau, sondern auch für die eigentliche Nutzinformation, die paketweise übertragen wird, verwendet. Mindestens eine Entschlüsselung mit RSA wird also für jedes der zahllosen Pakete in jedem MIX benötigt. k wird wieder als 1/64 gewählt, wobei aber diesmal die akzeptable Verzögerungszeit $a = 0,2$ gilt. Für ein weltweites Kommunikationsnetz mit $D_{tra} = 0,1$ (Szenario 3A) impliziert dies $b = 0,1$ und deshalb

$$m \leq 6,4 \qquad (4.3A)$$

und für jedes (Szenario 3B), beispielsweise ein lokales Kommunikationsnetz (Ortsbereich), impliziert dies $b \leq 0,2$ und deshalb

$$m \leq 12,8 \qquad (4.3B)$$

Also können für jedes Telefongespräch höchstens 12 MIXe verwendet werden, und bei weltweiten Kommunikationsnetzen nur 6. Beides ist wesentlich schlechter als bei Kanalvermittlung.

Mit Forderung (1) wird sehr großzügig umgegangen, d. h. es wird ignoriert, daß ein Angreifer die Zeiten, wann Telefongespräche bei Sender und Empfänger beginnen, korrelieren kann, vgl. Abschnitt 3.2.2.1. Dann sind die Ereignisse, für die jeweils die Kommunikationsbeziehung geschützt werden muß, nur das Senden und Erhalten von Paketen. Ihre Rate ist

$$r_{ev} = r_{con} \cdot d \cdot r_{sen}/U,$$

wobei r_{con} die Rate des Verbindungsaufbau und d die erwartete Dauer eines Telefongesprächs ist. Also gilt

$$r_{ev} = 10^{-4} \cdot 180 \cdot 64000/1000 = 1,152.$$

Für ein weltweites Kommunikationsnetz gilt

$$M \leq 0,5 \cdot 0,1 \cdot 1,152 \cdot N = 0,0576 \cdot N \qquad (5'.3A)$$

und

$$M \leq 0,5 \cdot 0,1^2 \cdot 32/4 \cdot 1,152 \cdot N = 0,04608 \cdot N \qquad (5''.3A)$$

Offensichtlich waren die Abschätzungen, die zu (5'.x) führten, nicht sehr scharf: Natürlich gilt die von (5".x) hergeleitete Grenze auch für den Fall, daß beliebige Folgen von MIXen gewählt werden.

Für ein beliebiges Kommunikationsnetz muß für b lediglich statt 0,1 jeweils 0,2 eingesetzt werden. Dies ergibt

$$M \leq 0,1152 \cdot N \qquad (5'.3B)$$

$$M \leq 0,18432 \cdot N \qquad (5''.3B)$$

All diese Formeln erlauben anscheinend einem relativ großen Prozentsatz der Teilnehmerstationen, als MIXe zu fungieren, bzw. suggerieren, daß nicht allzuviele bedeutungslose Pakete nötig wären, wenn alle Teilnehmerstationen als MIXe fungieren sollten. In der Realität sollte aber der oben erwähnte Angriff durch Korrelation von Paketsenderaten bei Sender und Empfänger zumindest nicht ohne Gegenmaßnahmen riskiert werden. Eine Gegenmaßnahme wäre, Telefongespräche nur zu Zeitpunkten, deren Abstand größer als t ist, zu beginnen oder zu beenden. Im Gegensatz zur Kanalvermittlung müßte dies von den Teilnehmerstationen überwacht

werden. Wenn die Verzögerungszeit D_{MIX} konstant ist (was nicht allzu schwierig zu erreichen ist, wenn jeder MIX zu jedem Paket einen Zeitstempel hinzufügt, den der nächste MIX liest) und da alle Pakete dieselbe Zahl MIXe benutzen, erhalten alle Empfänger das erste Paket eines Telefongesprächs eine feste Zeit nach den Zeitpunkten. Diese feste Zeit variiert nur durch die unterschiedliche Verzögerungszeiten zwischen letzten MIXen und Empfängern. Entsprechendes gilt für das letzte Paket eines Telefongesprächs.

Die durch dieses Verfahrens garantierte Anonymität ist nicht leicht mit der durch Kanalvermittlung garantierten zu vergleichen (sofern ein MIX-Verfahren mit 6 bis 12 MIXen pro Kommunikationsbeziehung überhaupt als anonym zu bezeichnen ist), insbesondere wenn unterschiedliche Pakete eines Telefongesprächs unterschiedliche Folgen von MIXen durchlaufen: Einerseits ist es ein Vorteil, daß nur bei Sender bzw. Empfänger, nicht aber bei den MIXen Anfang und Ende eines Telefongesprächs erkannt werden kann. Andererseits kann der Angreifer die Länge von Telefongesprächen korrelieren und, falls unterschiedliche Pakete eines Telefongesprächs unterschiedliche Folgen von MIXen durchlaufen, können möglicherweise Alternativen, die bei einem Paket möglich waren, durch andere Pakete ausgeschlossen werden.

3.2.3 DC-Netz

Insbesondere in den Abschnitten 2.5.3.1 und 3.1.2 haben sich folgende Ziele für die Realisierung der Anonymität schaffenden (Teil-)Schicht des DC-Netzes ergeben:

Z1 Die *Verzögerungszeit*, d. h. die Zeit, die vom Senden eines Zeichens bis zum Empfang der Summe (modulo der Zeichenanzahl des Alphabets) aller gesendeten Zeichen vergeht, soll möglichst gering sein, da dies für alle Kommunikationsdienste günstig und manche Mehrfachzugriffsverfahren notwendig ist. Trivialerweise muß die Verzögerungszeit kleiner als das Minimum aller bei den abzuwickelnden Diensten zulässigen Verzögerungszeiten sein.
Hieraus folgt zumindest für ein diensteintegrierendes Netz die Forderung, daß die Verzögerungszeit des DC-Netzes kleiner als die vom Menschen als störend empfundene Reaktionszeit sein muß. Wie in den „Annahmen und Notation bezüglich der Verkehrslast“ im Abschnitt 3.2.2.4 erwähnt, liegt ein sinnvoller Wert der Verzögerungszeit meiner Meinung nach unter 0,2 s, während CCITT maximal 0,4 s erlaubt.

Z2 Soll der Mehrfachzugriffskanal DC-Netz mit einem Reservierungsschema vergeben werden, so sollte die *Zeichenanzahl des Alphabets* zumindest im Reservierungskanal *groß genug*, insbesondere größer 2 sein, vgl. Abschnitt 3.1.2.3.5.
Entsprechendes gilt für den in Abschnitt 3.1.2.3.2 beschriebenen Kollisionsauflösungsalgorithmus mit Mittelwertvergleich, der für viele Dienste das bestmögliche Mehrfachzugriffsverfahren darstellt.
Eine große Zeichenanzahl des zur Überlagerung verwendeten Alphabetes ist auch für eine möglichst effiziente Abwicklung von Konferenzschaltungen im eingeschränkten Sinn günstig, vgl. Abschnitt 3.1.2.6.

Z3 Der Teilnehmergemeinschaft soll für ihre Nutzdatenübertragung eine *hohe Bitrate* zur Verfügung gestellt werden.

Z4 Die Realisierung soll möglichst *geringen Aufwand* verursachen.

Die für die Erreichung dieser Ziele relevanten *Entwurfsentscheidungen*, nämlich Festlegung der Alphabetgröße, Implementierung der modulo-Addierer und Pseudozufallszahlengeneratoren, Wahl einer geeigneten Topologie für die globale Überlagerung und Synchronisation des Überlagerns von Informationseinheiten und Schlüsseln werden im folgenden in dieser Reihenfolge behandelt.

Festlegung der Alphabetgröße (betr. vor allem: Z1, Z2, Z4): Geringer Aufwand und geringe Verzögerungszeit einerseits sowie große Zeichenanzahl des zur Überlagerung verwendeten Alphabets andererseits sind offensichtlich nur leicht widersprüchliche Ziele, da bei geeigneter, d. h. zu der Codierung der Informationseinheiten, Schlüssel und Übertragung passender Wahl der Zeichenanzahl des zur Überlagerung verwendeten Alphabets Teile eines Alphabetzeichens von der Teilnehmerstation bereits ausgegeben werden können, *bevor* der Rest des Alphabetzeichens, etwa durch die Nutznachricht, bestimmt ist. Entsprechendes gilt für die globale Überlagerung: Sind nur die Anfänge aller zu überlagernden Zeichen eingetroffen, kann der Anfang des Überlagerungsergebnisses bereits ausgegeben werden. Wie solch eine passende Codierung und passende, schnelle und unaufwendige Addierer bzw. Subtrahierer (modulo der Zeichenanzahl des zur Überlagerung verwendeten Alphabets) gewählt bzw. realisiert werden können, sei kurz skizziert:

Wie allgemein üblich, erfolge die Codierung der Informationseinheiten, Schlüssel und die Übertragung binär. Dann ist es sehr zweckmäßig, die Zeichenanzahl des Alphabets als 2^l mit einer festen natürlichen Zahl l zu wählen und auch die Alphabetzeichen in der üblichen Weise binär zu codieren: das neutrale Element als 0, usw. Werden nun die Binärstellen der Alphabetzeichen in aufsteigender Wertigkeit übertragen, so genügt ein Volladdierer bzw. Vollsubtrahierer, ein UND-Gatter und beispielsweise ein Schieberegister der Länge l, um die Überlagerung zweier Bitströme binärstellenweise modulo 2^l durchzuführen: Im Schieberegister befindet sich nur an einer Stelle eine 0. Die Stelle, an der sich die 0 zu Beginn befindet, wird mittels des UND-Gatters mit dem Übertrag des Volladdierers bzw. -subtrahierers konjunktiv verknüpft. Der Ausgang des UND-Gatters dient als Übertrag des Volladdierers bzw. -subtrahierers. Dadurch wird erreicht, daß der Übertrag des Volladdierers bzw. -subtrahierers zu Beginn der binärstellenweisen Überlagerung eines Zeichens immer 0 ist.

Da Volladdierer bzw. -subtrahierer, UND-Gatter und Schieberegister genauso schnell wie Addierer modulo 2 (XOR-Gatter) arbeiten, ist die Verzögerungszeit des gerade skizzierten modulo 2^l arbeitenden DC-Netzes exakt genausogroß wie die eines modulo 2 arbeitenden. Lediglich der Aufwand der Addierer bzw. Subtrahierer wächst linear mit l oder anders formuliert logarithmisch mit der Zeichenanzahl des zur Überlagerung verwendeten Alphabets. Da die Schaltungskomplexität zur Überlagerung für realistische Werte von l (z. B. dürfte immer $l \leq 32$ gelten) immer um Größenordnungen kleiner ist als die zur Erzeugung von kryptographisch starken Pseudozufallsbit- bzw. -zahlenfolgen (vgl. Abschnitt 2.2.2.3) und da die Annahme optimal kurzer Verzögerungszeit für das einzige, ein modulo 2 arbeitendes DC-Netz benötigende (in Abschnitt 3.1.2.3.6 als letztes geschilderte) Mehrfachzugriffsverfahren für realistische Bitraten unrealistisch ist, gibt es aus meiner Sicht keinen wirklichen Grund, ein modulo 2 arbeitendes DC-Netz zu errichten. Daß die Annahme optimal kurzer Verzögerungszeiten für realistische Bitraten unrealistisch ist, sei durch folgendes Beispiel verdeutlicht: Angenommen das DC-Netz habe nur die Bandbreite 64000 bit/s und das Übertragungsmedium habe die Signalaus-

breitungsgeschwindigkeit 200000 km/s, so kann ein DC-Netz mit optimal kurzer Verzögerungszeit allein aufgrund der Signalausbreitungsgeschwindigkeit nur einen Durchmesser von maximal 3,125 km haben. Nichtoptimale Leitungsführung etc. erlaubt nur einen wesentlich geringeren Durchmesser.

Auch eine Kombination eines im wesentlichen Teil seiner Bandbreite modulo 2 und einem kleinen, zur Reservierung verwendeten Teil modulo 2^l arbeitenden DC-Netzes erscheint nicht sehr sinnvoll, da hierbei in einer frühen Phase der Errichtung eines DC-Netzes ohne Not eine weitreichende und die Entwurfskomplexität der höheren Schichten vermutlich steigernde Entscheidung über das Verhältnis der Bandbreiten getroffen werden müßte.

Implementierung der modulo-Addierer (betr. vor allem: Z1, Z4): Da – wie bei der Festlegung der Alphabetgröße schon gezeigt – modulo-Addierer für alle in Betracht kommenden Alphabetgrößen mit geringem Aufwand so realisiert werden können, daß sie mit der technologieabhängigen minimalen Gatterverzögerungszeit als Verzögerungszeit des modulo-Addierers auskommen, kann jeder modulo-Addierer den gesamten Bitstrom verarbeiten, so daß keine Überlegungen bezüglich Parallelarbeit von modulo-Addierern angestellt zu werden brauchen.

Umgekehrt erscheint es bei Anschluß jeder Teilnehmerstation an mehrere DC-Netze aufwandsmäßig nicht lohnend, vorhandene modulo-Addierer mittels Multiplexern für mehrere der DC-Netze zu verwenden, da Multiplexer nicht wesentlich geringeren Aufwand als die beschriebenen modulo-Addierer verursachen. In Abschnitt 5.4 wird außerdem noch ausführlich dargestellt, daß ein (möglichst weitgehender) Verzicht auf gemeinsame Teile einen gleichzeitigen Ausfall mehrerer DC-Netze unwahrscheinlicher macht und deshalb wünschenswert ist.

Implementierung der Pseudozufallszahlengeneratoren (betr. vor allem: Z3, Z4): Da die Generierung von kryptographisch starken Pseudozufallsbit- bzw. -zahlenfolgen heutzutage für jedes DC-Netz nennenswerter Übertragungsrate nötig (vgl. Abschnitt 2.2.2.3), aber wesentlich langsamer als ihre Überlagerung und Übertragung ist, müssen ggf. mehrere Pseudozufallszahlengeneratoren parallel betrieben und ihre Ausgaben über einen Multiplexer zu einem um ihre Anzahl schnelleren Bitstrom verschachtelt werden.

Weder der Entwurf noch die Implementierung der Pseudozufallszahlengeneratoren muß innerhalb des DC-Netzes einheitlich sein. Theoretisch können sich je zwei Teilnehmer auf den Entwurf eines Pseudozufallszahlengenerators einigen, sich zwei gleichschnelle (anderenfalls muß die schnellere langsamer arbeiten) Implementierungen beschaffen und brauchen dann nur noch einen gemeinsamen und geheimen Startwert sowie möglicherweise einen öffentlich bekannten genauen Zeitpunkt zum synchronisierten Überlagerungsbeginn ihres Schlüssels. Der Vorteil dieser völlig dezentralen Auswahl von Pseudozufallszahlengeneratoren ist, daß sicherere und leistungsfähigere Pseudozufallszahlengeneratoren nach und nach im DC-Netz eingesetzt werden und vermutlich eine große Vielzahl angeboten wird, so daß es „nicht so schlimm ist“, wenn manche gebrochen werden sollten. Der Nachteil ist offensichtlich: ein Markt funktioniert nur dann gut, wenn der Konsument die Qualität der Waren (ggf. mit Hilfe von Experten) preiswert beurteilen kann. In Abschnitt 2.2.2.2 habe ich meine Skepsis gegenüber den heutzutage auf dem Markt angebotenen, größtenteils nach „geheimgehaltenen“ Algorithmen arbeitenden Kryptosystemen, die jeweils nur von (wenn die Geheimhaltung geklappt haben sollte) wenigen, größtenteils namentlich nicht bekannten „Experten“ analysiert wurden, bereits ausgedrückt.

Ebenso habe ich in den Abschnitten 2.2.2.3 (sowie dem Anhang) und 2.2.2.4 einige Vorschläge zur und Begründungen für eine Normung unterbreitet, die im Falle des DC-Netzes den kurzfristigen Austausch von Schlüsseln zwischen beliebigen Teilnehmern und damit eine flexiblere und gezieltere Gestaltung [Cha3_85, Chau_88] des Schlüsselaustauschs erlaubt. Außerdem werden durch die Verwendung standardisierter Implementierungen manche der in Kapitel 5 und 7 diskutierten Zuverlässigkeitsprobleme leichter lösbar.

Der heutzutage noch hohe Aufwand kryptographisch starker Pseudozufallszahlengeneratoren kann es für DC-Netze hoher Bandbreite erforderlich machen, bezüglich der kryptographischen Stärke der Pseudozufallszahlenerzeugung Kompromisse einzugehen. Diese können in separater oder kombinierter Anwendung der Maßnahmen bestehen, daß

- Teilnehmerstationen nur sehr wenige Schlüssel austauschen, daß
- manche Schlüssel mit effizienteren (und ggf. kryptographisch schwächeren) Pseudozufallszahlengeneratoren erzeugt werden oder daß
- ein Teil der Bandbreite mit schwächer erzeugten Schlüsseln überlagert wird.

Durch letzteres entstünde in jedem Teil der Bandbreite ein separates DC-Netz, wobei die Anonymität der Sender in den verschiedenen DC-Netzen unterschiedlich wäre, und – wie in Abschnitt 4.2 diskutiert – für verschieden sensitive Kommunikation verwendet werden könnte. Zu einem späteren Zeitpunkt könnten starke Pseudozufallszahlengeneratoren zusätzlich zu den effizienteren (und ggf. kryptographisch schwächeren) nachgerüstet werden.

Wahl einer geeigneten Topologie für die globale Überlagerung (betr. vor allem: Z1): Die Verzögerungszeit eines DC-Netzes setzt sich aus den für die Übertragung und Überlagerung benötigten Zeiten zusammen. Deshalb sind sowohl die *Übertragungs*- als auch die *Überlagerungstopologie* in aufeinander abgestimmter Weise so zu wählen, daß die Summe aller Verzögerungszeiten und damit die Verzögerungszeit des DC-Netzes möglichst gering ist.

Bei der Überlagerungstopologie (und auch bei der Übertragungstopologie, vgl. Abschnitt 3.3.3) gibt es zwei Extremfälle:

1. Die Zeichen werden in einem Ring von Teilnehmerstation zu Teilnehmerstation weitergereicht. Da das Überlagern in jeder Teilnehmerstation mindestens eine Gatterverzögerungszeit dauert, wächst daher die durch Überlagerung verursachte Verzögerungszeit bei m Teilnehmerstationen mit $O(m)$, d. h. mindestens proportional zu m.
2. Die Zeichen werden zu einer zentralen Station (entsprechend einer heutigen Vermittlungszentrale) übertragen und dort überlagert, wobei, wie in Bild 46 gezeigt, die durch Überlagerung verursachte Verzögerungszeit bei m Teilnehmerstationen für Gatter mit begrenzt vielen Eingängen und begrenzter Treiberleistung mit $O(\log(m))$, d. h. mindestens proportional zum Logarithmus von m wächst. Dieses geringe Wachstum bleibt erhalten, wenn die Überlagerung dezentral, aber weiterhin baumförmig geschieht, so daß für die globale Überlagerung nicht nur eine stern-, sondern auch eine baumförmige Topologie geeignet ist.

   Bei Überlagerung modulo 2^l ist, wie oben unter „Festlegung der Alphabetgröße“ beschrieben, ein etwa durch ein Schieberegister realisierbarer Zähler modulo l zur Unterdrückung des Überlaufs an den Zeichengrenzen nötig. Dieser Zähler braucht bei zentraler Realisierung der baumförmigen Überlagerung nur einmal vorhanden zu sein, da er

alle Volladdierer steuern kann, während er bei dezentraler Realisierung natürlich an jeder Überlagerungsstelle vorhanden sein muß.

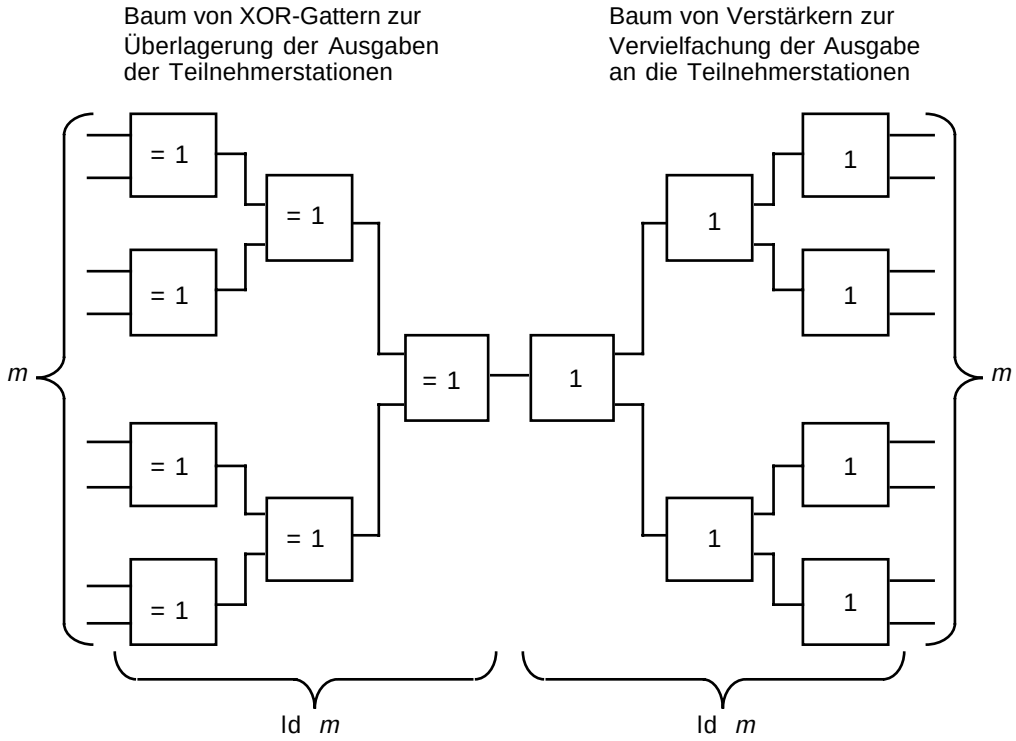


Bild 46: Verzögerungszeitminimale Überlagerungstopologie für Gatter mit 2 Eingängen und der Treiberleistung 2 am Beispiel binären überlagernden Sendens

Für diese Überlagerungstopologien geeignete Übertragungstopologien sowie das Wachstum der Summe aller Verzögerungszeiten und damit die Verzögerungszeit des DC-Netzes werden in Abschnitt 3.3.3 ausführlich behandelt.

Synchronisation des Überlagerns von Informationseinheiten und Schlüsseln (betr. vor allem: Z3, Z4): Wie schon mehrmals betont, müssen Informationseinheiten und Schlüssel synchronisiert überlagert werden. Geht die Synchronisation auch nur zwischen einem Paar paarweise ausgetauschter Schlüssel verloren, so können auf dem betroffenen DC-Netz keinerlei Informationseinheiten mehr erfolgreich übertragen werden. Die dann zu ergreifenden Maßnahmen werden in Abschnitt 5.4 behandelt.

Wenn das Übertragungsnetz, wie etwa für das ISDN geplant, in globaler Weise synchron arbeitet, kann diese Synchronität des Übertragungsnetzes auch für eine Synchronität des Überlagerns verwendet werden. Nun sind aber beispielsweise die Bitraten im geplanten ISDN klein verglichen mit der eines DC-Netzes vergleichbarer Nutzleistung. Ebenso ist die Rate akzeptabler Synchronisationsfehler im geplanten ISDN hoch verglichen mit einem DC-Netz vergleichbarer Zuverlässigkeit. Zusätzliche Maßnahmen scheinen also im allgemeinen Fall unumgänglich zu

sein, während in speziellen Fällen, beispielsweise bei Implementierung einer dezentralen ringförmigen Überlagerungstopologie auf einem ringförmigen Übertragungsnetz hoher Bitrate und Zuverlässigkeit (vgl. Abschnitt 3.3.3) alle Synchronisationsprobleme der Überlagerung in trivialer Weise lösbar sind.

Eine konzeptionell einfache, in der Realisierung aber sehr aufwendige Methode ist, Zeichenströme mit „Zeitstempeln“ (z. B. Sequenznummern) zu versehen und vor der globalen Überlagerung zu Puffern sowie bezüglich der Puffer die in Rechnernetzen üblichen Flußregelungsmechanismen (flow control mechanisms) einzusetzen.

In der Realisierung weniger aufwendige Methoden können durch Ausnutzung spezieller Überlagerungs- und Übertragungstopologien erreicht werden. Ist die Übertragungstopologie des Verteilkanals des DC-Netzes hierarchisch und wird der Takt des Übertragungsnetzes von oben nach unten phasenstabil weitergegeben, so kann jede am Überlagern beteiligte Station ihren Sendetakt aus dem Takt des Verteilkanals herleiten. Tun dies alle Stationen in gleicher Weise, sind ihre Sendetakte phasenstabil. Ist die Überlagerungstopologie ebenfalls hierarchisch und sind die Verzögerungszeiten auf den zugehörigen Übertragungsstrecken konstant, so kann durch stationsindividuelle Wahl der Phasenlage des Sendetaktes zum (Empfangs-)Takt des Verteilkanals des DC-Netzes erreicht werden, daß alle gesendeten Zeichenfolgen das hierarchische Überlagerungsnetz synchron durchlaufen.

3.2.4 RING-Netz

Insbesondere in den Abschnitten 2.5.3.2.1 und 3.1.4 haben sich folgende Ziele für die Realisierung der Anonymität schaffenden Schichten des RING-Netzes ergeben (Z1, Z3 und Z4 sind inhaltlich identisch mit denen beim DC-Netz):

- Z1 Die *Verzögerungszeit*, d. h. die Zeit, die vom Senden bis zum Empfang eines Zeichens vergeht, soll möglichst gering sein, da dies für alle Kommunikationsdienste günstig ist. Trivialerweise muß die Verzögerungszeit kleiner als das Minimum aller bei den abzuwickelnden Diensten zulässigen Verzögerungszeiten sein.
  Hieraus folgt zumindest für ein diensteintegrierendes Netz die Forderung, daß die Verzögerungszeit des RING-Netzes kleiner als die vom Menschen als störend empfundene Reaktionszeit sein muß. Wie in den „Annahmen und Notation bezüglich der Verkehrslast“ im Abschnitt 3.2.2.4 erwähnt, liegt ein sinnvoller Wert der Verzögerungszeit meiner Meinung nach unter 0,2 s, während CCITT maximal 0,4 s erlaubt.
- Z2 *Signale* müssen im Sinne von Abschnitt 2.5.3.2 *digital regeneriert* werden.
- Z3 Der Teilnehmergemeinschaft soll für ihre Nutzdatenübertragung eine *hohe Bitrate* zur Verfügung gestellt werden.
- Z4 Die Realisierung soll möglichst *geringen Aufwand* verursachen.

Die für die Erreichung dieser Ziele relevanten *Entwurfsentscheidungen*, nämlich Verzögerungszeit pro Station sowie Leitungsauswahl und Länge, Ausgabetaktgenerierung und Multiplexbildung werden im folgenden in dieser Reihenfolge behandelt.

Verzögerungszeit pro Station sowie Leitungsauswahl und Länge (betr. vor allem: Z1): Die Verzögerungszeit in jeder Station ist der Quotient aus der (möglicherweise nicht

ganzzahligen) Anzahl der Bitverzögerungen pro Station und der Bitrate des RING-Netzes. Wie bereits in Abschnitt 3.1.4.4 erwähnt, ist die Anzahl der Bitverzögerungen pro Station bei ökonomischer Dimensionierung sicher größer als 1/2, da erst in der „Mitte“ eines Bits dessen Wert feststeht (anderenfalls könnte die Bitrate ohne Probleme erhöht werden) und erst danach mit der Übertragung dieses Bitwertes begonnen werden kann. Durch Erhöhung der Bitrate des RING-Netzes wird die Verzögerungszeit jeder Station beliebig klein, wobei heutzutage hundert Mbit/s kein Problem darstellen und zukünftig etliche Gbit/s ebenfalls kein Problem darstellen dürften. Nimmt man die realistische Verzögerung von einem Bit und eine Bitrate von 1 Gbit/s an, so entspricht die Verzögerungzeit pro Station einer Weglänge von etwa 20 cm bei einer Signalausbreitungsgeschwindigkeit von etwa 200000 km/s in Kupfer- und Glasfaserkabeln. Da die Signalausbreitungsgeschwindigkeit nach oben durch die Lichtgeschwindigkeit im Vakuum $c_0 \approx$ 299792,5 km/s beschränkt ist, sind bei leistungsfähigen und geeignet entworfenen RING-Netzen Verzögerungszeiten pro Station klein bezüglich Signalausbreitungszeiten zwischen Stationen.

Da die Signalausbreitungsgeschwindigkeiten in den zur Diskussion stehenden Medien näherungsweise gleich und auch dort von der Frequenz, also auch der Bitrate weitgehend unabhängig sind [AlFi_77 Seite 572, 573], sind die Signalausbreitungszeiten zwischen Stationen über die Leitungsauswahl so gut wie nicht, über die Leitungsführung und die dadurch bedingte Leitungslänge aber erheblich zu beeinflussen. Eine minimale Leitungslänge wird durch direkte Verkabelung von benachbarten Stationen erreicht – also genau durch das, was in Abschnitt 2.5.3.2.1 aus Gründen der physischen Unbeobachtbarkeit angrenzender Leitungen gefordert wurde. In Mehrfamilienhäusern sollte der Ring die einzelnen Wohnungen direkt und nicht etwa über einen zentralen oder auch nur einige dezentrale Ring-Verkabelungs-Konzentratoren (ring wiring concentrators, vgl. [Stro_87]) verbinden.

Soll das RING-Netz als diensteintegrierendes Netz verwendet werden, d. h. eine Verzögerungszeit unter 0,2 s haben, so ergibt sich aus dem gerade Gesagten ein maximaler Ring-Umfang von 40000 km. Da bei einem diensteintegrierenden Netz benachbarte Teilnehmerstationen im Mittel sicherlich ganz erheblich weiter als 10 m voneinander entfernt sind, ergibt sich daraus eine maximale Teilnehmerstationenanzahl von 4 Millionen. Leider dürften Leistungs- (vgl. Kapitel 4) und Zuverlässigkeitsforderungen (vgl. Kapitel 5) an ein diensteintegrierendes Netz diese Grenze wesentlich nach unten verschieben.

Ausgabetaktgenerierung (betr. vor allem: Z2): Bezüglich der in Abschnitt 2.5.3.2 definierten, beim RING-Netz nötigen digitalen Signalregenerierung ist die Generierung des Ausgabetaktes der kritische Punkt. Während die maximale Ausgabespannung bzw. Lichtintensität etc. möglicherweise bei allen Stationen verschieden und möglicherweise auch noch von (Umgebungs-)Temperatur etc. abhängig sein mag, aber üblicherweise absolut nichts darüber aussagt, ob dies Bit von der sendenden Station direkt generiert oder von der vorherigen weitergeleitet wird, ist dies bezüglich der Ausgabetaktgenerierung bei der weitverbreitetsten Ringimplementierung gemäß ECMA-89 bzw. ANSI/IEEE Std 802.5-1985, seit 1986 ISO international standard IS 8802/5 nicht der Fall [Pfi1_85 Seite 31]:

In [ECMA89_85 Kapitel 6.4 und 6.5] wird vorgeschrieben, daß nur die amtierende Überwachungsstation (active monitor) ihren Ausgabetakt autonom generiert und alle anderen Stationen ihren Ausgabetakt kontinuierlich regeln, um in Phase mit ihrem Eingabetakt zu bleiben. Da

dieser Eingabetakt aber in einer Weise gewonnen wird, daß sein Verlauf nicht nur von dem Ausgabetakt der vorherigen Station, Eigenschaften der verbindenden Leitung und ggf. Signalstörungen, sondern auch von den empfangenen Bit*werten* abhängt (bit pattern sensitive timing jitter, [BCKK_83, KeMM_83, BaSa_85]) und dies in jeder Station (außer der amtierenden Überwachungsstation) der Fall ist, kann ein Angreifer, der eine Gruppe von *s* Stationen, die die amtierende Überwachungsstation nicht enthält, umzingelt hat, bei Vernachlässigung von Signalstörungen (z. B. Rauschen) den Sender einer Informationseinheit deterministisch identifizieren, indem er für alle Möglichkeiten die exakten Signalverläufe errechnet und mit den beobachteten vergleicht. Dies ist besonders einfach, da es für die in den Abschnitten 3.1.4.2 bis 3.1.4.3 als 2-anonym bewiesenen Ringzugriffsprotokolle durch verteiltes und anonymes Abfragen nur genau *s*-1 Möglichkeiten gibt. Bei dem in Abschnitt 3.1.4.4 als 2-anonym bewiesenen gibt es zwar erheblich mehr Möglichkeiten, jedoch ist auch bei ihm die Untersuchung der *s*-1 Möglichkeiten mit hoher Wahrscheinlichkeit erfolgreich. Alle diese Angriffe sind auch dann mit hoher Wahrscheinlichkeit erfolgreich, wenn es nur selten Signalstörungen oder nur solche geringer Amplitude gibt – genau die Ziele jedes (vernünftigen) Übertragungssystementwurfs.

Wie bereits in Abschnitt 2.5.3.2 angekündigt, kann die Forderung nach digitaler Signalregenerierung vergleichsweise einfach erfüllt werden, wie die folgenden 4 Möglichkeiten zeigen:

M1 Jede Station verwendet allein ihren Quarz-Oszillator zur Generierung des Ausgabetaktes. Der Eingabetakt wird wie üblich aus dem Eingabesignal gewonnen. Da Ein- und Ausgabetakt nur näherungsweise synchron (wenn auch mit sehr, sehr guter Näherung) und mit variabler Phase zueinander liegen, werden die empfangenen Bits mit dem Eingabetakt in einen elastischen Puffer (elastic buffer, [BCKK_83, KeMM_83, BaSa_85]) geschrieben und aus ihm mit dem Ausgabetakt ausgelesen – mit anderen Worten: alle Stationen verhalten sich in dieser Hinsicht wie die oben erwähnte amtierende Überwachungsstation. Ist der elastische Puffer leer bzw. voll, müssen Bits eingefügt oder weggelassen werden [KeMM_83 Seite 724].

M2 Wie M1, jedoch wird sichergestellt, daß Bits an speziellen Stellen eines Übertragungsrahmens bzw. Senderechtszeichens vorbeugend eingefügt oder weggelassen werden, so daß dadurch keine „transienten Übertragungsfehler“ generiert werden, die elastischen Puffer aber immer näherungsweise halb voll sind [Ross_86 Seite 13, Ross_87 Seite 32].

M3 Wie M1, jedoch wird statt dem Einfügen oder Weglassen von Bits der Ausgabetakt sehr langsam so geregelt, daß die elastischen Puffer immer näherungsweise halb voll sind [KeMM_83 Seite 725].

M4 Wie M1, jedoch erhält jede Station den Takt einer netzweiten Referenzuhr, wie dies sowieso geplant ist [McLi_85 Seite 341], und verwendet diesen Takt zur Herleitung ihres Ausgabetaktes [Pfi1_85 Seite 32].

Da M1, M2 und M3 das Problem zwar beliebig gut, nie aber vollständig lösen, da ein Angreifer bei ihnen statt einem kontinuierlich geregeltem Ausgabetakt nun das Einfügen und Weglassen von Bits bzw. eine langsame Regelung des Ausgabetaktes beobachten kann, empfehle ich, wo immer möglich, M4 zur Realisierung.

Multiplexbildung (betr. vor allem: Z3 und Z4): Für RING-Netze hoher Bitrate ist die Verwendung von Monomode-Glasfasern notwendig. Deren Bandbreite ist wiederum so groß,

daß die heute verfügbaren elektronischen Bauteile nur die Nutzung eines verschwindend kleinen Bruchteils erlauben, selbst wenn elektronische Bauteile höchster Geschwindigkeit und Kosten (z. B. GaAs) verwendet werden.

Liegt die benötigte Bitrate oberhalb des zur Zeit mit elektronischen Bauteilen preiswert Bewältigbaren, so kann die Bandbreite der Glasfaser mittels Wellenlängenmultiplex (WDM, [Unge_84 Seite 154] in verschiedene Kanäle aufgeteilt werden.

Ist dies nicht der Fall, so ergibt optischer Überlagerungsempfang (vgl. Abschnitt 3.2.1) oder Zeitmultiplex eine preiswertere und flexiblere Kanaleinteilung. In [BeEn_85] ist eine Zeitmultiplex verwendende, mit 5 Gbit/s arbeitende, durchgeführte Implementierung einer Ringstation beschrieben.

In jedem Fall sollte die Kanalaufteilung

- den Bedarf an Gattern höchster Schaltfrequenz minimieren, da diese Gatter üblicherweise höheren Aufwand (Anschaffungspreis, Energieverbrauch, Abwärme etc.) als Gatter niedrigerer Schaltfrequenz verursachen. Beispielsweise kann es bezüglich Aufwand günstiger sein, bei Ringen konstanter Kapazität Übertragungsrahmen (ÜR) nicht, wie in dem von Gunter Höckel [Höck_85, HöPf_85] entwickelten Modell, als Gruppe hintereinanderliegender Bits zu realisieren, sondern die Bits zu verschachteln: Dem 1. Bit des 1. ÜR folgt das 1. Bit des 2. ÜR, ... dem 1. Bit des letzten ÜR das 2. Bit des 1. ÜR usw. Dann steht jeder Station für die Ausführung des Ringzugriffsprotokolls in einzelnen ÜR mehr Zeit zur Verfügung. Dies ist insbesondere für das Füllen oder Kopieren des Inhalts eines ÜR günstig, da dann die Pufferspeicher der Stationen nicht mit der Bitrate des Ringes arbeiten müssen und deshalb entweder preiswert genügend groß dimensioniert werden können oder gar der Arbeitsspeicher von PCs als Pufferspeicher verwendet werden kann. Dies ist notwendig, da die Beweise in den Abschnitten 3.1.4.2 bis 3.1.4.5 davon ausgehen, daß jede Station innerhalb des betrachteten Ringkanals nicht nur einen beliebig großen Anteil senden *darf*, sondern auch *kann* – denn anderenfalls müßte sie das zeitlich nicht beschränkte Senderecht aufgrund fehlender Betriebsmittel abgeben, das tatsächlich ausgeführte Ringzugriffsprotokoll wäre eines mit zeitlich beschränktem Senderecht.
- die in Abschnitt 3.1.1 beschriebenen Kanaltypen mit jeweils geeigneten Bandbreiten ermöglichen. Es ist günstig, wenn die Bandbreite in Abhängigkeit der Verkehrslast dynamisch zwischen den verschiedenen Kanaltypen (und ggf. sogar noch einmal innerhalb der verschiedenen Kanaltypen) aufgeteilt werden kann [GöKü_85, Göld_85].

3.2.5 BAUM-Netz

Wie bereits in Abschnitt 2.5.3.2.2 erwähnt, ist ein Kollisionen verhinderndes Baumnetz (BAUM-Netz) ein aus pragmatischen Gründen, nämlich der Benutzung bereits vorhandener Breitbandkabel, wichtiges Beispiel für die Idee „Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung“. Bekanntlich sind die einzigen im Teilnehmeranschlußbereich bereits in nennenswerter Menge verlegten Breitbandkabel die der in vielen Ballungsgebieten existierenden Kabelfernsehnetze (die DBP nennt sie „Breitbandkabelverteilnetze“, im engl. Sprachraum spricht man von Common Antenna Television = CATV). Bei fast

allen Kabelfernsehnetzen handelt es sich technisch gesehen um baumförmige Koaxialkabelverteilnetze, die analoge Signale von der Wurzel des Baumes zu seinen Blättern (den Privathaushalten) verteilen.

Zur Ermöglichung von anonymem Senden und Verteilung muß ein kleiner Teil der Bandbreite der Koaxialkabelbaumnetze digitalisiert werden, und die Verstärker müssen zur Verstärkung in beiden Richtungen erweitert oder ausgetauscht werden. Beide Leistungsmerkmale sind im Bereich „Lokaler Netze“ seit langem üblich (vgl. WANGNET [Czaa_82, Elek_82]).

Für die Realisierung der Anonymität schaffenden Schichten des BAUM-Netzes gelten dieselben Ziele wie beim RING-Netz. Die für die Erreichung dieser Ziele relevanten *Entwurfsentscheidungen*, nämlich Verzögerungszeit pro Kollisionen verhinderndem Schalter, Ausgabetaktgenerierung der Kollisionen verhindernden Schalter und Umfang der Digitalisierung werden im folgenden in dieser Reihenfolge behandelt.

Verzögerungszeit pro Kollisionen verhindernder Schalter: Eine genügend geringe Verzögerungszeit des BAUM-Netzes wird bereits erreicht, wenn die Kollisionen verhindernden Schalter und Verstärker Verzögerungszeiten um oder unterhalb einer Millisekunde haben, da bei den üblichen Kabelfernsehnetzen auf dem Weg von der Wurzel zu den Blättern nur höchstens fünfmal verzweigt (und verstärkt) wird und die Weglänge von der Wurzel zum entferntesten Blatt deutlich unter 100 km liegt.

Ausgabetaktgenerierung der Kollisionen verhindernden Schalter: Die im Vergleich zum RING-Netz unkritische Verzögerungszeit pro Kollisionen verhinderndem Schalter erlaubt auch bei vergleichsweise niedrigen Bitraten alle in Abschnitt 3.2.4 beschriebenen Möglichkeiten M1, M2, M3 und M4 zur digitalen Signalregenerierung, da die bei M1, M2 und M3 benötigten elastischen Puffer großzügig dimensioniert werden können. Die vom Zugriffsverfahren „Kollisionen verhindernde Schalter“ verursachten kurzen und indeterministischen Übertragungspausen können von M2 besonders gut – nämlich zum Einfügen oder Weglassen von Bits – genutzt werden, so daß sich die Verwendung von M2 empfiehlt.

Umfang der Digitalisierung: Digitalisiert man 16 Mbit/s (wie bei WANGNET) in beiden Richtungen, so können selbst bei Verdopplung der heutigen „Telefon“-nutzung auf maximal 20% gleichzeitig 1250 Teilnehmer über ein teildigitalisiertes Koaxialkabelbaumnetz mit schmalbandigen Diensten versorgt werden. Da jede Teilnehmerstation potentiell auf jeden der (Telefon-)Kanäle zugreifen kann und im Durchschnitt erheblich weniger als 20% der Teilnehmer gleichzeitig „telefonieren“, können den größten Teil des Tages sogar etliche Teilnehmer je einige 64 kbit/s Kanäle gleichzeitig nutzen.

3.3 Ohne Rücksicht auf Anonymität realisierbare Schichten

In diesem Abschnitt wird zu den Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten die effiziente Realisierung der (Teil)Schichten beschrieben, die ohne Rücksicht auf Anonymität oder Unverkettbarkeit erfolgen kann. Gemäß Bild 30 in Abschnitt 2.6 gibt es solche (Teil)Schichten nur bei Verteilung, dem MIX- und DC-Netz.

Bei der Realisierung dieser (Teil)Schichten muß nicht nur auf genügende Leistungsfähigkeit, sondern auch auf hinreichende Zuverlässigkeit (ggf. auch unter Berücksichtigung von Sabotage) geachtet werden. Hierzu können beliebige Fehlertoleranz-Maßnahmen ergriffen werden, die schon hier angedeutet werden, da sich Kapitel 5 auf die Fehlertoleranz-Maßnahmen beschränken wird, die Einfluß auf Anonymität und Unverkettbarkeit haben.

3.3.1 Verteilung

Sollen Dienste mit nennenswerter Bandbreite pro Dienstteilnehmer für eine größere Zahl Teilnehmer oder hochauflösendes Fernsehen (HDTV, vgl. Abschnitte 1.1 und 2.3.1.1) verteilt werden, ist die Verwendung von Monomode-Glasfasern als Übertragungsleitungen notwendig.

Nachdem in Abschnitt 3.2.1 bereits die Vorteile von Wellenlängenmultiplex, vor allem aber der kohärenten optischen Nachrichtentechnik bei der Nutzung von Monomode-Glasfasern geschildert wurden, ist hier nur noch ein kurzer Hinweis auf *(analoge) optische Verstärkung* angebracht. Bei ihr können alle Signale eines relativ breiten (bezüglich des bei kohärenter optischer Nachrichtentechnik nötigen Kanalabstandes) Frequenzspektrums mit vergleichsweise sehr geringem Aufwand verstärkt werden [Baac_85 Seite 357]. Bei dieser Verstärkung findet keine digitale Signalregenerierung statt – sie ist bei wenigen Verstärkern hintereinander auch übertragungstechnisch überflüssig und zum Schutz des Empfängers ebenfalls.

Ist die Zuverlässigkeit des Verteilnetzes zu gering, so können auf diesen Schichten beliebige Fehlertoleranz-Maßnahmen ergriffen werden. Beispielsweise könnte jeder Teilnehmer mit mehreren, in verschiedenen Kabelkanälen verlegten Monomode-Glasfasern an verschiedene Verteilnetze angeschlossen werden.

3.3.2 MIX-Netz

Um die in Abschnitt 3.2.2.1 beschriebenen realen oder virtuellen Kanäle beim MIX-Netz schalten zu können, müssen auf den tieferen Schichten des Kommunikationsnetzes dann zwischen Teilnehmerstationen und MIXen sowie zwischen MIXen ebenfalls Verbindungen geschaltet werden, damit einerseits erkennbar ist, welche Bits zu welcher Verbindung gehören und ggf. kurze Verzögerungszeiten und/oder gleichmäßiger Informationsfluß und/oder Synchronisation des Umcodierens, Ausgebens und Übertragens garantiert werden können. Wie das einfache Kommunikationsnetzmodell in Abschnitt 3.2.2.4 gezeigt hat, ist insbesondere die durch die Gestaltung der gerade diskutierten Schichten festgelegte Verzögerungszeit zwischen MIXen

(D_{MtM}) kritisch: sie sollte – etwa durch direkte Verkabelung und hohe Bitrate zumindest zwischen MIXen (r_{tra}) – so gering wie möglich gehalten werden.

Ist es aus Gründen der Zuverlässigkeit wünschenswert, so können Teilnehmerstationen und MIXe sowie MIXe untereinander über mehrere unterschiedliche Leitungen (und ggf. Vermittlungseinrichtungen) verbunden werden.

3.3.3 Übertragungstopologie und Multiplexbildung beim DC-Netz

Die im folgenden diskutierte Wahl einer geeigneten Übertragungstopologie und Multiplexbildung beim DC-Netz hat zwar keine Auswirkung auf die Anonymitäts- und Unverkettbarkeitseigenschaften, aber umso gravierendere auf die Verzögerungszeit (Z1), die Bitrate (Z3), den Aufwand (Z4) und das Ausfallverhalten eines DC-Netzes.

Übertragungstopologie: Wie in Abschnitt 3.2.3 schon erwähnt, setzt sich die Verzögerungszeit eines DC-Netzes aus den für die Übertragung und Überlagerung benötigten Zeiten zusammen. Also müssen Überlagerungs- und Übertragungstopologie in aufeinander abgestimmter Weise günstig gewählt werden.

In [Cha3_85] schlägt David Chaum vor, binäres überlagerndes Senden auf einem physischen Ringnetz folgendermaßen zu implementieren (Bild 47):

> Jedes Bit einer Informationseinheit benötigt (etwa) zwei Ringumläufe: Im 1. Umlauf werden die lokalen Überlagerungsergebnisse der Stationen sukzessive global überlagert, indem jede Station ihr Eingabebit und ihr lokales Überlagerungsergebnis überlagert und das Ergebnis an die nächste Station sendet. Im 2. Umlauf wird das Ergebnis der globalen Überlagerung an alle Stationen verteilt. „Etwa“ bedeutet, daß in einem Ringnetz mit *m* Stationen nur 2*m*-2 Übertragungen von Station zu Station benötigt werden, da bereits die vorletzte Station des 1. Umlaufs das Ergebnis der globalen Überlagerung durch ihre globale Überlagerung erhält. Entsprechend ist es natürlich überflüssig, ihr und der nächsten Station das Ergebnis der globalen Überlagerung im 2. Umlauf nochmals mitzuteilen.

Verallgemeinertes überlagerndes Senden kann entsprechend implementiert werden.

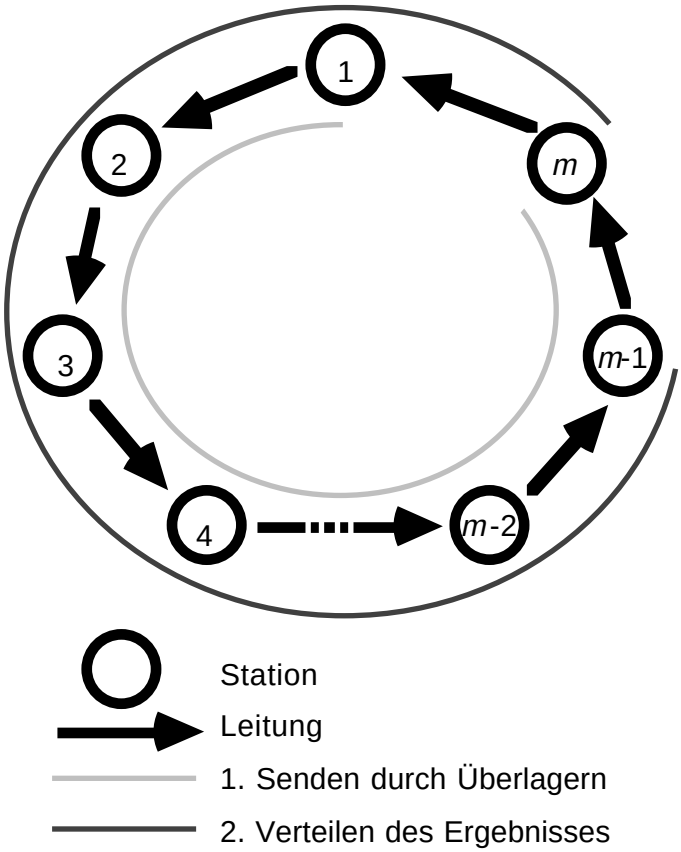


Bild 47: Implementierung von überlagerndem Senden auf einem Ringnetz

Diese Implementierung scheint sehr effizient zu sein, da sie – unter der Annahme gleichverteilten Verkehrs – den durchschnittlichen Übertragungsaufwand nur um einen Faktor etwas kleiner als 4 gegenüber einem üblichen Ringzugriffsprotokoll, bei dem der Empfänger die Informationseinheit vom Ring entfernt, erhöht, während dieser Faktor bei Stern- oder Baum-Netzen die Zahl der Stationen ist. Da aber die resultierende Übertragungsrate auf allen Leitungen jeweils gleich ist, können Implementierungen auf Stern- oder Baum-Netzen trotzdem besser sein, wenn ihre Verzögerungszeit geringer ist. Die folgenden Überlegungen zeigen, daß letzteres der Fall ist.

Bei David Chaums Implementierungsvorschlag wird der Ring sowohl als Überlagerungs- als auch als Übertragungstopologie verwendet. Wie in Abschnitt 3.2.3 erläutert, ist der Ring die – bezüglich Verzögerungszeit – denkbar schlechteste Überlagerungstopologie, da die durch Überlagerung verursachte Verzögerungszeit bei m Teilnehmerstationen proportional zu m statt proportional zu $\log(m)$ wächst. Nun ist dies noch nicht sehr schlimm, da durch Erhöhung der Bitrate des DC-Netzes (oder zumindest der Schaltgeschwindigkeit der modulo-Addierer) die Proportionalitäts-Konstante fast beliebig klein gewählt werden kann.

Ähnliches ist leider bezüglich der Übertragungstopologie nicht möglich, da die Signalausbreitungsgeschwindigkeit durch die Lichtgeschwindigkeit im Vakuum beschränkt ist.

Die durch Übertragung verursachte Verzögerungszeit bei *m* Teilnehmerstationen im Abstand *a* ist bei einem Ring proportional zu $a \bullet m$ statt wie bei Stern oder Baum typischerweise proportional zu $a \bullet \sqrt{m}$, wobei proportional zu $a \bullet \sqrt[3]{m}$ oder $a \bullet m$ die Grenzfälle darstellen:

Die durch Übertragung verursachte Verzögerungszeit ist proportional zum Durchmesser des Netzes, welcher das Maximum über die Abstände aller geordneten Paare von Netzstationen ist. Wenn sich in jedem Würfel der Kantenlänge *a* höchstens eine Teilnehmerstation befindet, wobei $a \geq 2$ m eine sehr vernünftige Annahme sein dürfte, ist der Durchmesser des vollvermaschten und damit jedes Netzes mit *m* Teilnehmerstationen mindestens $a \bullet \sqrt[3]{m}$. Sind die Würfel in einer Ebene angeordnet, was für diesen Zweck ein geeignetes Modell der Erdoberfläche und damit für ländliche Gebiete ist, so ist der Durchmesser jedes Netzes mit *m* Teilnehmerstationen mindestens $a \bullet \sqrt{m}$. Da geeignet entworfene hierarchische Netze einen Durchmesser nahe eines vollvermaschten Netzes haben, ist $a \bullet \sqrt{m}$ ein typischer Wert. Sind allerdings alle Teilnehmerstationen entlang einer Geraden angeordnet, so ist der beste erreichbare Durchmesser $a \bullet m$.

Da schon heute die Übertragungszeiten groß verglichen mit den Überlagerungszeiten sind (beispielsweise bewegt sich Licht in einer Glasfaser nur 4 cm in der Zeit, die bei der in Abschnitt 3.2.4 beschriebenen 5 Gbit/s Ringstation zum Empfang jedes Bits zur Verfügung steht), kann durch geeignete Wahl von Überlagerungs- und Übertragungstopologie also im wesentlichen ein Faktor von etwa $\sqrt{m}$ gewonnen werden. Wie die kleine Modellrechnung in Abschnitt 3.2.4, die eine maximale Teilnehmerstationenanzahl von 4 Millionen in jedem ringförmigen diensteintegrierenden Netz allein aufgrund der Signalverzögerungszeit ergab (woraus sich maximal 2 Millionen in jedem ringförmigen DC-Netz ergibt), zeigt, ist dieser Gewinn bei großen Kommunikationsnetzen wesentlich.

Multiplexbildung: Wie in Abschnitt 3.2.4 beim RING-Netz schon erwähnt, ist auch für DC-Netze hoher Bitrate eine Monomode-Glasfaser notwendig, deren Bandbreite durch geeignete Multiplexbildung preiswert zu nutzen ist.

Ob verschiedene Kanäle im Sinne des Abschnitts 3.1.2.7 oder separate DC-Netze im Sinne von „Implementierung der Pseudozufallszahlengeneratoren“ in Abschnitt 3.2.3 dieselben Multiplexer, Synchronisationslogik und Glasfaser etc. nutzen, ist eine Kosten- und Zuverlässigkeitsfrage:

Wenn immer eine gemeinsame Nutzung ohne Mehraufwand vermieden werden kann, sollte dies zur Vermeidung eines gleichzeitigen Ausfalls mehrerer Kanäle oder DC-Netze getan werden, vgl. „Implementierung der modulo-Addierer“ in Abschnitt 3.2.3 und Abschnitt 5.4.

Wäre die resultierende Zuverlässigkeit trotzdem zu gering, so muß – auch unter Inkaufnahme von Mehraufwand – eine gemeinsame Nutzung vermieden werden. Ein Beispiel für letzteres wäre die Verlegung einer zweiten Monomode-Glasfaser auf einem anderen Weg, um ein Durchtrennen einer Glasfaser im Teilnehmeranschlußbereich durch Heimwerker, Handwerker oder Baggerführer ohne Totalausfall der Kommunikationsdienste für diesen Teilnehmer zu tolerieren.