Netzwerktechnologien
3 VO

Univ.-Prof. Dr. Helmut Hlavacs
helmut.hlavacs@univie.ac.at

Dr. Ivan Gojmerac
gojmerac@ftw.at

Bachelorstudium Medieninformatik
SS 2012

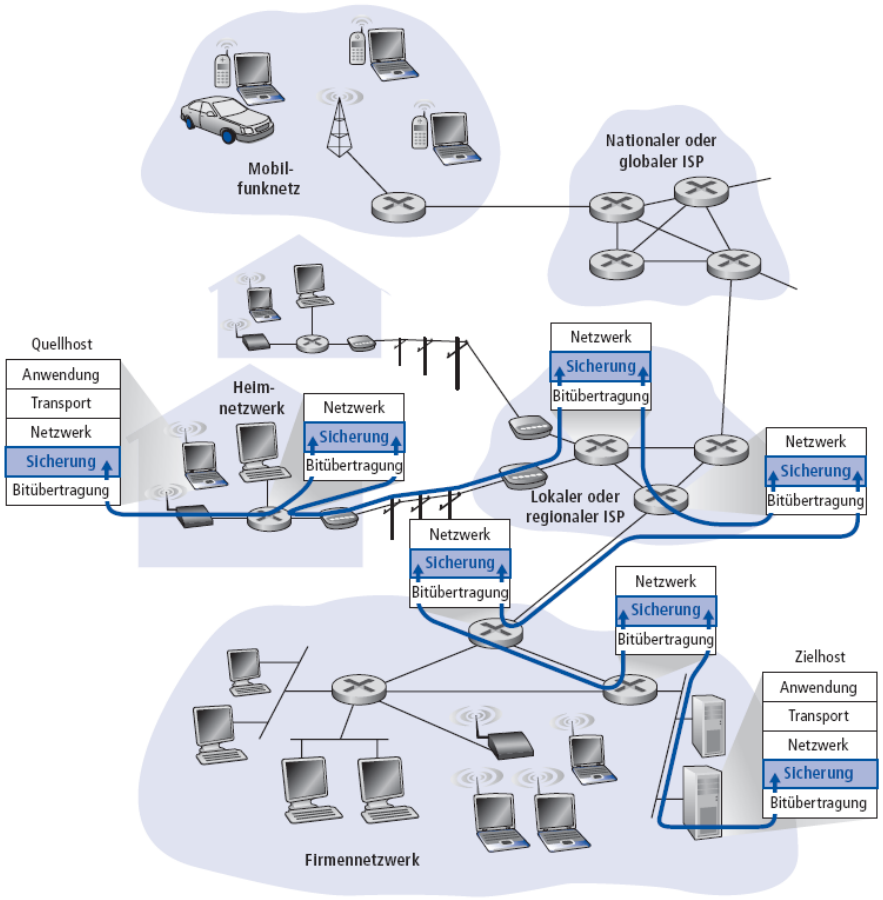
Kapitel 5 – Sicherungsschicht und lokale Netzwerke

5.1 Sicherungsschicht - Einleitung

Verwendete Terminologie:

- Hosts und Router sind **Knoten**
- Kommunikationskanäle auf dem Weg vom Sender zum Empfänger sind **Links**
  - Kabelgebundene Links
  - Drahtlose Links
  - LANs
- Ein Paket der Sicherungsschicht nennt man Rahmen (engl. **Frame**)
  - Ein Rahmen enthält üblicherweise ein Datagramm der Netzwerkschicht

Die **Sicherungsschicht** (link layer) hat die Aufgabe, Rahmen von einem Knoten über einen Link zu einem direkt benachbarten Knoten zu transportieren.



5.1 Sicherungsschicht - Einordnung

- Ein Datagramm wird von verschiedenen Protokollen der Sicherungsschicht über verschiedene Links transportiert:
  - *Beispiel:* Ethernet auf dem ersten Link, dann Frame Relay, dann IEEE 802.11 WLAN
- Jedes dieser Protokolle kann unterschiedliche Dienste anbieten
  - Diese Protokolle können z.B. zuverlässige oder nur unzuverlässige Übertragung anbieten

---

Analogie

- Reise von Princeton nach Lausanne
  - Taxi: Princeton zum JFK-Flughafen
  - Flugzeug: JFK-Flughafen nach Genf
  - Zug: Genf nach Lausanne
- Tourist = **Datagramm**
- Reiseabschnitt = **Link**
- Reisebüro = Routing-Protokoll
- Art des Transportes = **Protokoll der Sicherungsschicht**

5.1 Dienste der Sicherungsschicht

- Rahmenbildung und Zugriff auf den Link:
  - Verpacken eines Datagramms in einen Rahmen, Hinzufügen von Header und Trailer
  - Zugriff auf den Kanal (schwierig, wenn dieser von mehreren Knoten verwendet wird)
  - “MAC”-Adressen (Medium Access Control) werden im Header von Rahmen verwendet, um Sender und Empfänger zu kennzeichnen
    → **Verschieden von IP-Adressen!**

- Zuverlässige Datenübertragung zwischen benachbarten Knoten
  - Funktion ist bereits bekannt (Kapitel 3!)
  - Seltener Einsatz, wenn der Link sehr wenige Bitfehler verursacht (Glasfaser, Kupferkabel, usw.)
  - Drahtlose Links: hohe Bitfehlerrate

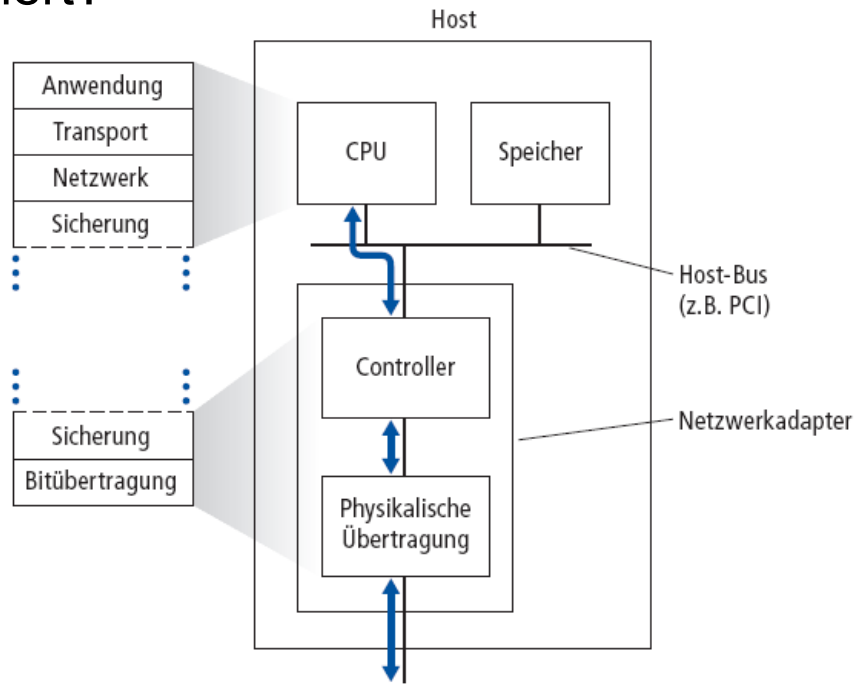
5.1 Dienste der Sicherungsschicht

- Flusskontrolle:
  - Anpassen der Sendegeschwindigkeit an den Empfänger
- Fehlererkennung:
  - Fehler entstehen beispielsweise durch Abschwächen des Signals auf der Leitung und durch Rauschen
  - Der Empfänger sollte Fehler erkennen können, dann:
    - Neuübertragung auslösen
    - oder Rahmen verwerfen
- Fehlerkorrektur:
  - Der Empfänger erkennt und korrigiert Bitfehler, ohne eine Neuübertragung anzufordern
- Halbduplex und Vollduplex:
  - Bei Halbduplex können die Knoten an beiden Enden der Leitung übertragen – jedoch nicht gleichzeitig

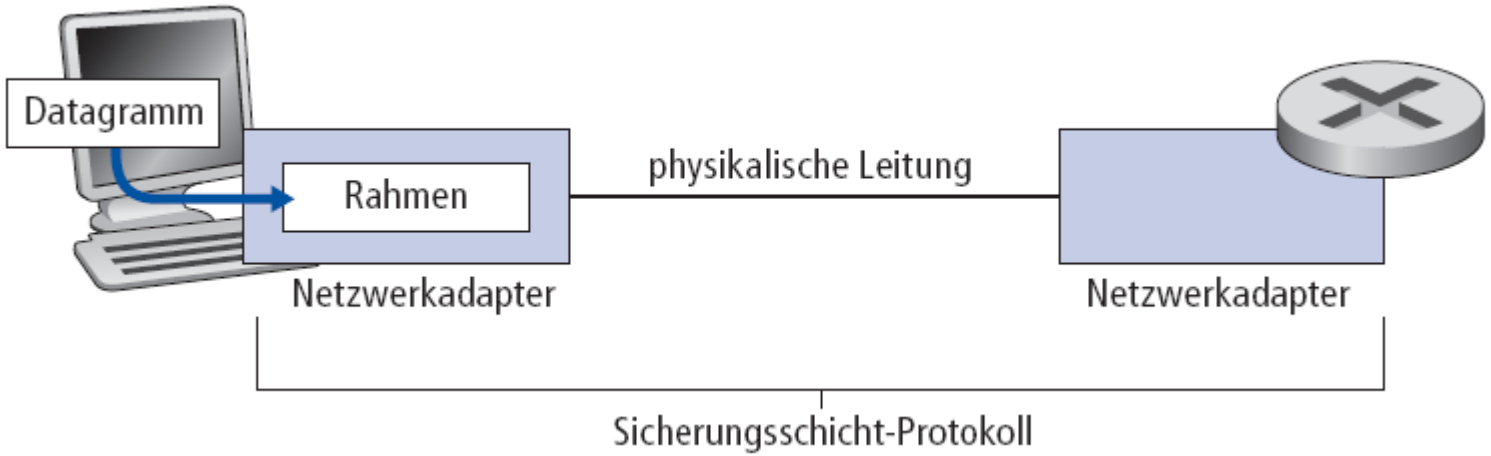
5.1 Sicherungsschicht - Einordnung

Wo ist die Sicherungsschicht implementiert?

- In jedem Host, in jedem Router
- Die Sicherungsschicht ist im Netzwerkadapter (Netzwerkkarte) implementiert
  - Ethernet-Netzwerkkarte, 802.11 WLAN-Karte
  - Enthält Sicherungsschicht und Physikalische Schicht
- An den Systembus des Hosts/Routers angeschlossen
- Kombination von Hardware, Software, Firmware



5.1 Kommunikation zwischen Netzwerkadaptern



Sender:

- Verpacken von Datagrammen in Rahmen
- Hinzufügen von Bits für die Fehlererkennung, die zuverlässige Datenübertragung, Flusskontrolle, usw.

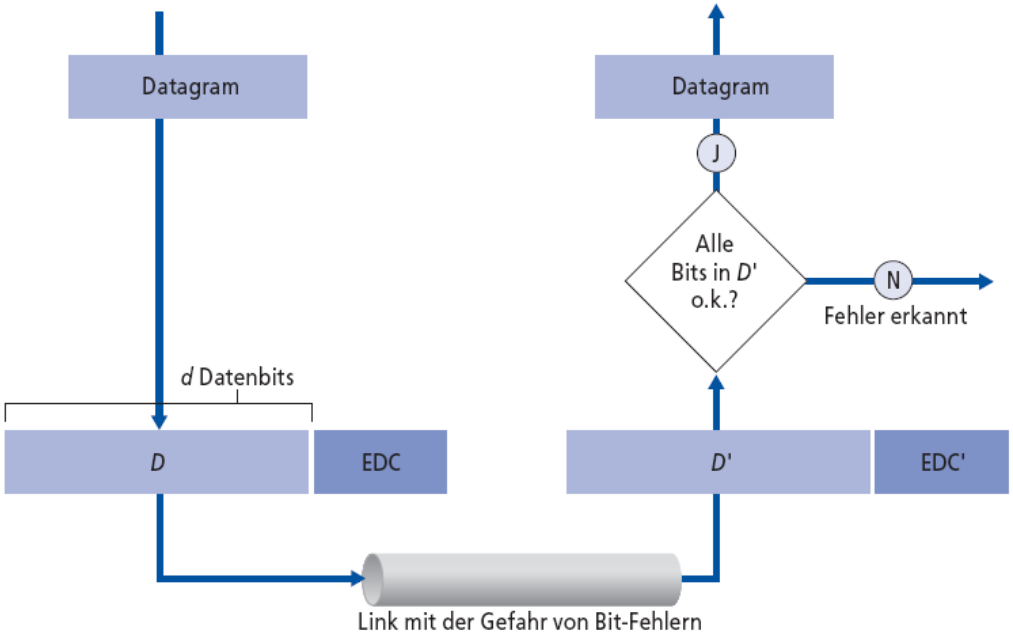
Empfänger

- Überprüfen auf Bitfehler, Flusskontrolle, usw.
- Extrahieren des Datagramms, Ausliefern an die Netzwerkschicht

5.2 Fehlererkennung

- **EDC** = Error Detection and Correction Bits (Redundanz)
- **D** = Daten, die durch EDC geschützt sind (kann die Header-Felder einschließen)

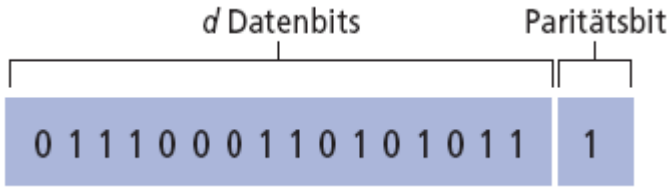
- Fehlererkennung ist nicht 100% zuverlässig!
  - Ein Sicherungsschichtprotokoll kann Fehler übersehen (*sehr selten!*)
  - Mehr EDC-Bits führen zu besseren Erkennungsraten



5.2 Paritätsprüfung

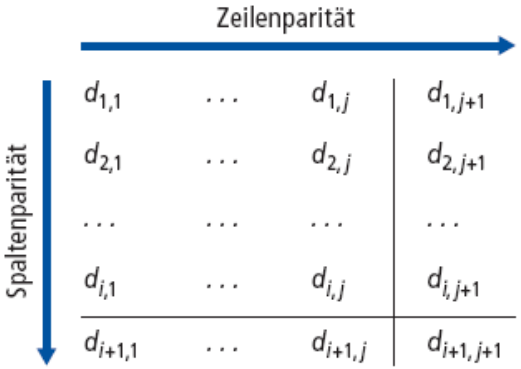
Ein-Bit-Parität:

Erkennt Ein-Bit-Fehler

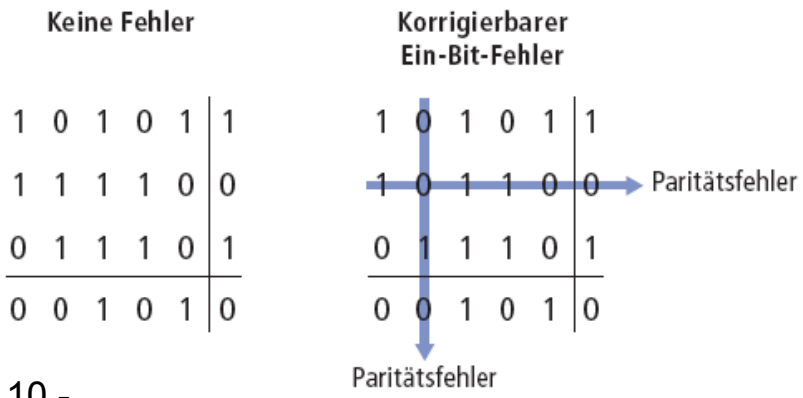


Zweidimensionale Parität:

Erkennt und korrigiert Ein-Bit-Fehler



Gerade Parität!



5.2 Internetprüfsumme

Ziel: Erkennen von Fehlern in übertragenen Segmenten auf der Transportschicht

Sender:

- Betrachte das Segment als eine Folgen von 16-Bit-Integerwerten
- Prüfsumme: Addition (im 1er Komplement) der Werte
- Sender schreibt das Ergebnis in das UDP-Prüfsummenfeld

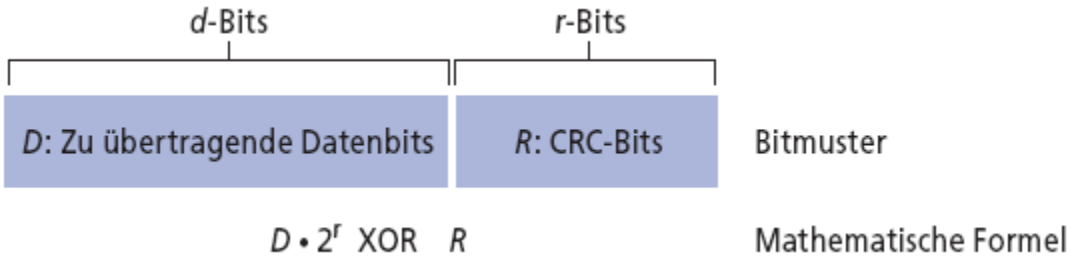
Empfänger:

- Berechne die Prüfsumme
- Passt diese zum Wert im Prüfsummenfeld:
  - Nein – Fehler erkannt
  - Ja – kein Fehler erkannt. Aber es könnten dennoch Fehler vorliegen!

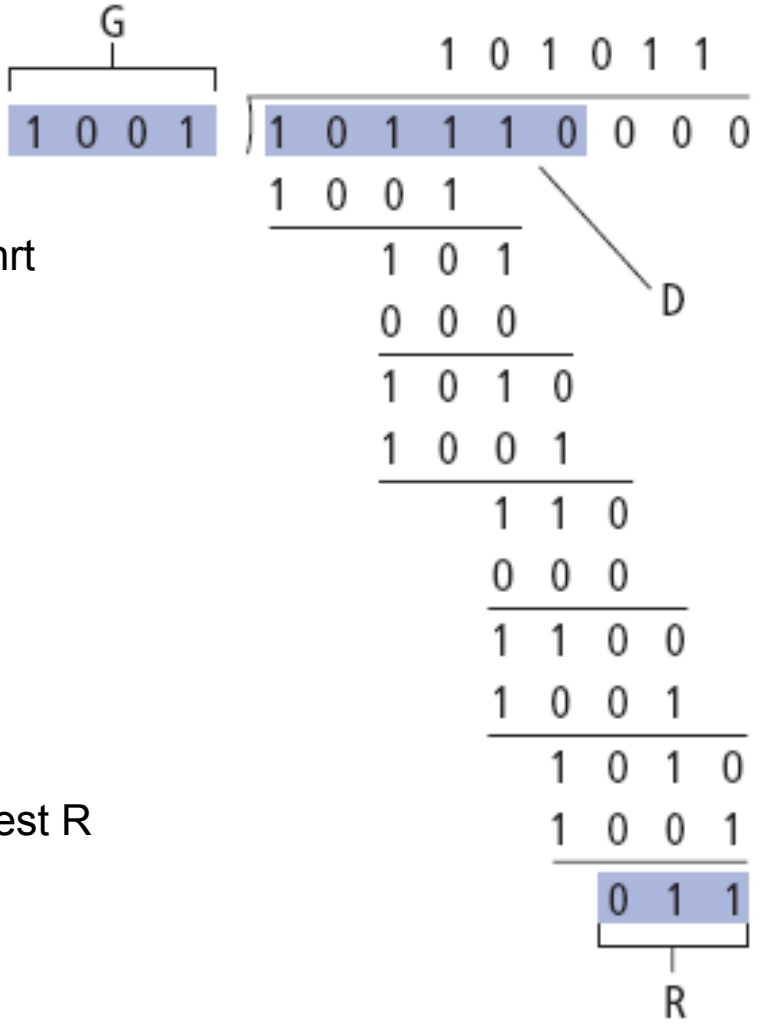
5.2 Bildung von Prüfsummen: Cyclic Redundancy Check (CRC)

- Betrachte die Datenbits (**D**) als eine binäre Zahl
- Wähle ein Bitmuster der Länge r+1 (Generator, **G**)
- Ziel: Wähle r CRC-Bits (**R**) so, dass gilt:
  - <D,R> ist modulo 2 durch G ohne Rest teilbar
  - Empfänger kennt G und teilt das empfangene <D',R'> durch G. Wenn es einen Rest gibt: Fehler erkannt!

  → Kann alle Burst-Fehler erkennen, die kürzer als r+1 Bit sind
- In der Praxis weit verbreitet (IEE 802.11 WLAN, ATM)



5.2 CRC Beispiel



- Vorbemerkung:
  - Alle Operationen werden modulo 2 durchgeführt
  - Addition und Subtraktion entsprechen der Verknüpfung mit XOR
  - Es gibt keinen Übertrag
- Es soll ein R gefunden werden:
  - $D \cdot 2^r$ XOR R = nG
- Dies ist äquivalent zu:
  - $D \cdot 2^r$ = nG XOR R
- Dies ist äquivalent zu:
  - Wenn wir $D \cdot 2^r$ durch G teilen, entspricht der Rest R

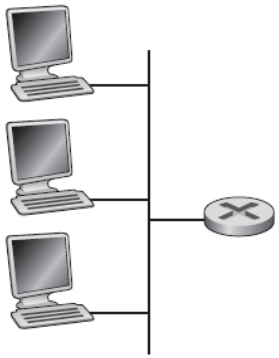
$$R = \text{Rest von } \left[\frac{D \cdot 2^r}{G}\right]$$

5.3 Links mit Mehrfachzugriff

Zwei Arten von “Links”:

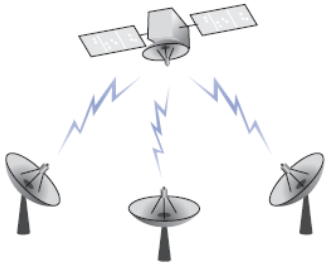
- **Punkt-zu-Punkt**
  - Einwahlverbindungen
  - Verbindung zwischen Ethernet Switch und Host
- **Broadcast** (gemeinsam verwendetes Medium)
  - Ursprüngliches Ethernet
  - Upstream bei HFC (Internetzugang über das Fernsehkabelnetz)
  - IEEE 802.11 WLAN

Gemeinsam genutzte Leitung
(z.B. Ethernet)

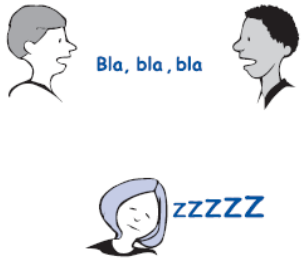


Gemeinsam genutzter Funkkanal
(z.B. WLAN)

Satellit



Cocktailparty



5.3 Protokolle für den Mehrfachzugriff

- Ein gemeinsam genutzter Broadcast-Kanal
- Mehrere gleichzeitige Übertragungen verschiedener Knoten:
  - **Kollision**, wenn ein Knoten mehrere Signale zur gleichen Zeit empfängt
  - Dadurch werden die Signale unbrauchbar

Protokolle für den Mehrfachzugriff (MAC-Protokolle)

- Verteilte Algorithmen, die bestimmen, wie sich die Knoten den Kanal teilen
- Bestimmen, wer wann senden darf
- Die dazu notwendige Kommunikation muss wiederum über den Broadcast-Kanal selbst abgewickelt werden
  → Kein zusätzlicher Kanal für die Koordination

5.3 Protokolle für den Mehrfachzugriff

Anforderungen an das perfekte Protokoll für den Mehrfachzugriff:

→ Gegeben: Ein Broadcast-Kanal mit R bps

1. Wenn nur ein Knoten übertragen möchte, dann kann er mit der Rate R senden
2. Wenn M Knoten übertragen möchten, dann kann jeder mit der Rate R/M senden
3. Dezentral:
   - Kein spezieller Knoten zur Koordination der Übertragungen
   - Keine Synchronisation von Uhren oder Zeitschlitzen
4. Einfach

5.3 Klassifikation von MAC-Verfahren

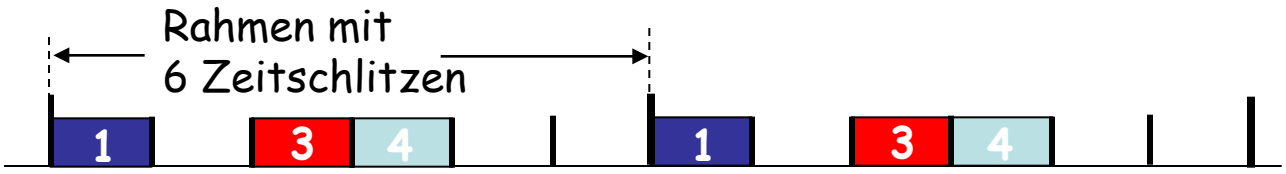
- Kanalaufteilungsprotokolle
  - Das Mediums wird in Subeinheiten zerlegt
  - Jeder Station wird eine Einheit zur exklusiven Benutzung zugeordnet
- Wahlfreier Zugriff (Random Access)
  - Datenrate wird nicht unterteilt
  - Stationen können wahlfrei auf den ganzen Kanal zugreifen
  - Dabei kann es zu Kollisionen kommen
  - Kollisionen müssen geeignet behandelt werden
- Abwechselnder Zugriff
  - Die Zugriffe der Stationen werden koordiniert, es darf abwechselnd gesendet werden
  - Kollisionen werden vermieden

5.3 Kanalaufteilung mittels TDMA

Time Division Multiple Access (**TDMA**, ~ Zeitmultiplexing)
→ Auf das Medium wird in Runden zugegriffen

- Jede Station bekommt einen festen Zeitschlitz zum Senden in jeder Runde
- Nicht verwendete Zeitschlitze gehen verloren

Beispiel: LAN mit 6 Stationen, 1,3,4 senden, 2,5,6 senden nicht:

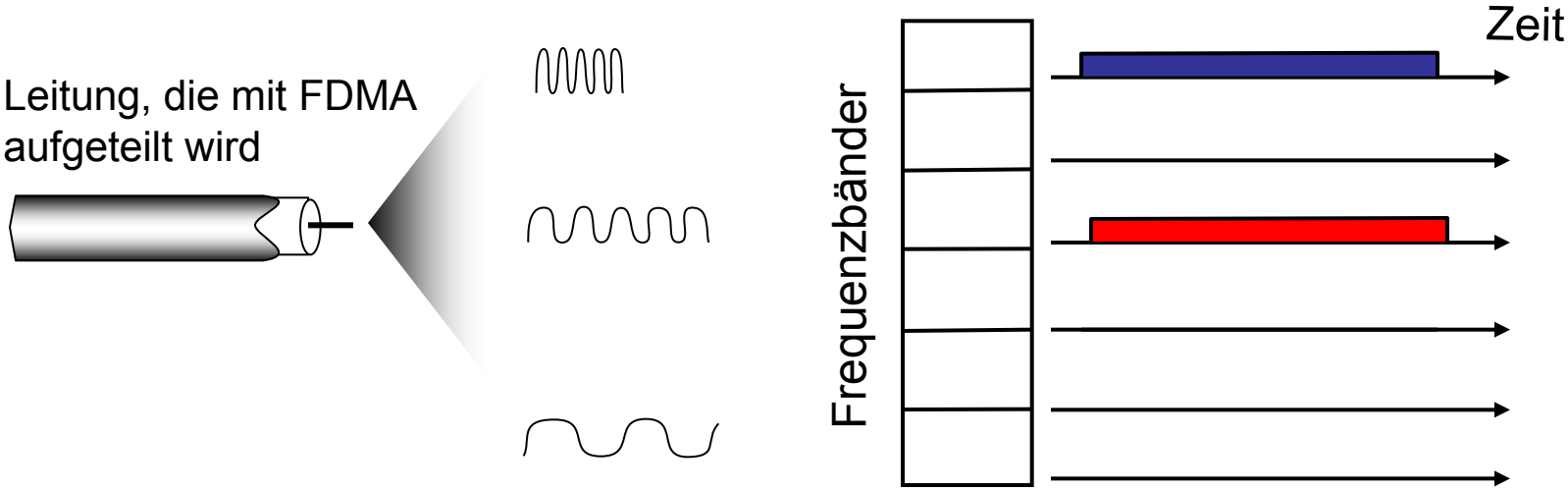


5.3 Kanalaufteilung mittels FDMA

Frequency Division Multiple Access (FDMA, ~Frequenzmultiplexing)
→ Das Spektrum des Mediums wird in Frequenzen aufgeteilt

- Jeder Station wird ein fester Frequenzbereich zugeteilt
- Wenn eine Station nicht sendet, wird der entsprechende Frequenzbereich nicht verwendet

Beispiel: LAN mit 6 Stationen, 1,3,4 senden, 2,5,6 senden nicht



5.3 Protokolle mit wahlfreiem Zugriff

- Wenn ein Knoten ein Paket senden möchte
  - Senden mit voller Datenrate des Kanals
  - Keine vorherige Koordination zwischen Knoten
- Wenn mehrere Knoten gleichzeitig übertragen: Kollision
- **Protokolle mit wahlfreiem Zugriff** legen fest:
  - Wie Kollisionen erkannt werden
  - Wie Kollisionen behandelt werden (z.B. durch eine verzögerte Neuübertragung)
- Beispiele für Protokolle mit wahlfreiem Zugriff:
  - Slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

5.3 Slotted ALOHA

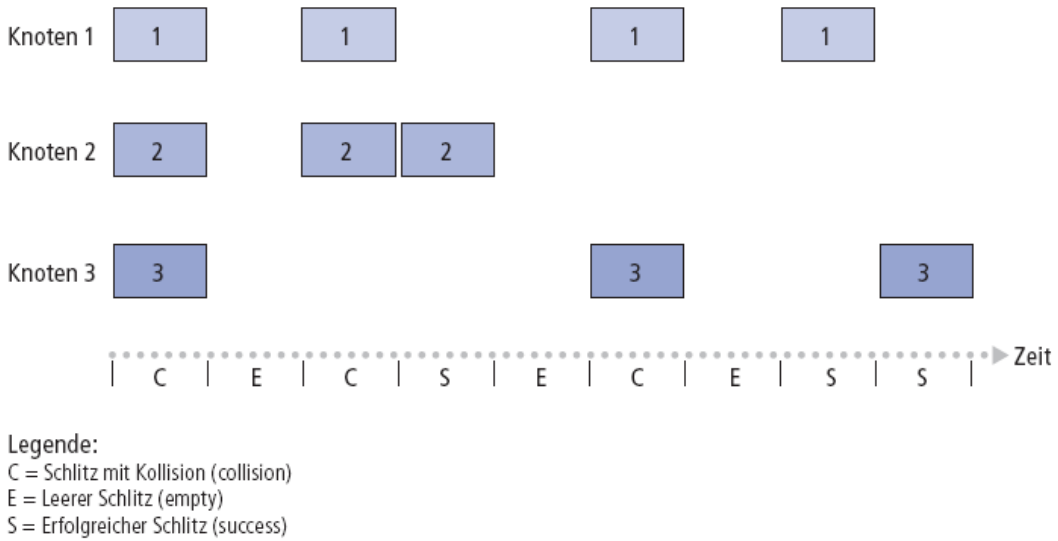
Annahmen:

- Alle Rahmen haben die gleiche Größe
- Zeitschlitze konstanter Größe, ausreichend für einen Rahmen
- Systeme starten ihre Übertragung nur zu Beginn eines Zeitschlitzes
- Systeme sind synchronisiert (sie kennen den globalen „Takt“ der Zeitschlitze)
- Wenn zwei oder mehr Systeme im gleichen Zeitschlitz senden, erkennen alle eine Kollision

Vorgehen:

- Wenn ein System Daten hat, überträgt es diese im nächsten Zeitschlitz
- Keine Kollision: nächsten Rahmen im nächsten Zeitschlitz senden
- Kollision: Übertragung mit Wahrscheinlichkeit p im nächsten Zeitschlitz, bis Übertragung erfolgreich ist

5.3 Slotted ALOHA



Legende:
C = Schlitz mit Kollision (collision)
E = Leerer Schlitz (empty)
S = Erfolgreicher Schlitz (success)

Vorteile

- Einzelnes System kann die volle Bandbreite des Mediums nutzen
- Dezentral
- Einfach

Nachteile

- Synchronisation der Zeitschlitze notwendig
- Kollisionen verschwenden Bandbreite
- Leere Zeitschlitze
- Systeme können Kollisionen in kürzerer Zeit als die Dauer eines Zeitschlitzes erkennen

5.3 Effizienz von Slotted ALOHA

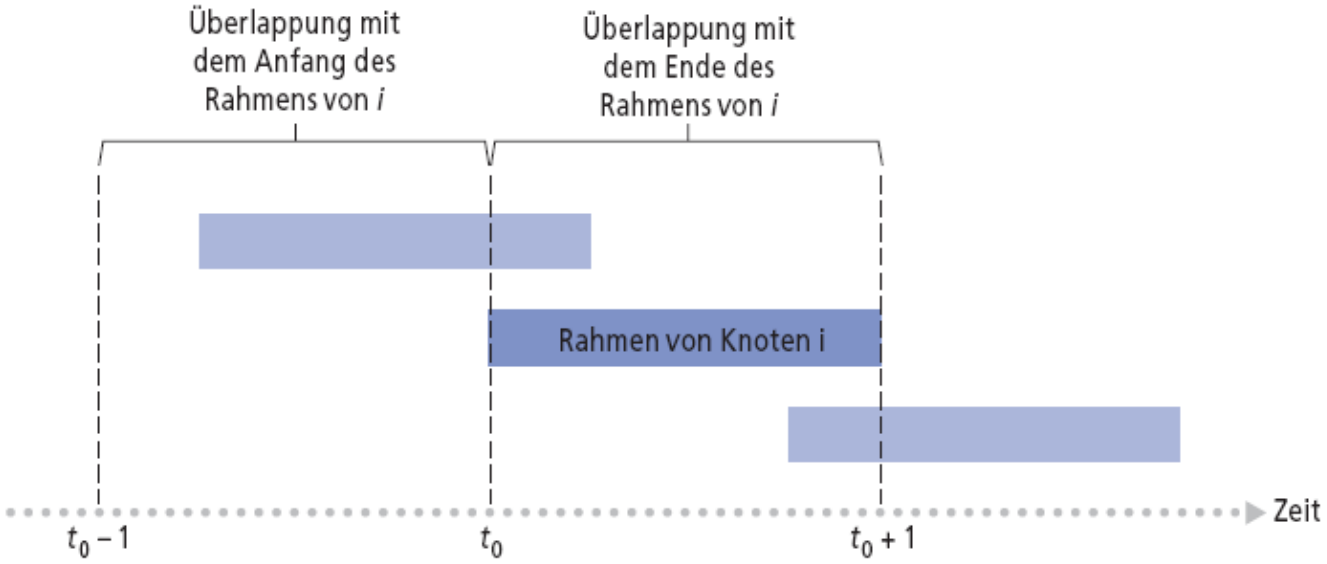
Effizienz: Durchschnittlich erzielte Datenrate, wenn viele Systeme viele Rahmen senden wollen, dividiert durch die Rate des Mediums.

- Annahme: N sendewillige Systeme, jedes überträgt in einem Zeitschlitz mit Wahrscheinlichkeit p
- Wahrscheinlichkeit, dass das erste System Erfolg hat: $p(1-p)^{N-1}$
- Wahrscheinlichkeit, dass ein beliebiges System Erfolg hat: $Np(1-p)^{N-1}$
- Für eine optimale Auslastung finde p*, welches diesen Ausdruck maximiert
- Berechne dann den Grenzwert des Ausdrucks, wenn N gegen unendlich geht (siehe auch http://tinyurl.com/cm6ny4z)

→ **Maximale Effizienz: 1/e ~ 37%**

5.3 Reines ALOHA

- Einfacher, keine Synchronisation notwendig
- Wenn neue Daten zum Senden ankommen:
  - Direkt übertragen
- Wahrscheinlichkeit für Kollisionen erhöht sich:
  - Ein zum Zeitpunkt t_0 gesendeter Rahmen kollidiert mit anderen Rahmen, die im Bereich $[t_0-1,t_0+1]$ gesendet wurden



5.3 Effizienz von reinem ALOHA

P(erfolgreiche Übertragung) = P(System überträgt) *
P(kein anderes System überträgt in $[p_0-1,p_0]$) *
P(kein anderes System überträgt in $[p_0,p_0+1]$)

$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$
$= p \cdot (1-p)^{2(N-1)}$

Wähle optimales p und lasse N gegen unendlich gehen ...

- **Maximale Effizienz: 1/2e ~ 18% → Halb so effizient wie Slotted ALOHA !**

5.3 CSMA

Carrier Sense Multiple Access (CSMA)

Zuhören vor dem Übertragen:

- Wenn der Kanal als leer erkannt wird → Übertrage den Rahmen
- Wenn der Kanal als besetzt erkannt wird → Übertragung verschieben

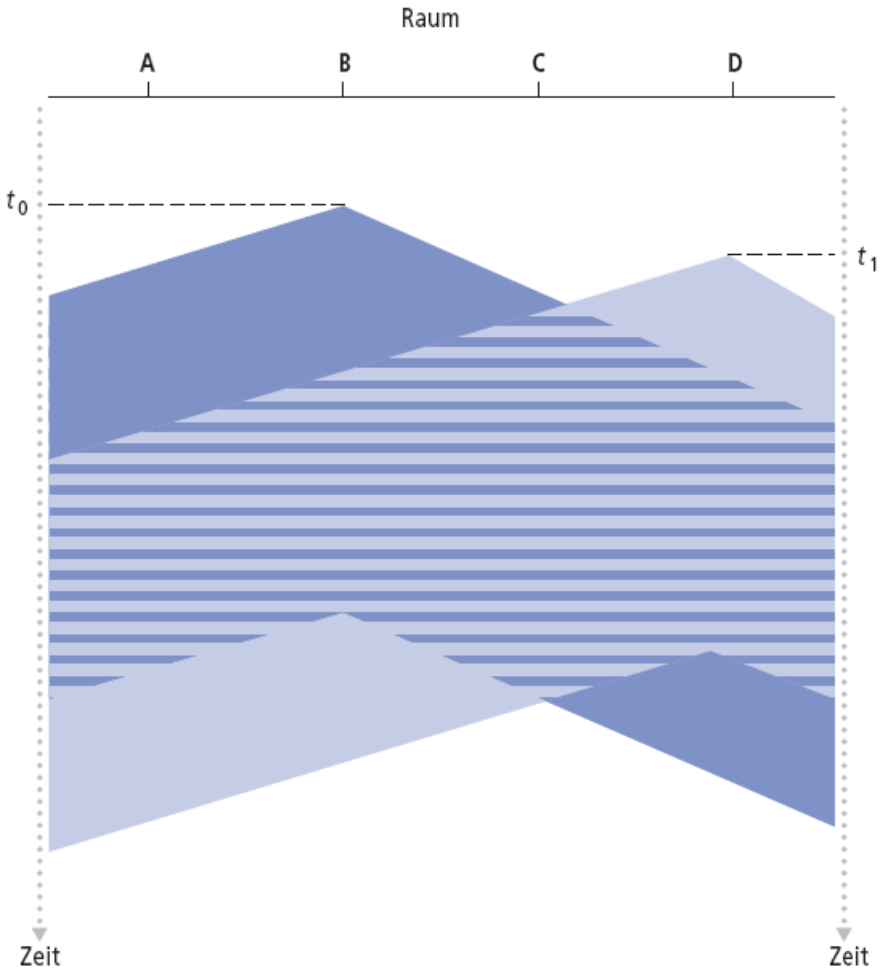
Analogie: *Nicht dazwischenreden, wenn jemand anderes gerade etwas sagt!*

5.3 CSMA - Kollisionen

- Kollisionen können immer noch auftreten:

  Die Ausbreitungsverzögerung kann dazu führen, dass man die Übertragung eines anderen Knotens nicht rechtzeitig erkennt!

- Kollision:
  - Dauert die ganze Übertragungszeit
    → Zeit wird verschwendet



5.3 CSMA/CD

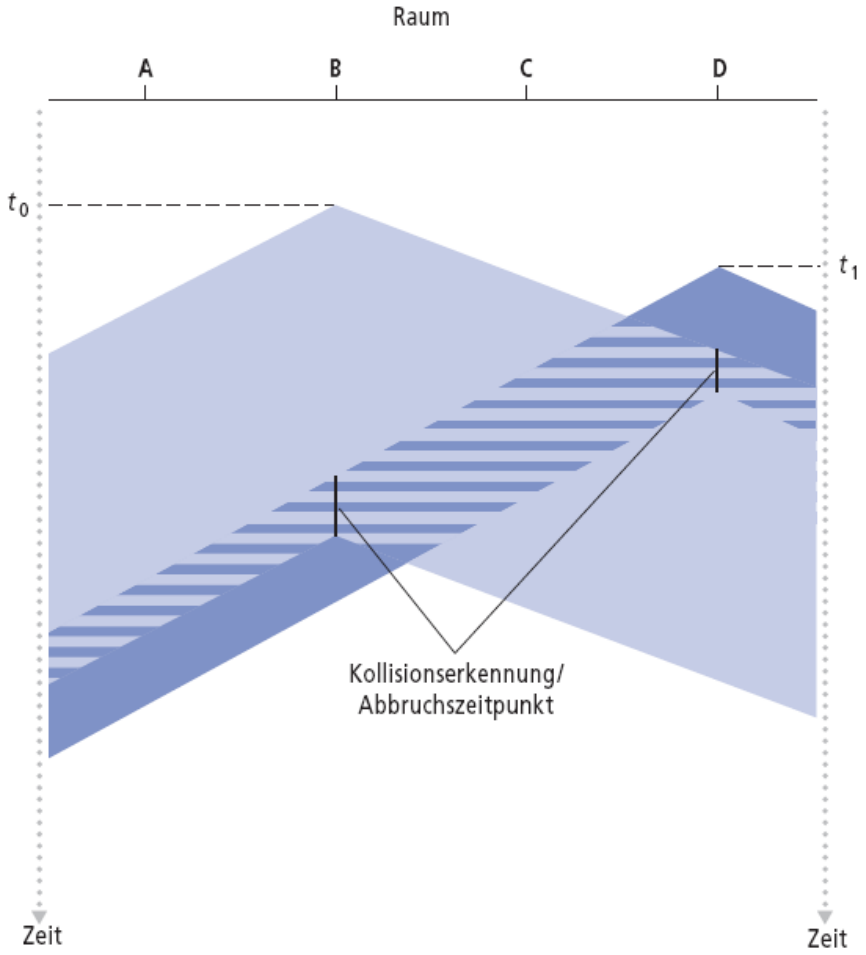
CSMA/CD (Collision Detection): Carrier Sensing wie in CSMA

- Kollisionen werden schnell erkannt
- Übertragungen, die kollidieren, werden abgebrochen

- Kollisionserkennung:
  - Einfach in drahtgebundenen LANs: Messe die empfangene Signalstärke und vergleiche sie mit der gesendeten Signalstärke
  - Schwierig in drahtlosen LANs: Die empfangene Signalstärke wird von der eigenen Übertragung dominiert

- Analogie: *der höfliche Diskussionsteilnehmer*

5.3 CSMA/CD


Raum
A
B
C
D
t_0
t_1
Kollisionserkennung/
Abbruchszeitpunkt
Zeit
Zeit

5.3 Effizienz von CSMA/CD

- Hängt von der Signallaufzeit t_{prop} zwischen konkurrierenden Stationen ab
  - Wenn diese gegen 0 geht, dann geht auch die Wahrscheinlichkeit für eine Kollision gegen 0 und somit die Effizienz gegen 1.
  - Wenn die Signallaufzeit groß wird, dann steigt das Risiko einer Kollision und die Effizienz sinkt.
- Hängt von $t_{übertragung}$ (der durchschnittlichen Zeit zur Übertragung eines Paketes) und damit von der Paketgröße ab.
  - Geht diese gegen unendlich, dann geht die Effizienz gegen 1.
- Bei Existenz vieler sendewilliger Stationen gilt:
  - Effizienz $\approx 1/(1+5t_{ausbreitung}/t_{übertragung})$
- Herleitung dazu in: S. Lam, „A Carrier Sense Multiple Access Protocol for Local Networks“, Computer Networks, Vol. 4, pp. 21-32, 1980.

5.3 CSMA/CD

MAC-Protokolle mit Aufteilung des Mediums:

- Teilen den Kanal effizient und fair auf, wenn die Last konstant verteilt ist
- Ineffizient bei dynamischer Verteilung der Last. Wenn die Partitionierung gleichmäßig erfolgt, aber nur einer von N Sendern tatsächlich aktiv ist, dann wird nur ein Anteil von 1/N der Bandbreite verwendet!

MAC-Protokolle für den wahlfreien Zugriff

- Effizient, wenn die Auslastung des Netzwerkes gering ist
- Bei hoher Last: Kollisionen

Protokolle mit abwechselndem Zugriff

- Versuchen, beide Vorteile zu vereinen!