Peer-to-Peer-Netzwerke

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Christian Schindelhauer

Sommersemester 2006

22. Vorlesung

20.07.2006

schindel@informatik.uni-freiburg.de

Inhalte

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Kurze Geschichte der Peer-to-Peer-Netzwerke**
- **Das Internet: Unter dem Overlay**
- **Die ersten Peer-to-Peer-Netzwerke**
  - Napster
  - Gnutella
- **CAN**
- **Chord**
- **Pastry und Tapestry**
- **Gradoptimierte Netzwerke**
  - Viceroy
  - Distance-Halving
  - Koorde
- **Netzwerke mit geordneter Speicherung**
  - P-Grid
  - Skip-Net und Skip-Graphs
- **Selbstorganisation**
  - Pareto-Netzwerke
  - Zufallsnetzwerke
  - Topologie-Management
- **Sicherheit in Peer-to-Peer-Netzwerken**
- **Anonymität**
- **Datenzugriff: Der schnellere Download**
- **Peer-to-Peer-Netzwerke in der Praxis**
  - eDonkey
  - FastTrack
  - Bittorrent
- **Ausblick**
  - Juristische Situation
  - Anwendungen
  - Offene Fragen Situation

Methoden der Anonymisierung

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Dining Cryptographers**
  - Wer hat's geschickt?
- **Onion Routing**
  - Verwickelte Umwege...
- **F2F-P2P**
  - Friend-to-Friend
- **Dark-Net**
  - War das was?
- **Steganographie**
  - nichts zu sehen...
- **k-aus-n-Verschlüsselung**
- **Verschlüsselte Inhalte**
  - Denn sie wissen nicht, was sie speichern...
- **Verschlüsselte, unterschriebene Index-Einträge**
  - gezeichnet: Zorro

Secret Sharing Systems

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Aufgabe**
  - n Leute sollen eine Geheimnis bewahren,
  - dass aber nur bei Kooperation von k dieser Leute offenbart werden kann
- **Schema von Blakley**
  - In einem k-dimensionalen Raum bestimmt der Schnitt von k k-dimensionalen Hyper-Ebenen (mit Dimension k-1) genau einem Punkt
  - Dieser Punkt ist das Geheimnis
  - Mit nur k-1 Dimensionen erhält man eine Linie
- **Konstruktion**
  - Eine dritte Instanz wählt zu dem Punkt n nicht parallele k-dimensionale Hyper-Ebenen und verteilt diese auf die n Leute

Verschlüsselte Daten

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Peer speichern nur verschlüsselte Daten**
  - Dem Speichernden ist es nicht möglich die Daten zu lesen
  - Die Daten werden vom Veröffentlicher verschlüsselt
- **Zusätzlich können diese Daten vom Veröffentlicher auch unterschrieben werden, so dass**
  - dieser die Daten ändern oder löschen kann
  - kein anderer die Daten unbefugt löscht
- **Diese können gelesen werden, wenn**
  - Der Veröffentlicher den Schlüssel über einem anderen Weg den Abfrager mitteilt oder
  - Der Abfrager einen Indexeintrag gefunden hat auf einem anderen Peer, der zum Entschlüsseln genügt
    - Dadurch wird der Veröffentlicher nicht offenbart
- **Vorteil**
  - Der Speichernde kann für die Inhalte nicht belangt werden (?)
- **Nachteil**
  - Der Speichernde kann die Wichtigkeit der Inhalte nicht beurteilen
    - Löschen oder nicht Löschen

Verschlüsselte, unterschriebene Indexeinträge

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Methode**
  - Der Suchbegriff wird durch eine kryptographische Hash-Funktion bearbeitet und abgelegt
  - Dieser verschlüsselte Index wird kombiniert mit der Identifikation des Speichers
  - Der Index enthält den Schlüssel zur Entschlüsselung des Datums
  - Beides wird unterschrieben durch den Veröffentlicher
- **Vorteil:**
  - Die Suche kann ohne den Veröffentlicher durchgeführt werden
  - Alleine mit diesem Index kann die Datei entschlüsselt werden
  - Nur durch das Suchen nach dem Index können die Dateien gelesen werden
  - Nur der Veröffentlicher kann den Such-Index verändern oder löschen (wegen digitaler Unterschrift)
- **Nachteil:**
  - Anfällig für eine Wörterbuch-Attacke
  - Keine Suche nach ähnlichen Begriffen möglich

Free-Haven

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **von Roger R. Dingledine, Michael Freedman, David Molnar, Brian Sniffen und Todd Kamin 2000**
- **Ziel**
  - Verteilter Datenspeicher der robust gegen Angriffe von starken Gegnern ist
  - Angreifer versucht Daten zu zerstören
- **Design**
  - Gemeinschaft von Servern, welche sich gegenseitig Speicherplatz bereitstellen
  - Dokumente werden gemäß Secret Sharing auf Server verteilt
  - Diese Teile werden im Hintergrund zwischen den Servern ausgetauscht
  - Für die Abfrage fragt ein Client einen Server (mittels geschützter Kommunikation), der ihn dann eine geeignete Menge von Server mitteilen kann zur Rekonstruktion der Datei
  - Die Kommunikation erfolgt über Onion Routing

Free-Haven

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Operationen:**
  - Einfügen von Dokumenten
  - Herunterladen von Dokumenten, wobei die Authentizität des Dokuments bewiesen werden kann
  - Ablaufdatum für Dokumente
    - Bis zum Ablaufdatum ist das Dokument nicht zerstörbar
    - Dann kann es gelöscht werden
  - Einfügen von Servern
  - Mechanismus zum Erkennen von inaktiven oder toten Servern
- **Free-Haven**
  - Publisher, Reader, Server und Document-Anonymität
  - aber keine Query-Anonymität
  - Aber nur unter Verwendung von vertrauenswürdigen Servern

Free-Net

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **von Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore Hong, 2000**
- **Ziel**
  - Peer-to-Peer-Netzwerk
  - Erlaubt Veröffentlichung, Replikation, Beschaffung von Daten
  - Anonymität von Autoren und Lesern
- **Dateien**
  - sind orts-unabhängig referenziert
    - durch verschlüsselte und unterzeichnete Index-Dateien
    - Autor ist nicht rekonstruierbar
  - sind gegen unbefugtes Überschreiben oder Löschen geschützt
  - sind verschlüsselt
    - Inhalt ist nur durch Kenntnis der andernorts abgelegten Index-Datei in Kombination mit dem Suchbegriff lesbar
  - werden repliziert
    - auf dem Anfragepfad der Suchanfrage
  - und nach dem “Least Recently Used” (LRU) Prinzip gelöscht

Free-Net

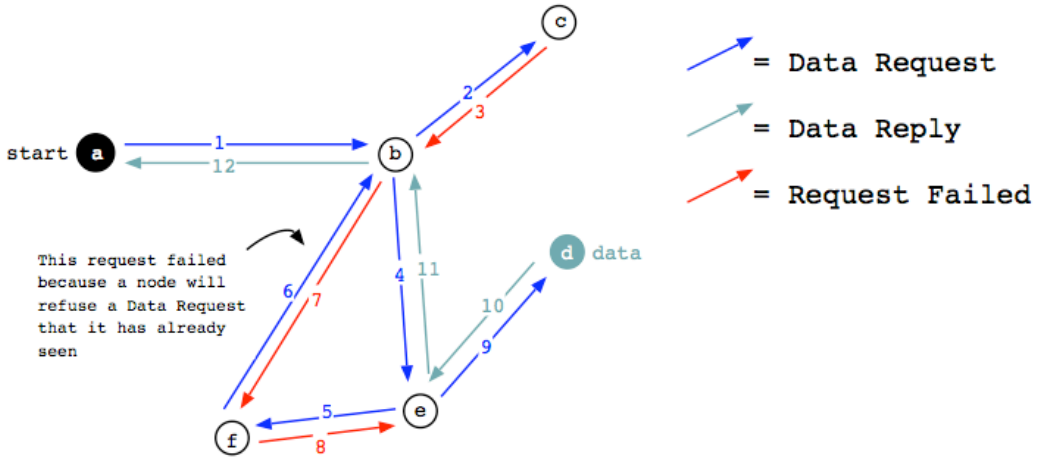
Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Netzwerkstruktur**
  - stark verwandt mit Gnutella
  - Netzwerkaufbau durch Nachbarkanten
    - aber kein F2F-Netzwerk, da bei der Suche Abkürzungen eingebaut werden können
  - Ähnlich wie Gnutella ist das Netzwerk Pareto-verteilt
- **Speichern von Dateien**
  - Jede Datei kann durch den kodierten Adress-String und dem signierten Index-Schlüssel (signed subspace key) gefunden, entschüsselt und gelesen werden
  - Jede Datei wird mit der Information des Index-Schlüssels gespeichert, aber ohne kodierten Adress-String
  - Dadurch kann kein Server diese Datei lesen
    - es sei denn er führt eine Wörterbuch-Attacke durch
- **Speichern von Index-Daten**
  - Der Adress-String, kodiert durch eine kryptographische Hash-Funktion führt zu den passenden Peer, der die Index-Daten bestehend aus dem Adress-String und dem signierten Index-Schlüssel besteht
  - Mit diesen Index-Daten kann die Datei gefunden werden

Free-Net

Suche

- "steepest-ascent hill-climbing"
  - Anfragen werden an den Peer weitergeleitet, welcher dem Such-Index am ähnlichstens ist
- mit Time-to-Live-Feld
- Auf der anderen seite wandern Dateien zu dem Peer dessen Kodierung dem Such-Index der Datei am ähnlichsten ist



Effizienz von Free-Net

- **Free-Net ist ähnlich wie Gnutella ein Pareto-Netzwerk**

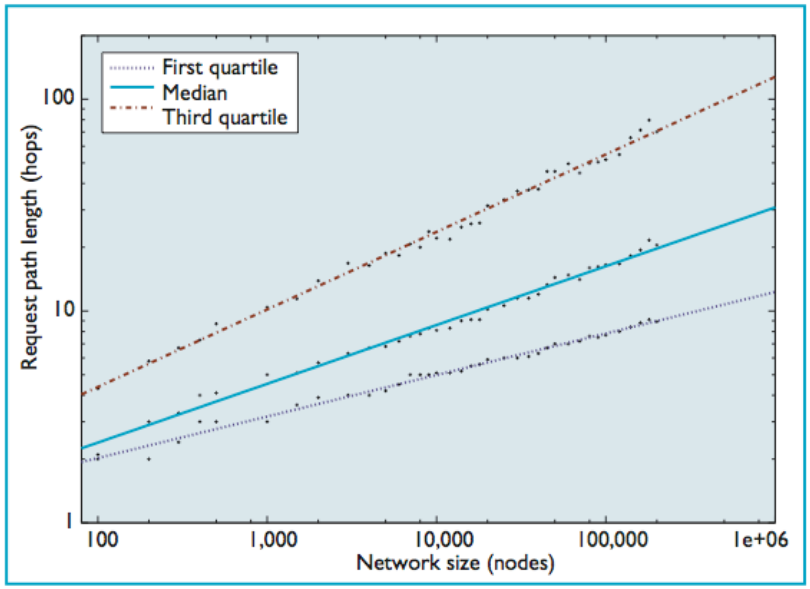


Figure 3. Request path length versus network size.The median path length in the network scales as $N^{0.28}$.

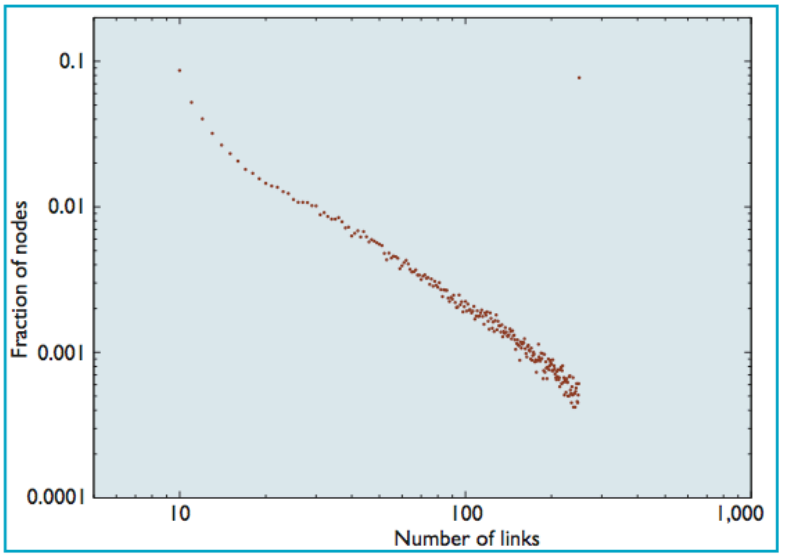


Figure 2. Degree distribution among Freenet nodes.The network shows a close fit to a power-law distribution.

- **Die Suchzeit ist im Durchschnitt polynomiell**

Gnu-Net

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

- **Krista Bennett, Christian Grothoff, Tzvetan Horozov, Ioana Patrasca, Tiberiu Stef, 2006**
- **Ziele**
  - Vertrauenswürdiges, anonymes, verteiltes File-Sharing
  - wenig Nachrichten-Verkehr, geringer CPU-Overhead
  - Abwehrmaßnahmen gegen bösartige Hosts
- **Methoden**
  - GNUnets teilt große Dateien in Blöcke, die durch einen baumförmigen Code zusammengehalten werden
    - Kodierte Knoten beschreiben die Hash-Werte der Kinder im Baum
  - Trust-Management
    - Knoten können jeder Zeit ohne zentrale Kontrolle dem Netzwerk beitreten
    - Knoten starten mit geringen Vertrauen (untrusted)
    - Erst durch positive Mitwirkung wird das Vertrauen in diese Peers erhöht
    - Je größer das Vertrauen, desto mehr Anfragen dürfen sie in das Netzwerk stellen

Ende der 22. Vorlesung

Albert-Ludwigs-Universität Freiburg
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Peer-to-Peer-Netzwerke

Christian Schindelhauer

schindel@informatik.uni-freiburg.de