

Seminar: IT-Sicherheit

Securing Content in Structured Overlay Networks

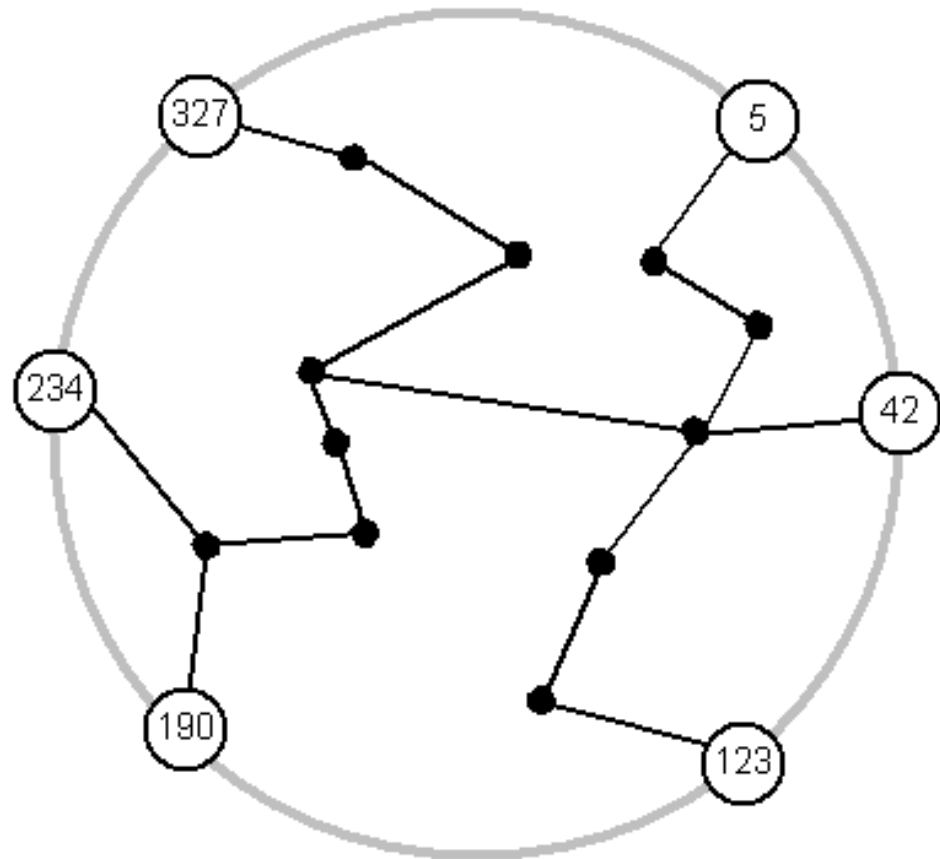
Vorgetragen von Florian Rudolph und Henning Stein

Gliederung

- Structured Overlay Networks
- Distributed Hash Tables (DHT)
- Content
- Sicherheit
- Sicheres Routing
- Ausblick

Structured Overlay Networks

- Netzwerke, die „über“ das Internet gelegt sind
- „Structured“
- Jeder Knoten erhält eine ID
- Routing auf Overlay-Ebene



Distributed Hash Table

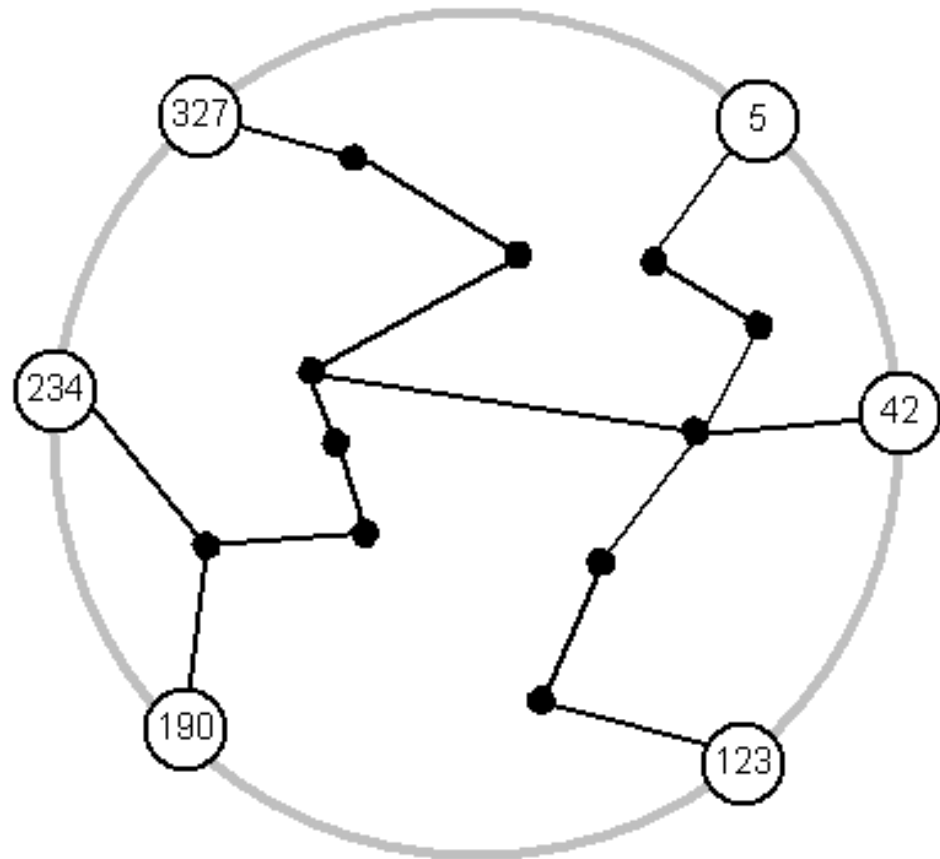
- Es wird ein Paar aus Schlüssel und Wert angegeben
- Der Hashwert des Schlüssels ergibt die ID desjenigen Knoten, der den Wert speichern soll
- Knoten speichern den Wert

Schnittstellen von DHT

- Routing Interface
 - Der DHT kennt nur eine Operation: Das Schicken einer Nachricht an einen Knoten
 - Die Applikation muss sich selbst um die Replikation von Daten kümmern, um die Verfügbarkeit zu sichern
- Storage Interface
 - Der DHT hat zwei Operationen
 - Daten im Netzwerk ablegen
 - Daten aus dem Netzwerk herausholen
 - Weniger Kontrolle durch Applikation, daher einfacher zu verwenden

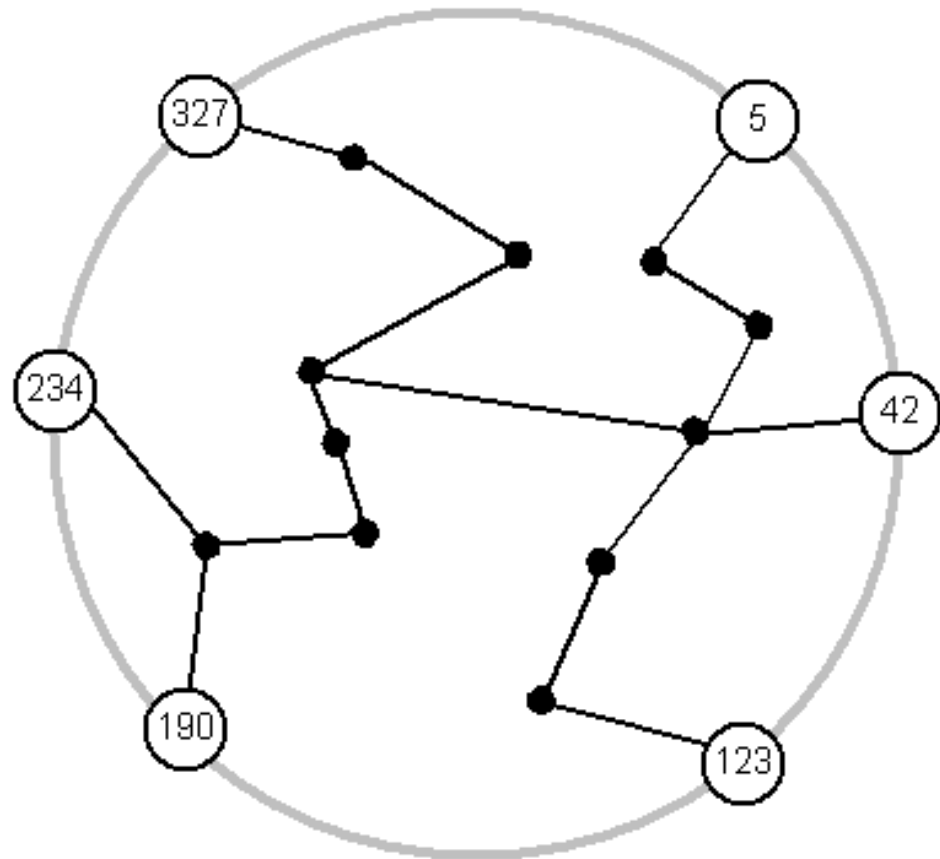
Iteratives Routing

- Kommunikation
Knoten 5 ↔ Knoten
234
- Knoten 5 fragt Knoten
42
- Knoten 42 sagt:
„Frag Knoten 123, mit
der IP-Adresse X“
- Knoten 5 fragt Knoten
123



Rekursives Routing

- Kommunikation
Knoten 5 ↔ Knoten
234
- Knoten 5 fragt Knoten
42
- Knoten 42 fragt Knoten
123
- Knoten 123 fragt
Knoten 190
-



Content

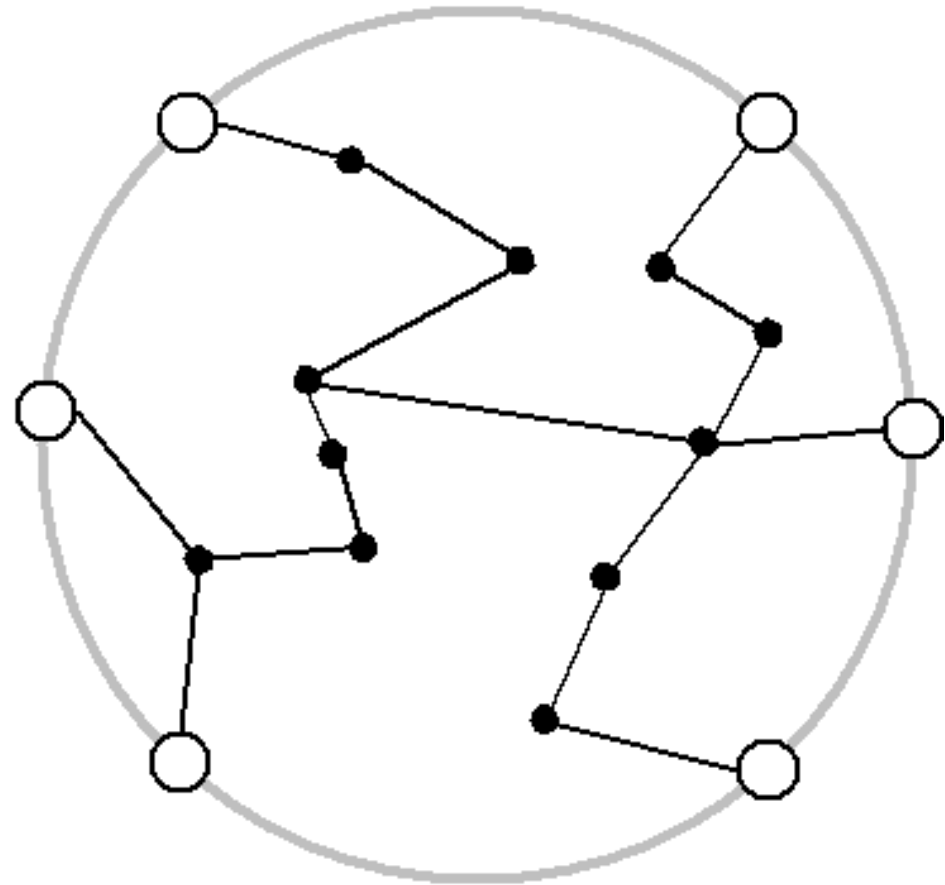
- Beliebige Daten
 - Eine Datei
 - Ein Verweis auf eine Datei
 - Verteilte Backups
 - Zuordnung SIP-URI ↔ IP-Adresse
 - Namen ↔ IP-Adressen (DNS)

Sicherheit

- Verfügbarkeit
- Integrität (Anwendungsabhängig)
 - Zentrale Zertifizierungsstelle
 - Self-certifying
 - Reputation
- Vertraulichkeit (Anwendungsabhängig)
- Anonymität (Anwendungsabhängig)

Sicheres Routing als Grundlage eines sicheren Overlay Network

- Knoten X fügt Content ein
- Y (böse) speichert den Content
- Z will Content abrufen
 - Y gibt nichts heraus (Verfügbarkeit)
 - Y gibt anderen Content heraus (Integrität)



Lösungsansatz: Sichere Knoten-IDs

- Knoten können IDs nicht frei wählen
 - Hash der IP-Adresse
 - Zuweisung durch zentrale Stelle
 - Zertifikat mit Bindung an Knoten-ID

Sichere Routing Table Updates

- Voraussetzung sichere Knoten IDs
- Zwei Routing Tables
 - Einen für effizientes Routing
 - Einen als Backup mit eingeschränkter Funktionalität

Sichere Nachrichtenweiterleitung

- Annahme, dass nur begrenzte Anzahl an Knoten unsicher ist
- Nachrichten an Knoten senden mit anschließender Überprüfung

Ausblick

- CAN, Chord, Pastry untersuchen
- Erstellung einer Klassifikation von Angriffen und Lösungen
-