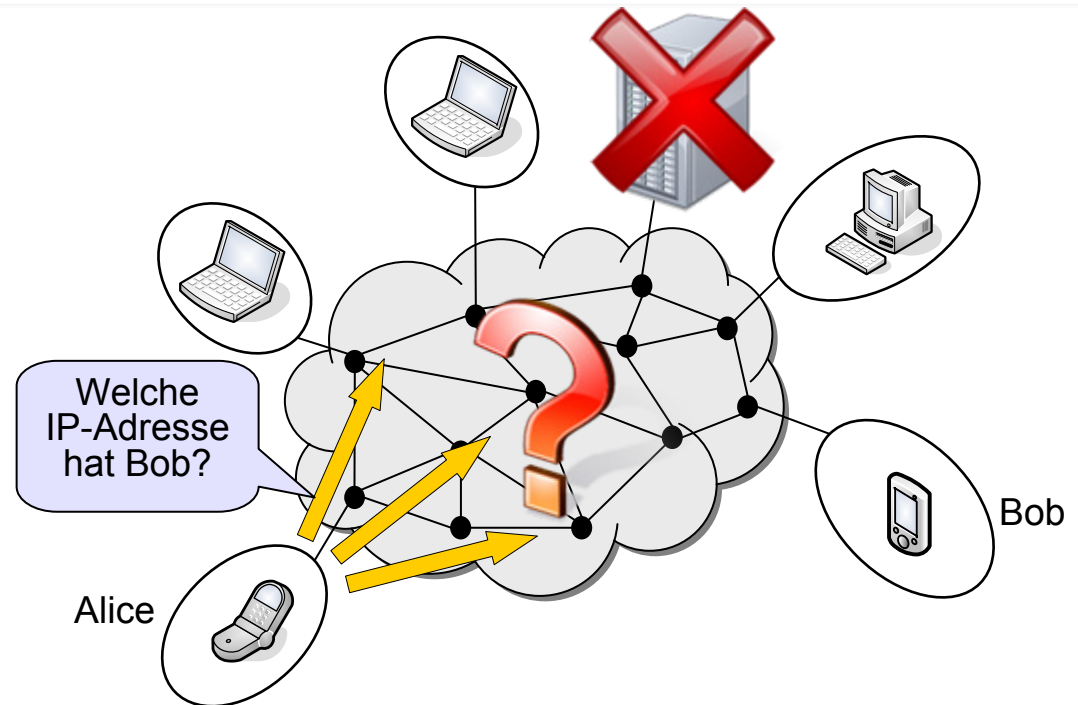


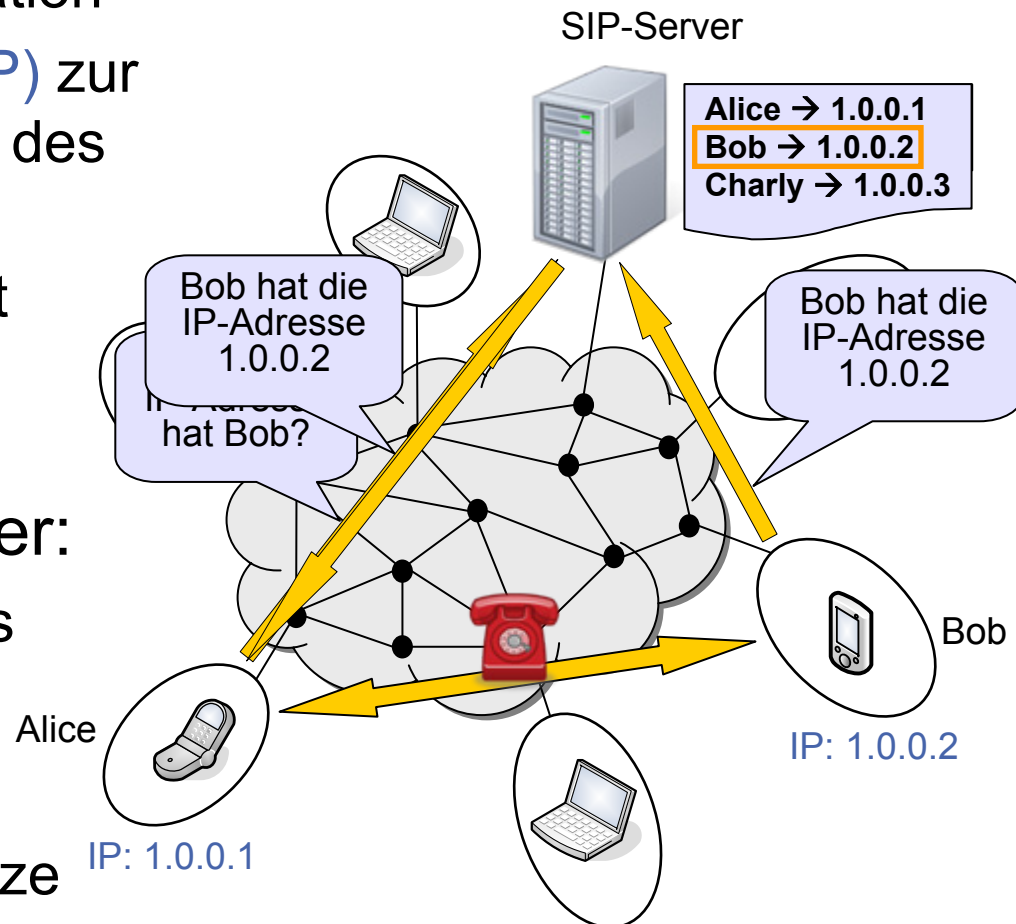
Sichere und effiziente Namensauflösung für dezentrale IP-Telefonie

Ingmar Baumgart



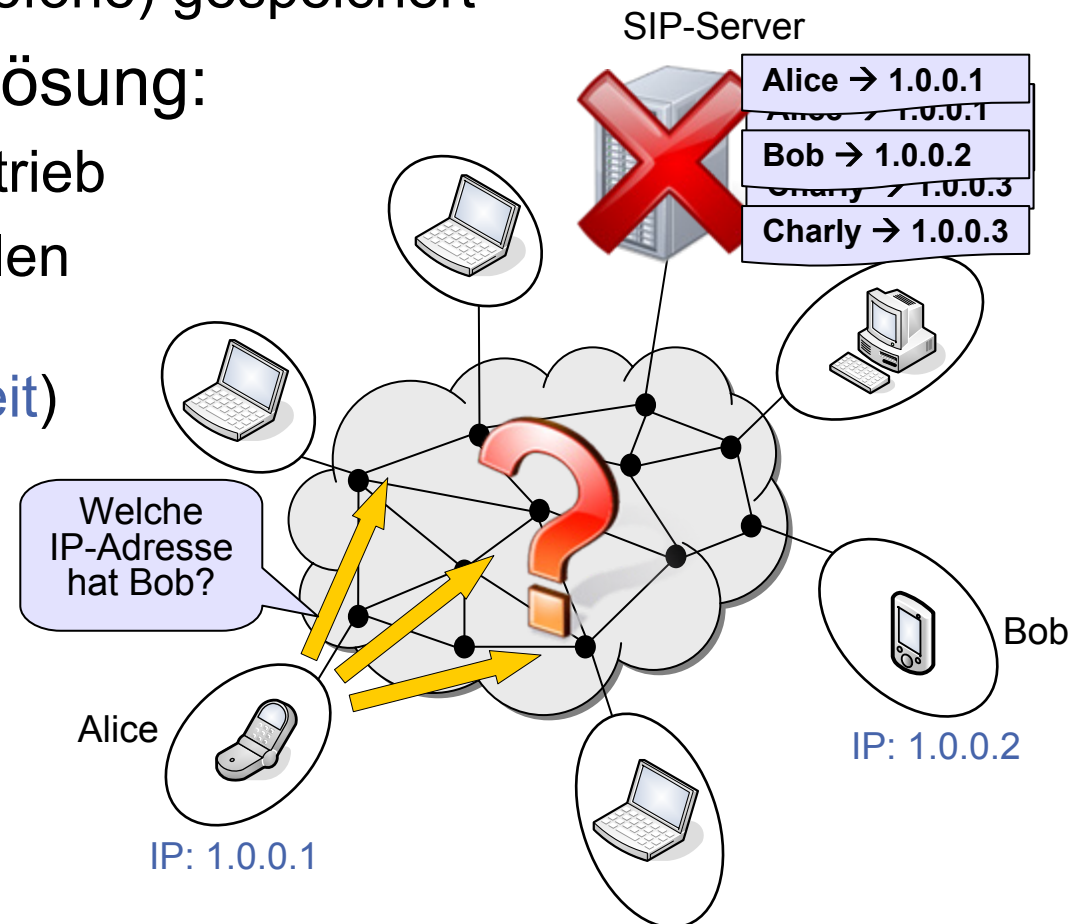
IP-Telefonie mit zentralem Server

- Trend: Zunehmende Verbreitung von **IP-Telefonie**
 - **Kostenersparnis** durch gemeinsames IP-Netz (z.B. Internet) für Sprach- und Datenkommunikation
 - **Session Initiation Protocol (SIP)** zur Signalisierung und Auffindung des Kommunikationspartners
 - Zentraler **SIP-Server** speichert dynamische Zuordnung von Namen zu IP-Adressen
- Nachteile mit zentralem Server:
 - Kosten für Betrieb des Servers
 - Eingeschränkte Skalierbarkeit
 - Keine Ausfallsicherheit
 - Ungeeignete für spontane Netze



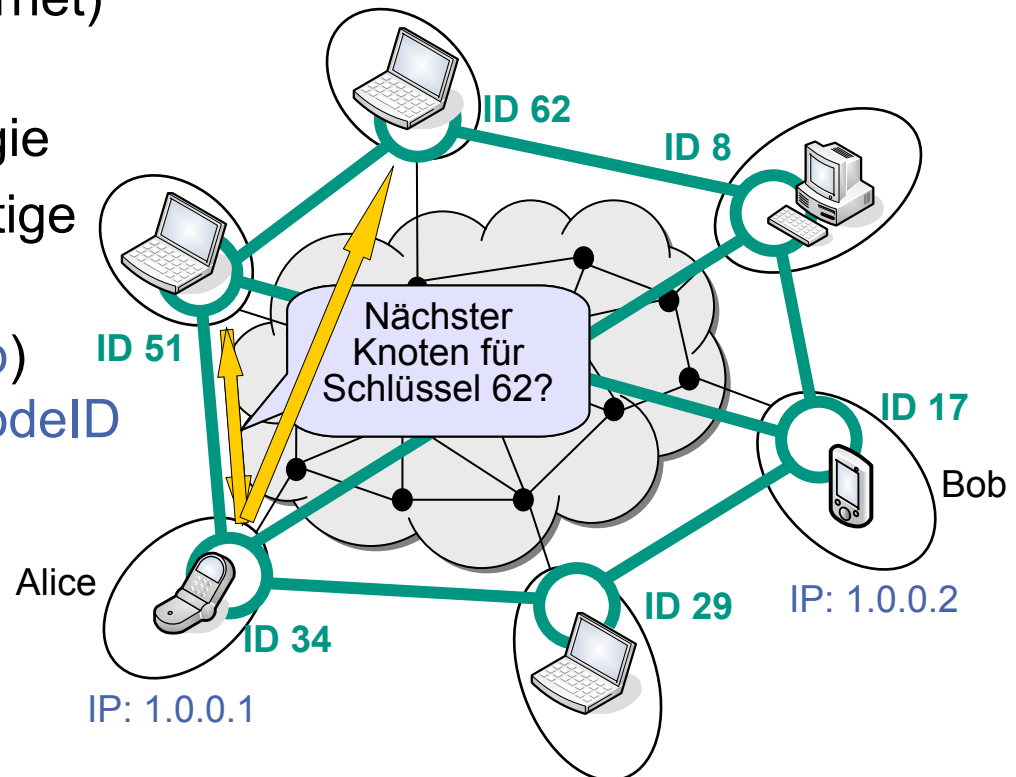
Dezentrale IP-Telefonie

- SIP-Server kann durch **Peer-to-Peer-Netz** ersetzt werden
 - Namenszuordnungen werden dezentral auf den beteiligten Endgeräten (Computer, Telefone) gespeichert
- Vorteile der Peer-to-Peer-Lösung:
 - **Keine Kosten** für Server-Betrieb
 - Zusätzliche Teilnehmer stellen Ressourcen für den Betrieb zur Verfügung (**Skalierbarkeit**)
 - Dezentrale Struktur erhöht die **Ausfallsicherheit** (kein Single-Point-of-Failure)
- Effiziente Auffindung der Namenszuordnung?



Strukturierte Peer-to-Peer-Netze

- Dezentrale Ablage der Namenszuordnungen durch strukturiertes Peer-to-Peer-Netz:
 - Schlüsselbasiertes Routing (*Key-based Routing, KBR*)
 - Logische Overlay-Topologie über vorhandenem physischen Underlay-Netzwerk (z.B. Internet)
 - Overlay-Routingtabelle mit Nachbarn in Overlay-Topologie
 - Jede Knoten hat eine eindeutige Overlay-Adresse (*NodeID*)
 - Effiziente Auffindung (*Lookup*) von Knoten anhand deren *NodeID*



Strukturierte Peer-to-Peer-Netze

- Dezentrale Ablage der Namenszuordnungen durch strukturiertes Peer-to-Peer-Netz:

- Schlüsselbasiertes Routing (*Key-based Routing, KBR*)

- Verteilte Hashtabelle (*Distributed Hash Table, DHT*)

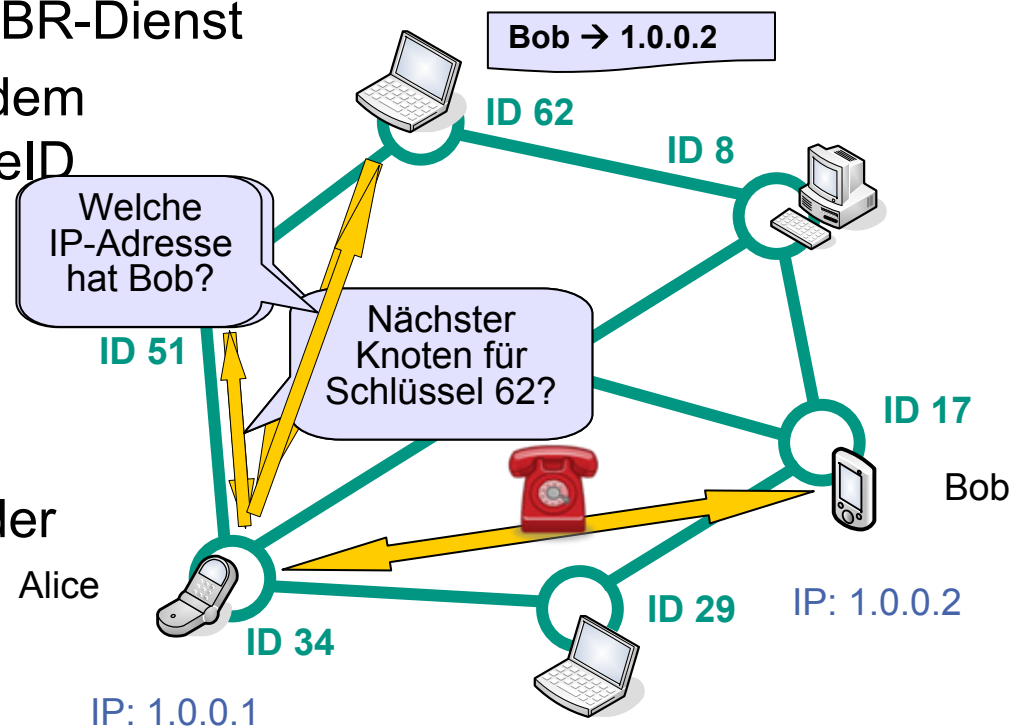
- Verteilte Datenablage über KBR-Dienst

- Namenszuordnung wird auf dem Knoten mit der nächster NodeID zu $H(Name)$ gespeichert

- Beispiel:

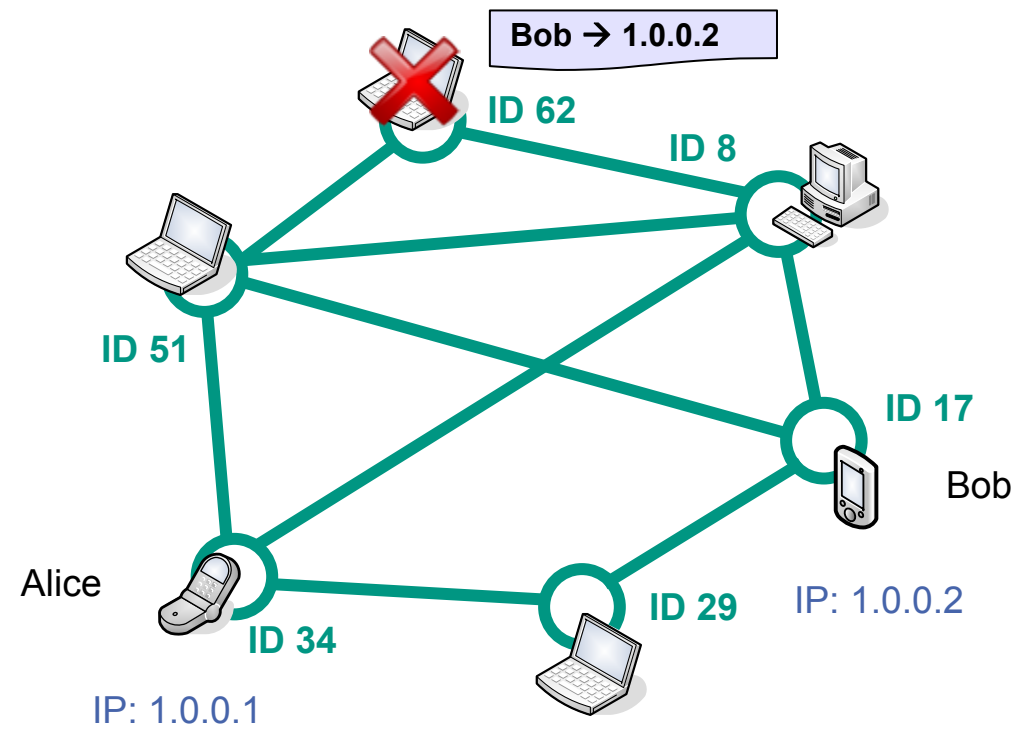
- $H(„Bob“) = 61$

- Über einen KBR-Lookup nach Schlüssel 61 wird der zuständige Knoten mit NodeID 62 aufgefunden



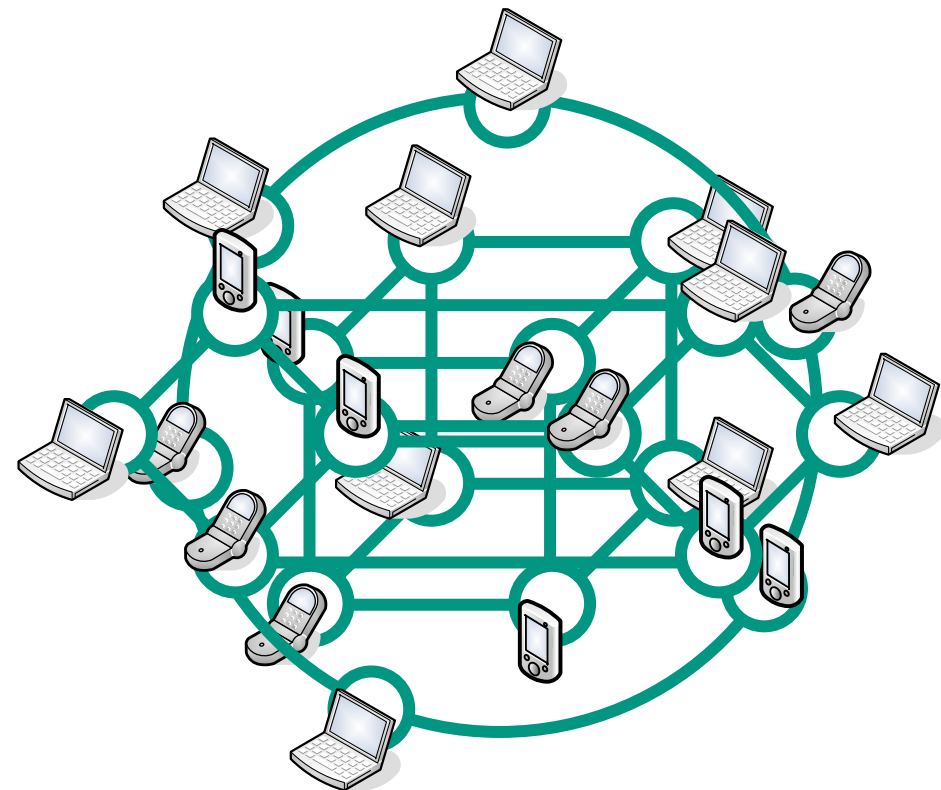
Problemstellungen

- Zuverlässiger Dienst in Netzen mit Knotenfluktuation



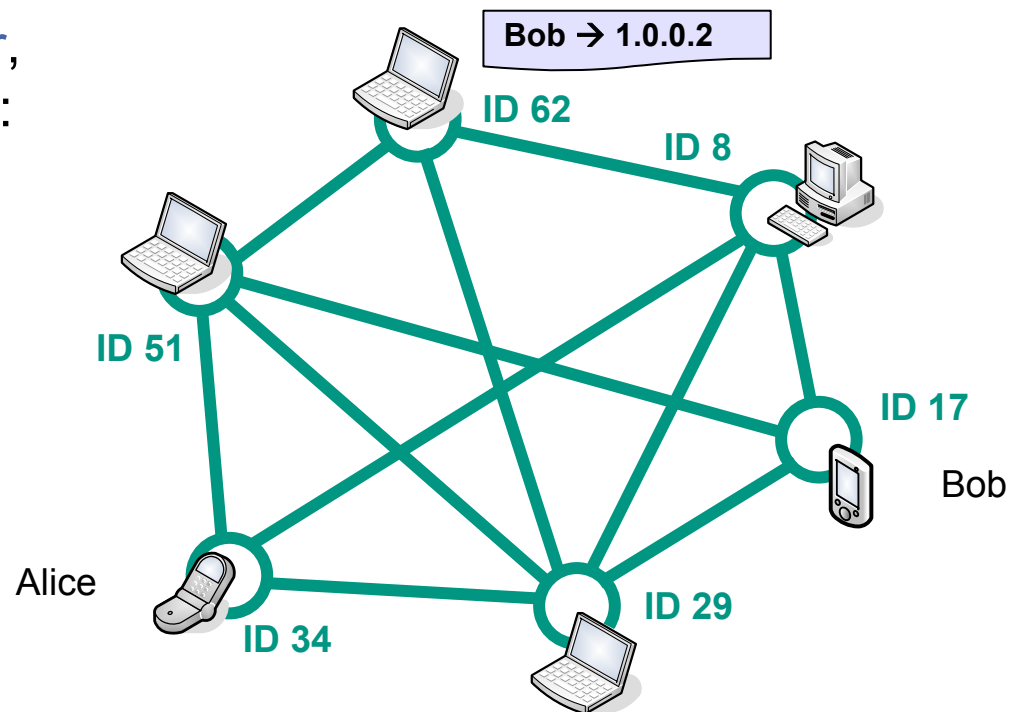
Problemstellungen

- Zuverlässiger Dienst in Netzen mit Knotenfluktuation
- Wahl eines geeigneten KBR-Protokolls für den Namensdienst
 - Vielzahl an KBR-Protokollen (*Chord, Kademlia, Bamboo, ...*) mit unterschiedlichen Eigenschaften (z.B. Overlay-Topologie)



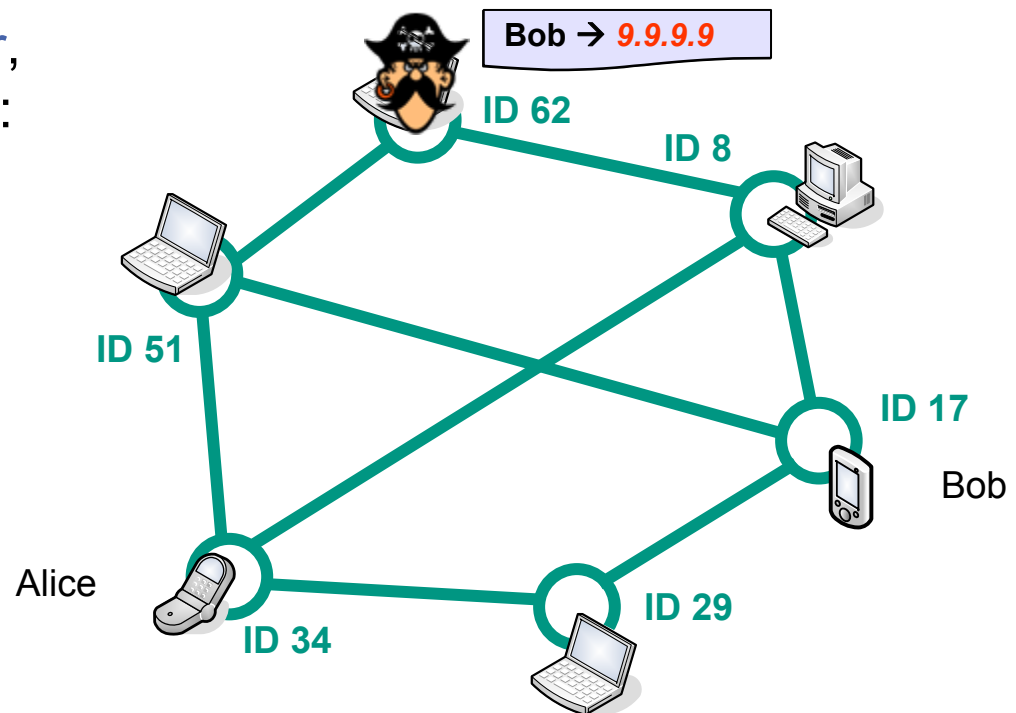
Problemstellungen

- Zuverlässiger Dienst in Netzen mit Knotenfluktuation
- Wahl eines geeigneten KBR-Protokolls für den Namensdienst
 - Vielzahl an KBR-Protokollen (*Chord, Kademia, Bamboo, ...*) mit unterschiedlichen Eigenschaften (z.B. Overlay-Topologie)
- Wahl geeigneter KBR-Parameter
 - Verschiedene **Protokollparameter**, die sich gegenseitig beeinflussen:
 - Größe der Routingtabelle
 - Stabilisierungsintervalle
 - **Abwägung** zwischen Zuverlässigkeit, Latenz und Kommunikationsaufwand



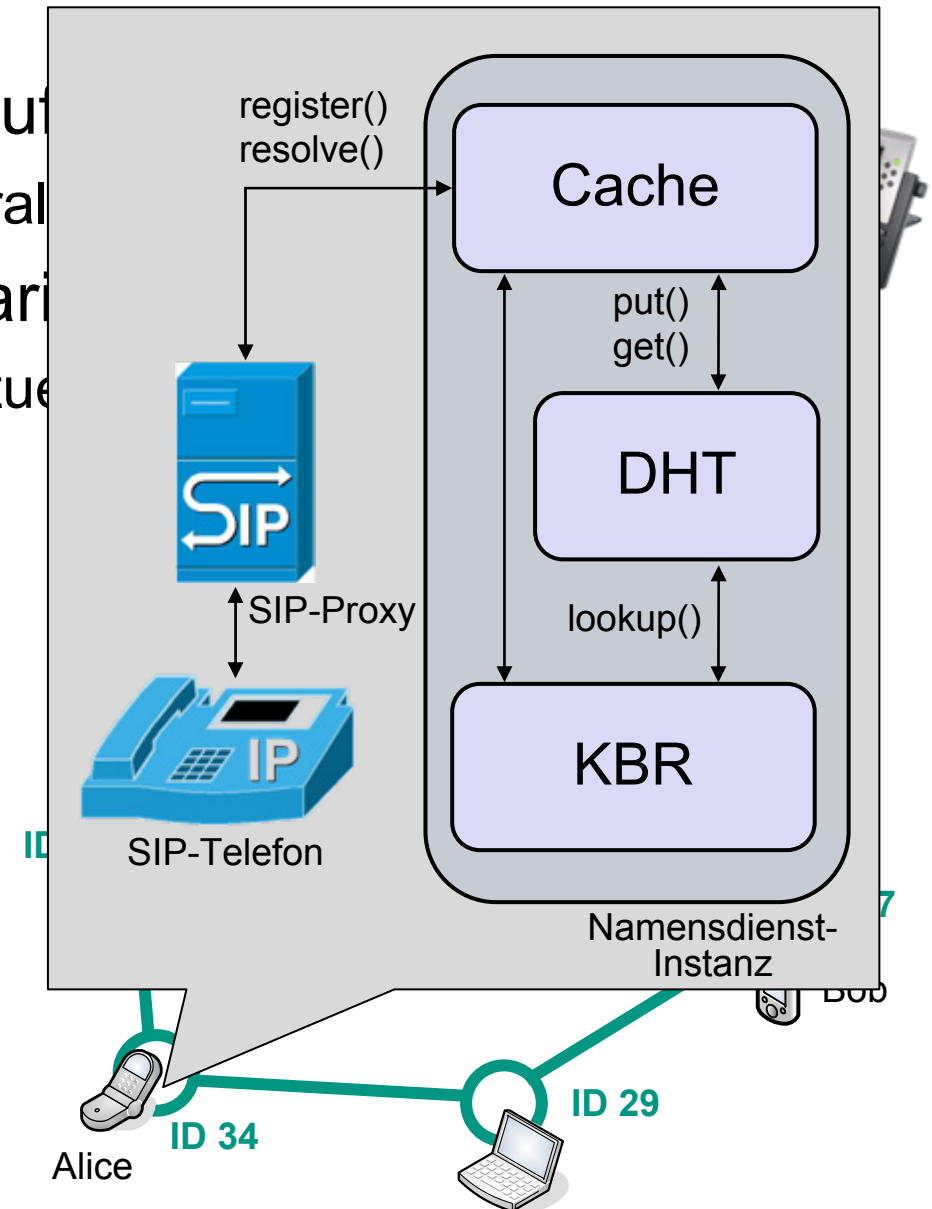
Problemstellungen

- Zuverlässiger Dienst in Netzen mit Knotenfluktuation
- Wahl eines geeigneten KBR-Protokolls für den Namensdienst
 - Vielzahl an KBR-Protokollen (*Chord, Kademia, Bamboo, ...*) mit unterschiedlichen Eigenschaften (z.B. Overlay-Topologie)
- Wahl geeigneter KBR-Parameter
 - Verschiedene **Protokollparameter**, die sich gegenseitig beeinflussen:
 - Größe der Routingtabelle
 - Stabilisierungsintervalle
 - **Abwägung** zwischen Zuverlässigkeit, Latenz und Kommunikationsaufwand
- Sicherheit
 - Dezentrales Netz ohne vertrauenswürdige Teilnehmer



Dezentraler Namensdienst P2PNS

- Generische, verteilte Namensauflösung
 - Dezentrale IP-Telefonie, dezentral
- Gleiche Aufgabe in allen Szenarien
 - Auflösung eines Namens zur aktuellen
- Modulare Architektur
 - Ermöglicht Adaption an das jeweilige Anwendungsszenario
 - Wiederverwendbarkeit einzelner Komponenten
- Bietet Sicherheit in vollständig dezentralen Umgebungen:
 - Eindeutige Nutzernamen
 - Verhindert Identitätsdiebstahl

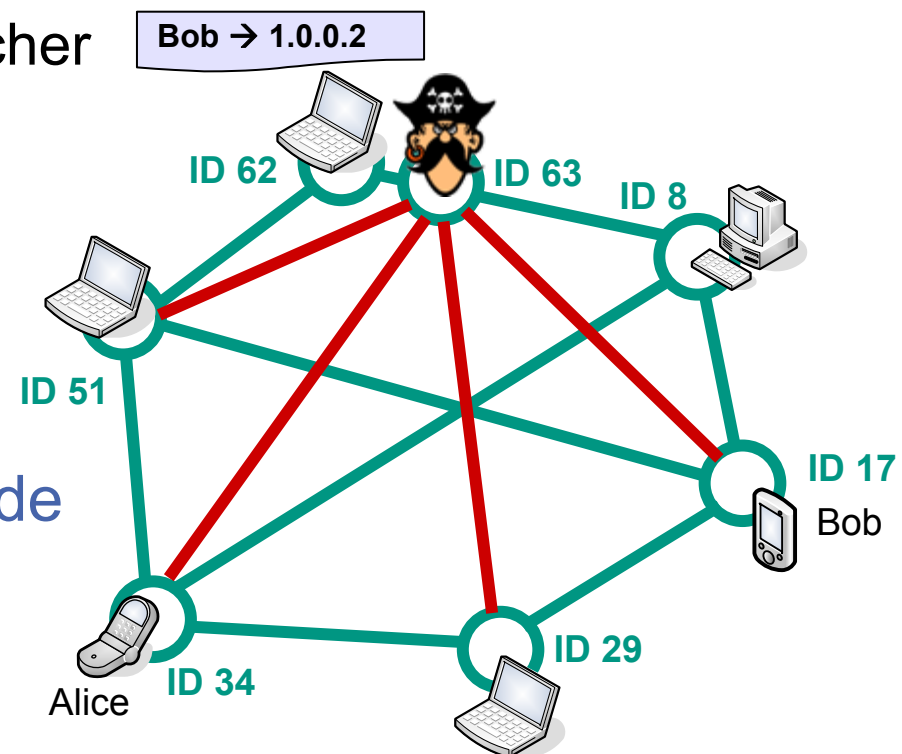


Sicherheitsmechanismen (KBR)

- Sichere NodeIDs zur Authentifizierung von Nachrichten
 - Freie NodeID-Erzeugung wird durch Kryptopuzzles beschränkt
 - Jede Nachricht enthält eine ECDSA-Signatur sowie den öffentlichen Schlüssel k_{pub} des Absenders (~60-100 Bytes)
- Sichere Routingtabellenwartung

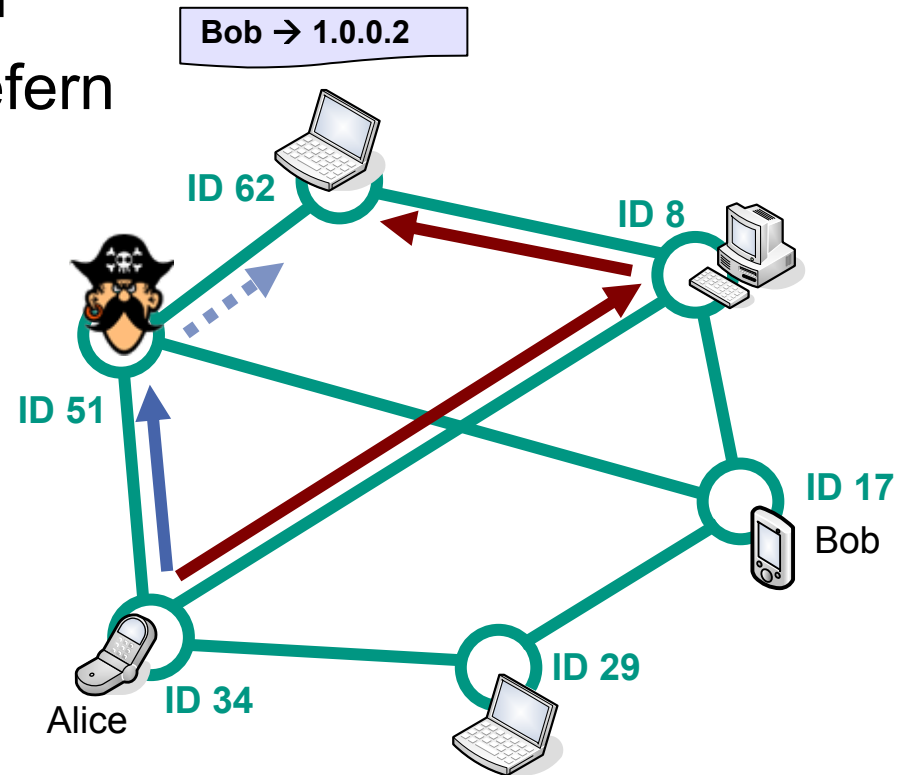
- Knoten werden erst nach erfolgreicher Authentifizierung eingetragen
- Neue Knoten werden nur in Routingtabelle aufgenommen, um ausgefallene Knoten zu ersetzen

- Iterativer Lookup über disjunkte Pfade



Iterativer Lookup über disjunkte Pfade

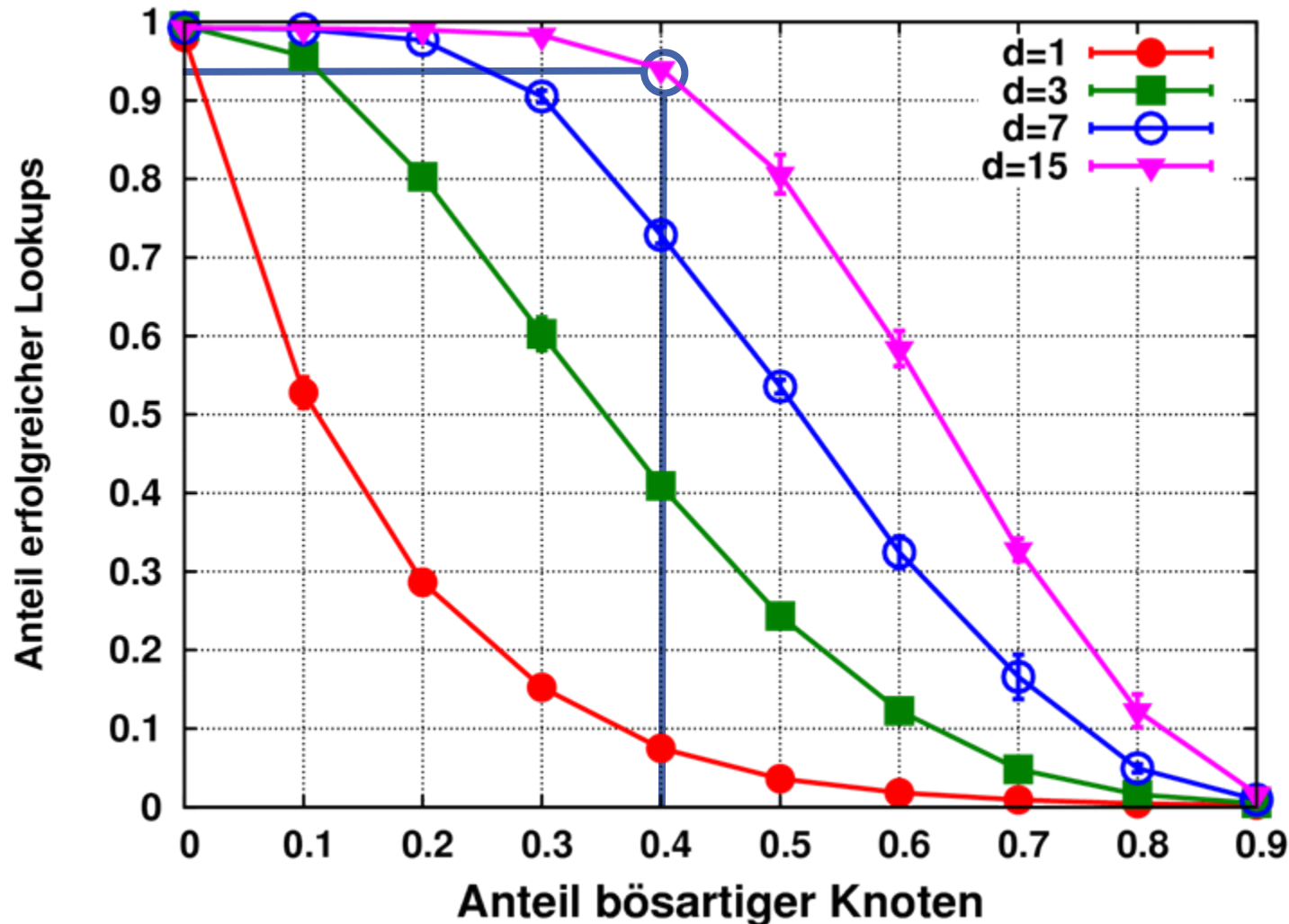
- Angreifer auf dem Lookup-Pfad kann
 - Keine Folgeknoten zurückliefern
 - Ungültige Folgeknoten zurückliefern
 - Den Lookup vorzeitig beenden
- Durch die parallele Verwendung von d disjunkten Lookup-Pfaden kann Lookup-Erfolgsrate gesteigert werden
- Lookup ist erfolgreich, sofern **mindestens ein** Pfad ohne bössartige Knoten verwendet wird:



$$p_{\text{lookup}}(m, h, d) = 1 - \left(1 - (1 - m)^h\right)^d$$

m Anteil Angreifer
 h Mittlere Pfadlänge
 d Anzahl disjunkter Pfade

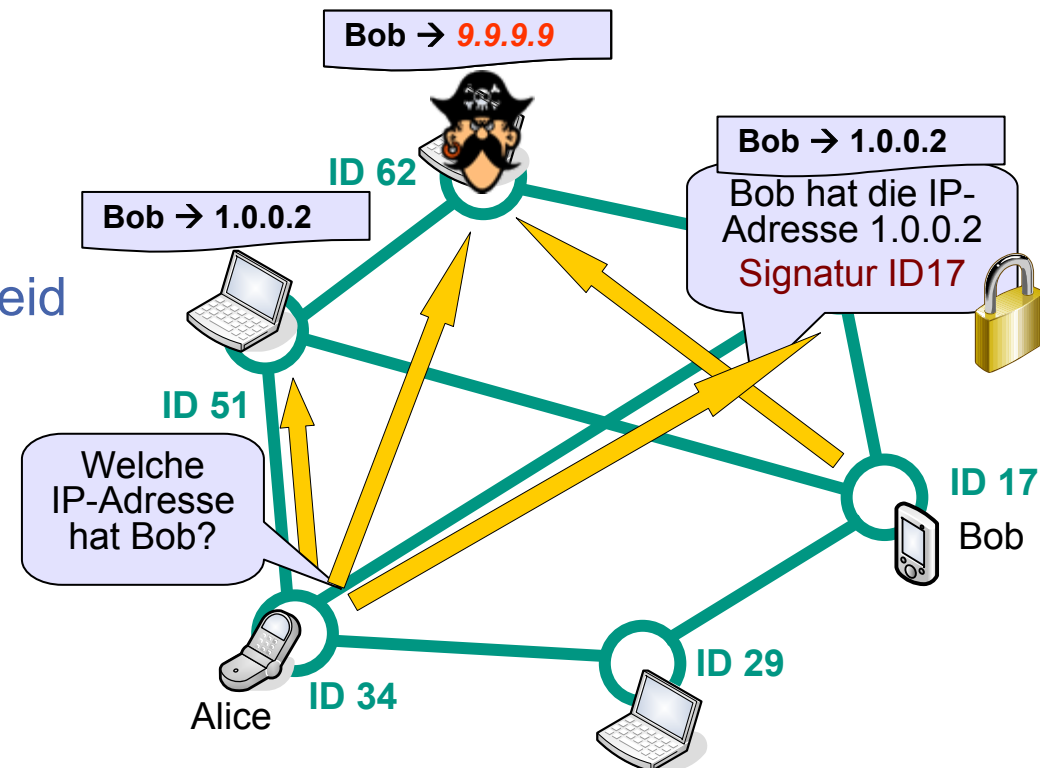
Lookup-Erfolgsrate mit disjunkten Pfaden



- Bei 40% bössartigen Knoten können mit $d=15$ Pfaden noch über 94% erfolgreiche Lookups erzielt werden ($N=10000$)

Sicherheitsmechanismen (DHT)

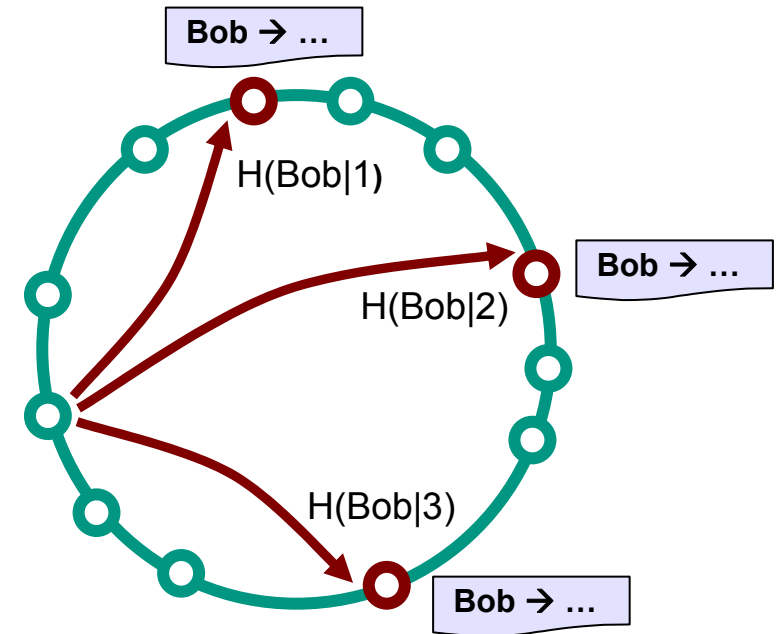
- Abgelegte Namenszuordnungen dürfen nur durch den **Eigentümer** des Namens verändert werden
 - Änderungswünsche werden mit k_{priv} des Eigentümers signiert
- Unter einem Hashwert darf nur eine **einzelne** Namenszuordnung abgelegt werden
 - Eindeutige Namen (First come first serve)
- Kontingentierungsverfahren
- Namenszuordnungen werden auf s Knoten **repliziert**
 - Parallele Abfrage aller Replikate mit **Mehrheitsentscheid**
 - Bei Knotenfluktuation erfolgt **sichere Datenwartung mit Mehrheitsentscheid**
 - Welche Knoten eignen sich für die Ablage der Replikate?



DHT-Replikationsvarianten (I)

■ Hash-Replikation

- Zuständige Knoten ergeben sich durch $H(\text{Name} \mid i)$ mit $i=1, \dots, s$
- Streuung der Hashfunktion führt mit hoher Wahrscheinlichkeit implizit zu disjunkten Pfaden
- Datenauffindung erfolgreich, falls die **Mehrheit** aller d Pfade gutartig:



$$P_{\text{total,hashRep}}(m, s) = \sum_{i=\lfloor \frac{s}{2} \rfloor}^s \binom{s}{i} \underbrace{\left(1 - (1 - m)^h\right)^{s-i}}_{\text{Pfad mit Angreifer}} \underbrace{\left(1 - m\right)^{h \cdot i}}_{\text{Pfad ohne Angreifer}}$$

m Anteil Angreifer
 s Anzahl Replikate
 h Mittlere Pfadlänge

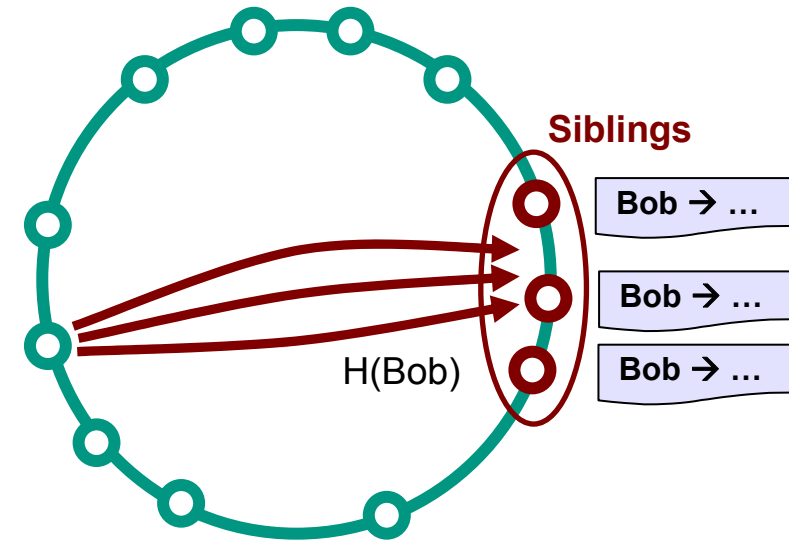
Pfad mit Angreifer

Pfad ohne Angreifer

DHT-Replikationsvarianten (II)

■ Sibling-Replikation

- Nächste s Knoten zu $H(\text{Name})$ sind zuständig (**Siblings**)
 - Symmetrische Nachbarschaft
- Mit iterativem Lookup über d disjunkte Pfade ist die Datenauffindung erfolgreich, falls
 - mindestens **ein** Pfad sowie
 - die Mehrheit der Replikationsknoten gutartig sind:



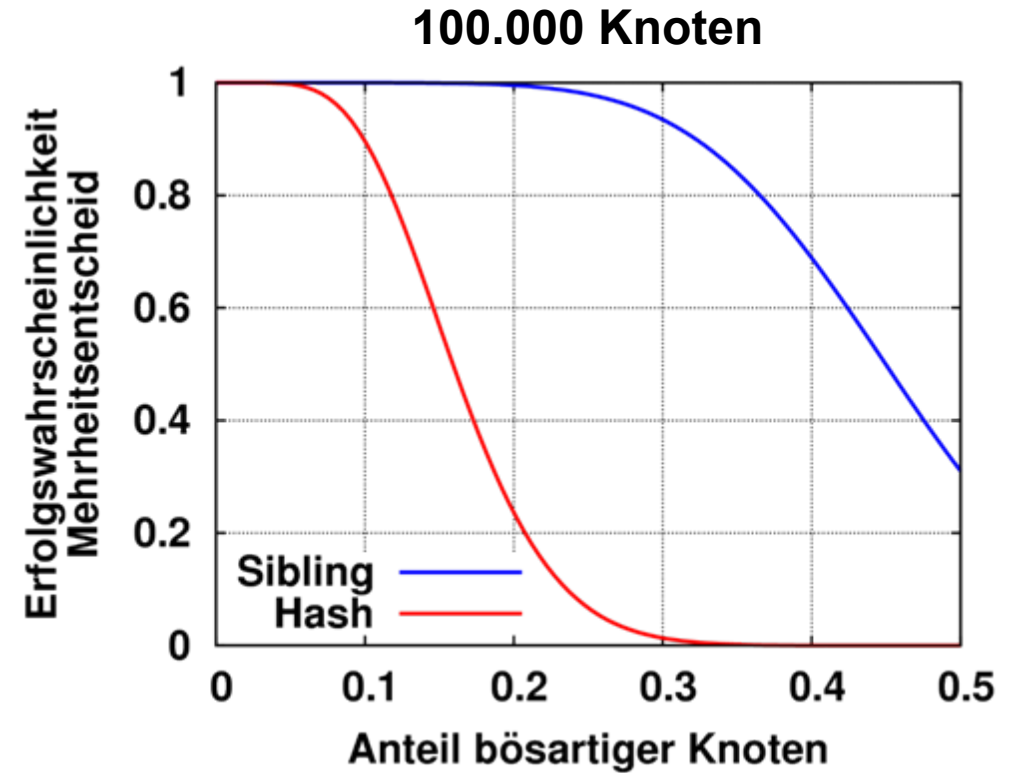
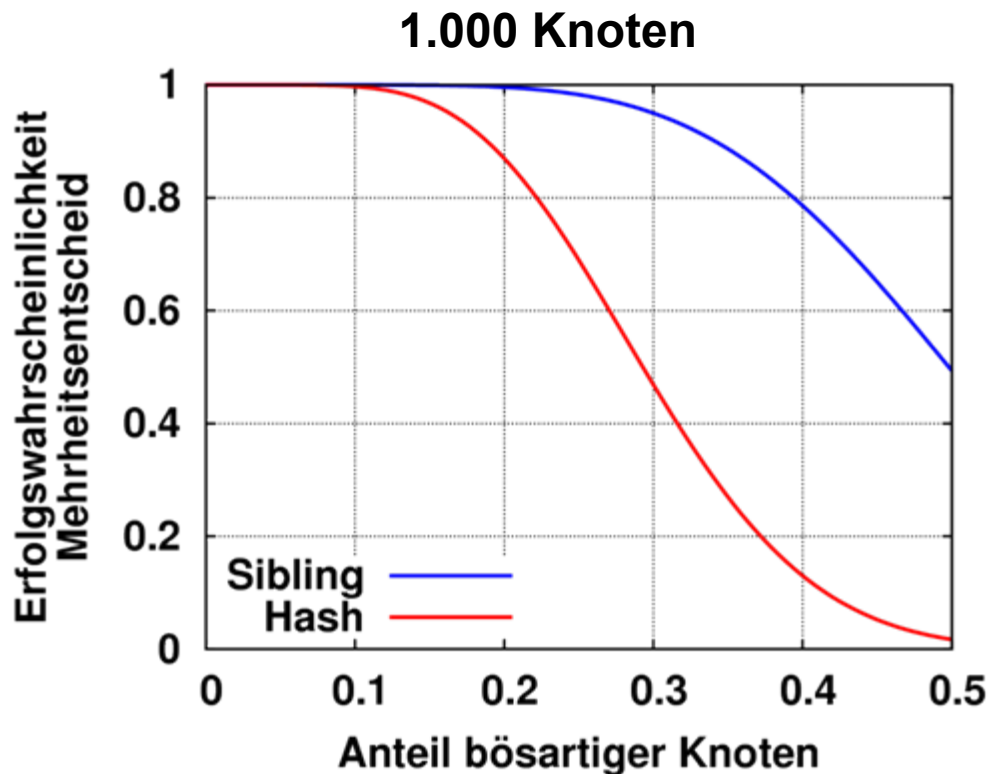
$$P_{\text{total,sibRep}}(m, d, s) = \underbrace{\left(1 - \left(1 - (1 - m)^h\right)^d\right)}_{\text{Mindestens ein Pfad ohne Angreifer}} \cdot \underbrace{\sum_{i=\lfloor \frac{s}{2} \rfloor}^s \binom{s}{i} m^{s-i} (1 - m)^i}_{\text{Mehrheit der Replikationsknoten gutartig}}$$

m Anteil Angreifer
 s Anzahl Replikate
 h Mittlere Pfadlänge
 d Anzahl disjunkter Pfade

Mindestens ein Pfad ohne Angreifer

Mehrheit der Replikationsknoten gutartig

DHT-Replikationsvarianten (III)



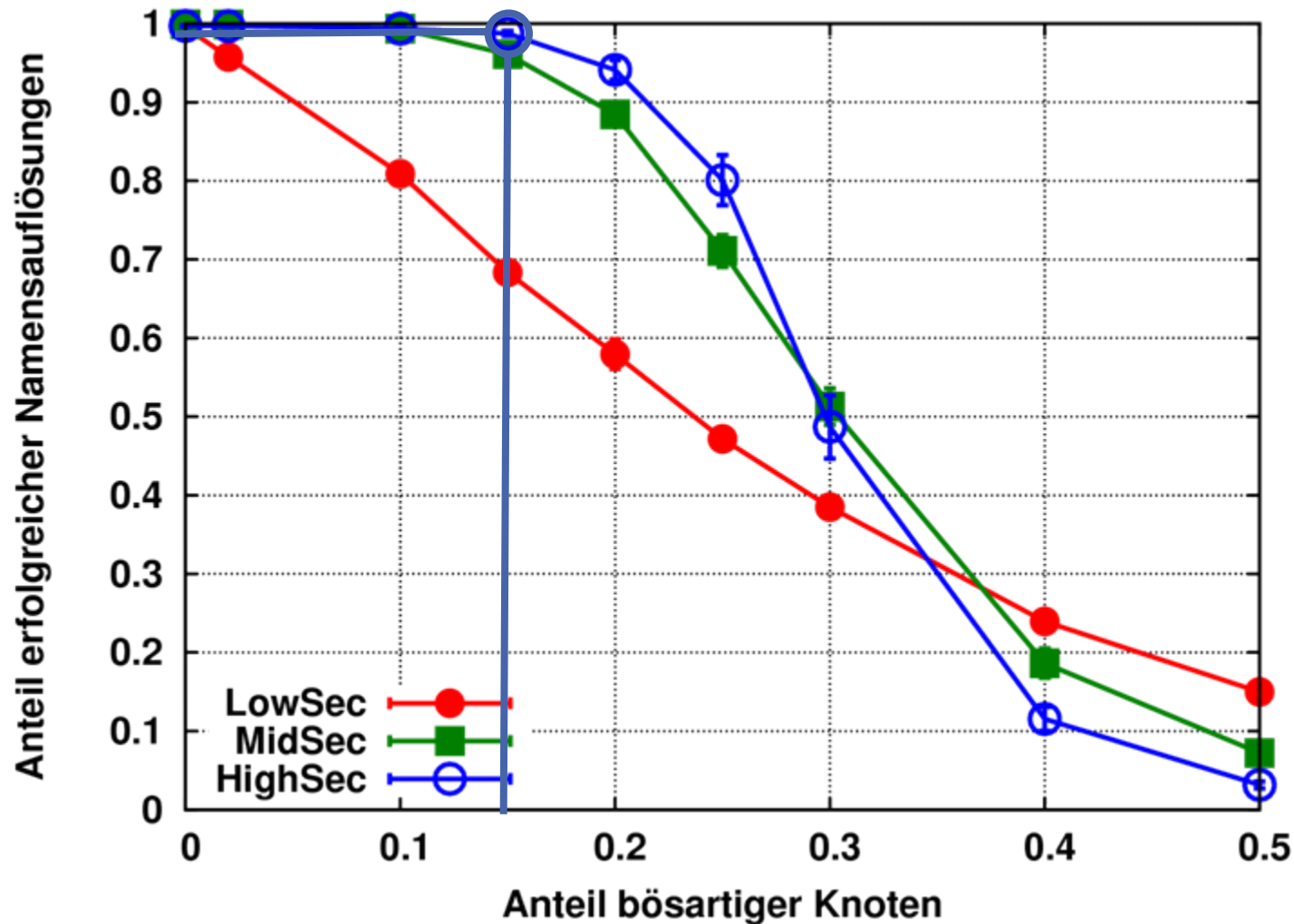
- Theoretische Wahrscheinlichkeit für $s=15$ Replikate und $d=15$ Pfade
- Mit der **Sibling-Replikation** lassen sich deutlich höhere Erfolgswahrscheinlichkeiten als mit der **Hash-Replikation** erzielen

Gesamtevaluation des Namensdienstes

- Standardszenario mit Simulation von Angreifern
- Simulationsablauf:
 - Jeder Knoten registriert einen Namen
 - Bei jedem Netzbeitritt wird die Namenszuordnung aktualisiert
 - Jeder Knoten führt pro Stunde zwei Namensauflösungen durch
- Verschiedene Parameterkombinationen für Sicherheit
 - Abwägung zwischen Zuverlässigkeit, Latenz und Kommunikationsaufwand
 - Ermittlung geeigneter Parameter anhand von Simulationsreihen:

	Disjunkte Pfade d	Anzahl Replikate s	Mehrheitsentscheid
LowSec	1	7	
MidSec	7	15	
HighSec	15	31	

Gesamtevaluation: Einfluss von Angreifern



- Bei 15% bössartiger Knoten können noch 99% aller Namensauflösungen erfolgreich durchgeführt werden

Zusammenfassung

- Dezentraler Namensdienst P2PNS bietet **generische Namensauflösung** für verschiedene Anwendungsszenarien
- Schwerpunkt auf **Sicherheit** des Namensdienstes in **vollständig dezentralen Umgebungen**
 - Ohne zentralen Vertrauensanker wird Sicherheit zentraler Systeme nicht erreicht
 - Für vielen Anwendungsfelder jedoch ausreichendes Sicherheitsniveau erzielbar
- **Ausblick**
 - Namensgebung und Adressierung im zukünftigen Internet
 - Detektion und Ausschluss bössartiger Knoten
 - Integration sozialer Vertrauensbeziehungen



Vielen Dank für die Aufmerksamkeit!

Fragen?

