# Analyse und Verbesserung von Routingprotokollen für Friend-to-Friend Overlays [1]

Stefanie Roos[2]

**Abstract:** Friend-to-Friend (F2F) Overlays beschützen Meinungsfreiheit und private Kommunikation im Angesicht Internet-weiter Überwachung und Zensur. Um Eingriffe in die digitale Kommunikation von Nutzer und deren Überwachung zu erschweren, geben Teilnehmer von F2F Overlays ihre Kontaktdaten nur an Teilnehmer weiter, mit denen sie eine wechselseitige in der physischen Welt begründete Vertrauensbeziehung verbindet. Diese restriktiven Verbindungsmöglichkeiten haben Auswirkungen auf die Flexibilität beim Aufrufen von Diensten. Das potentielle Ergebnis sind lange Wartezeiten und hoher Kommunikationsaufwand. Momentan existierte Friend-to-Friend Overlays werden auf Grund von langen Wartezeiten momentan nur wenig genutzt.

In dieser Arbeit untersuchen wir, ob dieser Mangel an Effizienz tatsächlich ein inhärentes Problem dieser Systeme ist oder ob lediglich die konzeptionellen Entscheidungen, die in den existierenden Systemen getroffen wurden, das Potential dieser Systeme nicht optimal nutzen. Insbesondere betrachten wir den Zusammenhang zwischen Vertraulichkeit, Verfügbarkeit, und Effizienz.

In der diesem Beitrag zu Grunde liegenden Dissertation analysieren wir zum einen existierende Systeme und identifizieren im Zuge dessen die konkreten Gründe für ihren Mangel an Performance. In diesem Zusammenhang spielt auch die Entwicklung von geeigneten Nutzermodellen und Evaluationsmethoden eine wichtige Rolle, da diese Methoden zukünftige Arbeiten erleichtern und eine bisher fehlende Basis zum Vergleich verschiedenere Ansätze schaffen. Zum anderen entwickeln wir VOUTE, Virtual Overlays Using Tree Embeddings, ein effizientes Friend-to-Friend Overlay, dass die Stärken zweier Ansätze, Virtual Overlays und Greedy Embeddings, kombiniert, während Effizienznachteile durch die Kombination weitgehend überwunden werden. Wir erreichen Verfügbarkeit und Vertraulichkeit durch weitere Schutzmaßnahmen, insbesondere eine Konstruktion für ausfall- und angriffsresistente Greedy Embeddings sowie ein Protokoll zur beweisbar anonymen Adressierung von Teilnehmern. Wir zeigen, dass die Kommunikationskosten zum Senden von Nachrichten sowie zum Erhalt der notwendigen lokalen Informationen (poly-)logarithmisch in der Anzahl an Teilnehmern ansteigen. Unsere praktische Evaluation bezeugt, dass VOUTE die Wartezeiten um mehr als einen Faktor 2 verringert und zusätzlich einen deutlich geringeren Kommunikationsaufwand aufweist. Gleichzeitig wird eine vergleichbare oder höhere Widerstandsfähigkeit gegen Zensur erreicht.

## 1 Hintergrund

Globale Kommunikationsnetze erlauben es weltweit zu publizieren und kommunizieren. Sie ermöglichen uns, Ideen und Einblicke mit potentiell Millionen oder gar Milliarden an Menschen zu teilen, ohne dafür einen hohen Aufwand an Zeit und finanziellen Mitteln aufbringen zu müssen. Insbesondere geben soziale Medien Minderheiten, Verfolgten, Aktivisten und Whistleblowern die Chance, auf kritische Situationen und Missachtung von Menschenrechten aufmerksam zu machen. Im Anschluss an solche Enthüllungen ermöglicht

[1] Originaltitel: Analyzing and Enhancing Routing Protocols for Friend-to-Friend Overlays, Doktorarbeit, Technische Universität Dresden, 2016

[2] University of Waterloo, sroos@uwaterloo.ca

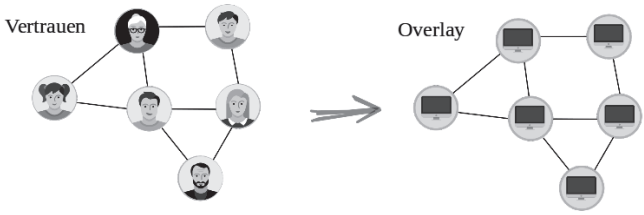



Abb. 1: Friend-to-Friend Overlay: Verbindungen auf Anwendungsebene spiegeln Vertrauensbeziehungen wieder

digitale Kommunikation die Organisation von lokalen oder globalen Hilfsaktionen und Protesten. Weitreichende digitale Überwachung durch Geheimdienste wie die NSA[3]und Zensur durch Regierungen wie im 'Arabischen Frühling'[4] untergraben diese wichtigen Möglichkeiten der freien Meinungsäußerungen.

Das grundlegende Problem im momentanen Internet ist die zentrale Kontrolle über angebotene Dienste. Die Existenz von wenigen globalen Dienstanbietern ermöglicht Überwachung und Zensur im großen Maße durch datenschutzrechtlich kritisch zu bewertende Gesetze[5], Hacking[6] oder den versehentlichen Verlust an sensitiven Nutzerdaten[7].

Als Alternative zu zentral kontrollierten Diensten gibt es eine Reihe an dezentralen Systemen wie Tor [DMS04], I2P [CS14], BitTorrent [Po05] und Diaspora[8], die es entweder erlauben, die existierenden Dienste anonym zu nutzen, oder alternative Dienste dezentral zur Verfügung stellen. Allerdings erlauben diese Systeme es, eine Vielzahl an scheinbar unabhängig aber in Wahrheit zentral kontrollierten Dienstanbietern in das System einzuschleusen. Diese kommunizieren dann mit echten Teilnehmern des Systems und beobachten oder zensieren deren Kommunikation. Sobald die Menge solcher zentral kontrollierten Teilnehmern die Teilnehmermenge dominiert, hat eine einzelne Partei wieder die Fähigkeit zur großflächigen Überwachung und Zensur. Des weiteren verlangt jedes dieser Systeme die Kommunikationen mit anderen unbekannten Teilnehmern, die kompromittiert sein können.

Friend-to-Friend Overlays (F2F Overlays) sind ein viel versprechender Ansatz, globale Kommunikation ohne Zensur und Überwachung zu realisieren. F2F Overlays, bildlich dargestellt in Abb. 1, sind Peer-to-Peer (P2P) Systeme, in denen Teilnehmer nur die Kontaktdaten, im Allgemeinen die IP Adresse, von anderen Teilnehmern nur erhalten, wenn sie mit diesen Teilnehmern eine wechselseitige Vertrauensbeziehung haben, die auf Interaktion in der physischen Welt beruht. Auf diese Art verbergen sie die Kontaktdaten eines Nutzer im

[3] http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
[4] https://www.journalism.co.uk/news-features/citizen-journalism-cyber-censorship-arab-spring/s5/a548289/
[5] http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-die-wichtigsten-texte-zum-comeback-der-vds-a-1068480.html
[6] https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0
[7] http://www.reuters.com/article/2013/06/21/us-facebook-security-idUSBRE95K18Y20130621
[8] https://diasporafoundation.org/

System vor nicht vertrauenswürdigen Teilnehmern und erschweren das Einschleusen von Teilnehmern deutlich.

Um tatsächlich eine nutzbare Alternative zu existierenden Systemen darzustellen, müssen F2F Overlays eine Vielzahl an Anforderungen erfüllen. Vertraulichkeit ist das grundlegende Ziel von F2F Overlays. Hier ist nicht nur die Vertraulichkeit von Inhalten ein Ziel, sondern vor allem der Schutz von Metadata. Es soll verborgen werden, wer wann mit wem kommuniziert und welche Inhalte publiziert oder aufruft. Auch die Teilnahme am Netzwerk und die Struktur des sozialen Graphen ist zu verbergen. Des weiteren müssen F2F Overlays resistent gegen Angriffen auf die Verfügbarkeit des Dienstes sein. Das Ziel ist, den Anteil an erfolgreichen Anfragen an einen Dienst zu maximieren. Ferner ist Effizienz und Skalierbarkeit von enormer Bedeutung, um Nutzer zu überzeugen, diese Dienste zu benutzen. Im Bereich von P2P Systemen haben sich polylogarithmische Schranken an Anfragedauer und -aufwand als realisierbar und angemessen schnell erwiesen, beispielsweise in BitTorrents verteilten Hashtabellen [CW07]. Zudem sollten Dienste gleichmäßig auf Nutzer verteilt werden, um Überbelastung und folglich Stau und Verzögerungen zu vermeiden. Nur wenn alle Anforderungen erfüllt sind, kann ein F2F Overlay ein sinnvolle Alternative zu momentanen Diensten anbieten.

Unser Beitrag liegt in der Entwicklung eines F2F Overlays, das die obigen Anforderungen an Vertraulichkeit, Verfügbarkeit und Effizienz erfüllt. Unser Vorgehen ist in drei Schritte gegliedert. Zunächst erarbeiten wir sinnvolle Annahmen an Nutzer und Angreifer sowie Methoden zur Evaluation von Lösungsvorschlägen. Auf Basis dieser beurteilen wir im zweiten Schritt existierende Ansätze, insbesondere Virtual Overlays und Greedy Embeddings, ein allgemeiner Ansatz für das effiziente Finden von Routen in Netzen mit Konnektivitätseinschränkungen. Wir zeigen, dass keiner der Ansätze unseren Anforderungen genügt und identifizieren die exakten Gründe. Der dritten Schritt ist die Entwicklung und Evaluation von VOUTE, Virtual Overlays Using Tree Embeddings. VOUTE kombiniert die Vorteile von Virtual Overlays und Greedy Embeddings mit erweiternden Schutzmaßnahmen zur Erhöhung von Vertraulichkeit und Verfügbarkeit. Eine besondere Stärke der Arbeit liegt in der multi-dimensionalen Auswertung. Wir erarbeiten realistische Nutzermodelle durch automatisierte Messungen von mehreren tausend Nutzern in Freenet [Cl10], einem anonymen Kommunikationsnetzwerk. Im Zuge dessen erarbeiten wir Verbesserungen für Freenets momentane Algorithmen und integrieren sie in das System. Basierend auf den Ergebnissen evaluieren wir existierende und eigene Ansätze in weit reichenden Simulationsstudien. Wir beweisen die Skalierbarkeit unserer Ansätze durch asymptotische Schranken beruhend auf graph-theoretischen und stochastischen Überlegungen. Des weiteren evaluieren wir die Anonymität und Angriffsresistenz theoretisch. In den folgenden Abschnitten fassen wir unsere Ergebnisse zusammen und betonen bedeutende Erkenntnisse. Für die Details der entwickelten Algorithmen und ihrer Evaluation, verweisen wir auf eine Vielzahl an Publikationen in angesehenen Konferenzen wie INFOCOM und PETs sowie Journalen [HRS13, Ro14a, Ro14b, RNS15, RS15, RBS16, RS16, Ro17].

## 2 Annahmen und Methoden

Unser erster Beitrag besteht in der Erarbeitung von Nutzermodelle und Methoden. Wir beginnen mit einer allgemeinen Definition der notwendigen Algorithmen. F2F Overlays realisieren eine Vielzahl an Anwendungen, die alle auf zwei fundamentalen Funktionalitäten basieren. Erstens schicken Nutzer Nachrichten zu anderen Nutzern, mit denen sie nicht notwendigerweise eine Vertrauensbeziehung haben. Typische Beispiele sind ein Aktivist und ein Journalist oder zwei Nutzer eines Gesundheitsforums. Die zweite Funktionalität ist das Veröffentlichen und Aufrufen von Inhalten. Knoten und Inhalte werden anhand ihrer Adresse gefunden. Eine weitere wichtige Eigenschaft eines P2P Systems ist der Umgang mit dynamischen Nutzermengen. Teilnehmer, im Folgenden als Knoten in einem Netzwerk repräsentiert, sind im Allgemeinen nicht konstant online. Das Netzwerk muss sich stabilisieren, sobald ein Knoten online oder offline geht. Dadurch ergeben sich 6 Algorithmen, aufgeführt in Tab. 1.

| | |
|---|---|
| $\mathbf{AdGen}_{node}(e)$ | Adressengenerierung für Knoten $e$ |
| $\mathbf{R}_{node}(s, \mathbf{AdGen}_{node}(e))$ | Routing von $s$ zu $e$ |
| $\mathbf{AdGen}_{content}(c)$ | Adressengenerierung für Inhalt $c$ |
| $\mathbf{R}_{content}(s, \mathbf{AdGen}_{content}(c))$ | Routing $s$ zu einem Knoten der $c$ speichert |
| $\mathbf{S}_J(v)$ | Stabilisierung nachdem $v$ beitritt |
| $\mathbf{S}_D(v)$ | Stabilisierung nachdem $v$ austritt |

Tab. 1: Algorithmen für grundlegende Funktionalitäten

Wir gehen davon aus, dass Adressen lokal generiert werden und daher keinen Kommunikationsaufwand verursachen. Für die Routing- und Stabilisierungsalgorithmen fordern wir polylogarithmische Kommunikationskomplexität. Wir modellieren einen Angreifer, der versucht durch Manipulation dieser Algorithmen die Identität von Nutzer zu ermitteln oder die Verfügbarkeit zu unterwandern. Wir gehen von einem lokalen, internen, und aktiven Angreifer aus, der Algorithmen durch Verwerfen, Fälschen, Wiedereinspielen und Verändern von Nachrichten manipuliert. Der Angreifer kann eine beliebige Menge an Knoten in das System integrieren, aber die Anzahl an Verbindungen zu ehrlichen Teilnehmern ist gering. Diese Bedingung spiegelt die Schwierigkeit Vertrauensbeziehungen aufzubauen wieder und die Stärke des Angreifers ist durch die Anzahl an Kanten zu ehrlichen Knoten definiert. Dieses Angreifermodell ist stärker als externe oder honest-but-curious Angreifer, die das System nur beobachten oder dem Protokoll folgen.

Unsere Methodenentwicklung bedenkt zwei Aspekte. Zum einen passen wir Methoden aus P2P Systemen an die restriktive Natur von Verbindungen in F2F Overlays an. Des weiteren sind die Komplexitäten der Routing- und Stabilisierungsalgorithmen im Allgemeinen abhängig und verändern sich potentiell über die Zeit. Wir modellieren die verschiedenen Kommunikationskomplexitäten als korrelierte stochastische zeitliche Prozesse.

Unsere Nutzermodelle beschäftigen sich vordergründig mit der Struktur des sozialen Graphen der Vertrauensbeziehungen und der typischen Sitzungslänge. Hier bezeichnet Sitzungslänge die Zeit zwischen einem Eintritt und folgenden Austritt aus dem Netzwerk. Wir gehen von verbundenen sozialen Graphen aus, da sonst kein Nachrichtenfluss möglich ist. Ferner ist der Durchmesser von sozialen Graphen meist gering. Wir gehen davon aus,

dass der längste kürzeste Pfad zwischen zwei Knoten höchstens logarithmisch mit der Knotenanzahl skaliert. Modelle für Sitzungslängen lassen sich mit großer Genauigkeit in Freenet [Cl01] gewinnen, wie im folgenden skizziert. Freenetteilnehmer haben persistente Pseudonyme und Teilnehmer können Pseudonyme anderer zufällig gewählter Teilnehmer anfragen. Eine große Anzahl an solcher Anfragen von verschiedenen instrumentierten Freenetknoten, die wir in das Netzwerk eingebunden haben, erlauben mit hoher Genauigkeit festzustellen, ob ein Nutzer online ist. Durch Abstraktion der konkreten Daten zu Verteilungen lassen sich verallgemeinerte Modelle erstellen. Wir beobachteten in einem Zeitrahmen von 9 Tagen mehr als 10,000 Nutzer, von denen im Schnitt 3500 parallel Freenet nutzten. Je nachdem wie hoch wir unsere Sicherheit in die Hypothese, dass ein Knoten nicht online ist, wählen, ergeben sich Sitzungslängen zwischen 49 und 110 Minuten. Die empirischen Verteilungen der Sitzungslänge lassen sich gut durch Lognormal- oder Weibullverteilungen modellieren.

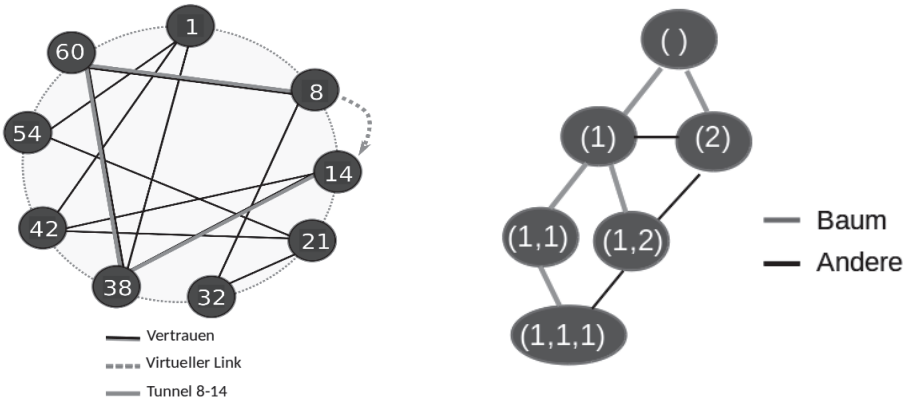
Diese Nutzermodelle und Methoden bilden die Grundlage für die praktischen und theoretische Evaluation in den folgenden Sektionen.

## 3 Evaluation existierender Ansätze

Im zweiten Beitrag beurteilen wir existierende Ansätze auf der Basis der entwickelten Methoden und Modelle. Insbesondere betrachten wir die Ansätze Virtual Overlays und Greedy Embeddings. Abb. 2 illustriert die zwei Konzepte.

Außer diesen Konzepten existieren es auch verschiedene F2F Overlays, die sich auf Filesharing konzentrieren. Unstrukturierte Ansätze wie Turtle [Po06] und OneSwarm [Is10] eignen sich für das Teilen von Inhalten, die von einer Vielzahl an Teilnehmer gespeichert werden, aber sie sind zu ineffizient für andere Anwendungen wie Chats. GnuNet's 2-Phasen-Routing [EG11], das Inhalte vielfach replizieren muss, um diese verlässlich finden zu können, ist ebenso eingeschränkt. Der F2F Modus des bekannten zensurresistenten anonymen Kommunikationssystem Freenet [Cl10] hat sich in der Praxis und durch theoretische Evaluation als ineffizient erwiesen [Va09, RS13].

Virtual Overlays orientieren sich an strukturieren P2P Systemen wie Chord [St01]. Strukturierte Systeme ordnen ihre Knoten in Topologien wie Ringen oder Bäumen an, die einfache und effiziente Protokolle zur Routenfindung erlauben. Diese Anordnung beruht auf dem Anpassen von Verbindungen auf der Anwendungsebene und ist nicht ohne die Preisgabe von IP Adressen nicht in dieser Form möglich. Virtual Overlays ersetzen daher eine einzelne Verbindung auf der Anwendungsebene durch einen Tunnel bestehend aus mehreren Verbindungen im F2F Overlay, wie in Abb. 2a dargestellt. Dies ermöglicht die Anwendung von Routingalgorithmen, die diese Tunnel wie Kanten in einem strukturierten System benutzen. Eine besondere Herausforderung ist das Aufrechterhalten dieser Tunnel bei Knoteneintritten -und austritten. MCON [Va09] flutet das Netzwerk für die Tunnelkonstruktion, das heißt Nachrichten werden zu allen Nachbarn weitergeleitet bis Knoten mit geeigneten zufällig gewählten Adressen gefunden wurden. X-Vine [MCB12] basiert auf einem effizienteren Stabilisierungsprotokoll: Knoten nutzen das Routingprotokoll um




(a) Virtual Overlays (b) Greedy Embeddings

Abb. 2: Existierende Ansätze: Virtual Overlays ersetzen benötigte Verbindungen zwischen Teilnehmern ohne Vertrauensbeziehung durch Pfad aus sich wechselseitig vertrauenden Teilnehmern. Greedy Embeddings weisen Teilnehmern Adressen auf Basis ihrer Position in einem Spannbaum zu.

neue virtuelle Nachbarn zu finden. Der neue Tunnel entspricht der Konkatenation der Tunneln auf dem gefundenen Pfad. Es ist unklar wie sich das über einen längeren Zeitraum auf die Länge der Tunnel auswirkt.
Unser Beitrag liegt zunächst in der Entwicklung eines allgemeinen Modells für Virtual Overlay. Im Rahmen dieses Modells beweisen wir, dass jedes Virtual Overlay, das auf Tunneln basiert, entweder einen hohen Stabilisierungsaufwand hat oder über die Zeit die Tunnellänge und damit die Routinglänge ansteigt. Die Idee des Beweises ist, zunächst von im Mittel polylogarithmisch skalierenden Stabilisierungskomplexität auszugehen. Dann betrachten wir Routingkomplexität und Stabilisierungskomplexität als stochastische zeitliche Prozesse. Es lässt sich zeigen, dass die Routingkomplexität über die Zeit tendenziell zunimmt, bis sie nicht mehr polylogarithmisch in der Anzahl an Knoten ist. Demnach können Virtual Overlays nicht langfristig effizient sein [RS15].

Greedy Embeddings dagegen sind vordergründig für effizientes Routing in Netzwerken mit unabänderlichen Verbindungen wie Sensornetze konstruiert [PR04, Kl07]. Wie in Abb. 2b für Prefix Embedding [HRS13] dargestellt, wird zunächst ein Spannbaum konstruiert. Dann wird die Position der Knoten im Spannbaum durch eine Adresse widergespiegelt, in unserem Beispiel ist diese Adresse ein Vektor, der aus der Adresse des Elternknotens und eines Enumerationsindex besteht. Knoten veröffentlichen diese Adressen und können über sie kontaktiert werden. Jeder Knoten auf dem Pfad leitet die Nachricht an den Nachbarn weiter, der den kürzesten Pfad im Spannbaum zum Zielknoten aufweist. Die Kommunikationskomplexität skaliert demnach linear in der Baumtiefe, die im Allgemeinen logarithmisch in der Knotenanzahl skaliert. Im Mittel ist effiziente Stabilisierung erreichbar, da der Spannbaum lokal repariert werden kann und eine komplette Neuberechnung nur bei Austritt der Wurzel nötig ist. Demnach sind Routing und Stabilisierung effizient möglich.
Wir untersuchen, ob Inhalte in Greedy Embeddings gleichmäßig über Knoten verteilt werden können. Wir zeigen, dass dies im Allgemeinen nur möglich ist, wenn die Anzahl an

Knoten in einen Unterbaum gut approximiert werden kann [Ro17]. Selbst wenn diese Angaben sich nicht negativ auf die Vertraulichkeit auswirken würden, muss der Algorithmus zur Ermittlung dieser Zahlen resistent gegen Manipulation sein and damit Byzantine Agreement [LSP82] garantieren. Die regelmäßige Ausführung eines Algorithmus zum Byzantine Agreement lässt sich nicht mit unseren Anforderungen an die Effizienz vereinbaren. Demnach sind Greedy Embeddings nicht fähig, Inhalte angemessen zu verteilen, und jegliche Anpassung der momentanen Ansätze würde entweder Schwachstellen oder ineffiziente Schutzmaßnahmen nach sich ziehen.

| System | Routinglänge |
|---|---|
| Freenet | $\approx 10.000,0$ |
| MCON | $14,0$ |
| Prefix | $6,2$ |
| Shortest Paths | $4,3$ |

Tab. 2: Vergleich der Länge der gefundene Pfade zwischen Start- und Endpunkten für diverse Ansätze

| System | Stabilisierungsaufwand |
|---|---|
| Freenet | NA |
| MCON | $> 600000,0$ |
| Prefix | $4,5$ |

Tab. 3: Vergleich Stabilisierungskosten für Ein- und Austritte für diverse Ansätze

Simulation-basierte Ergebnisse bezüglich Virtual Overlays und Greedy Embeddings sind in Tab. 2 und 3 zu finden. Die Ergebnisse beruhen auf einen Untergraphen von Facebook mit ungefähr 64.000 Knoten und über 600.000 Kanten. Die Mittelwerte wurden über 20 Experimente mit je 10.000 zufälligen gewählten Start- und Endpunkten beziehungsweise ausfallenden Knoten ermittelt. Auf Grund der periodischen Stabilisierung in Freenet ist ein Vergleich mit MCON und Prefix, die auf Eintritte und Austritte direkt reagieren, nicht direkt möglich. Jedoch ist die Ineffizienz von Freenet allein auf Grund der langen Pfade gegeben, wie Tab. 2 zeigt. Greedy Embeddings wie Prefix Embedding erreichen geringe Pfadlängen und Stabilisierungskosten, jedoch zeigen andere Arbeiten ihre schlechten Lastverteilung beim Speichern von Inhalten [Ro14b, Ro17].

Zusammenfassend zeigen unsere Ergebnisse, dass Virtual Overlays inhärent ineffizient sind. Dagegen weisen Greedy Embeddings drastische Schwächen in der Lastverteilung auf.

## 4 VOUTE: Virtual Overlays Using Tree Embeddings

Unser dritter und bedeutendster Beitrag liegt in der Entwicklungen von VOUTE [RBS16], Virtual Overlays Using Tree Embeddings, einem F2F Overlay, das die Schwächen der vorherigen Ansätze durch eine Kombination der beiden Ansätze überwindet. VOUTE ist vor allem durch die folgenden 3 Beiträge gekennzeichnet:

- ein resistenten Routingprotokoll $\mathbf{R}_{node}$ basierend auf parallelen Greedy Embeddings sowie dessen theoretische und praktische Evaluierung
- ein Protokoll zur Generierung von anonymen Adressen, welche die Identität des Empfängers und die Topologie verbergen, sowie der entsprechenden Anonymitätsbeweis, und

- ein Algorithmus $\mathbf{R}_{content}$ zum Speichern und Aufrufen von Inhalten, der strukturierte Overlays auf Basis von Adressen im Greedy Embedding realisiert

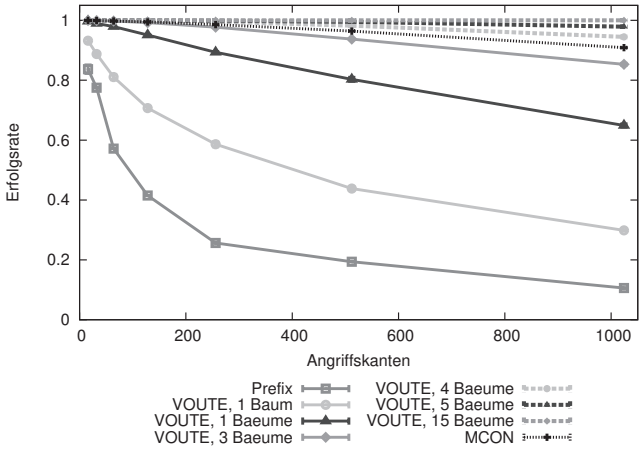



Abb. 3: Verschiedene Parameterwahlen für $\mathbf{R}_{node}$ und ihr Einfluss auf die Erfolgsrate

Unser erster Beitrag besteht in der Konstruktion des Routingalgorithmus $\mathbf{R}_{node}$. Wir nutzen Prefix Embedding, um den Knoten Adressen zuzuweisen. Jedoch ist Prefix Embedding nicht auf Ausfall- und Angriffsresistenz ausgelegt. Wir erhöhen diese indem wir dem Routingalgorithmus einen Backtracking Modus hinzufügen, der alternative Pfade bedenkt. Ferner modifizieren wir den Routingalgorithmen, sodass er bevorzugt nicht über die Wurzel des Baums weiterleitet und dadurch den Einfluss dieses einzelnen ausgewählten Teilnehmers reduziert. Unsere einflussreichster Neuerung hier ist die Entwicklung eines rundenbasierten probabilistischen Spannbaumprotokolls, das parallel mehrere Spannbäume mit möglichst diverser Elternwahl aufbaut. Knoten wählen Elternknoten, die sich nicht zuvor in anderen Bäumen gewählt haben. Wenn sie keinen solchen Elternknoten zur Wahl haben, entscheiden sie probabilistisch, ob sie auf weitere Einladungen warten oder einen bereits zuvor gewählten Elternknoten mehrfach auswählen. Wir zeigen, dass die Tiefe der Bäume maximal linear in der Anzahl an Bäumen ansteigt. Daraus folgt, dass die Routinglänge maximal linear in der Anzahl der Bäume wächst während Routing- und -Stabilisierungskosten quadratisch in der Anzahl an Bäumen ansteigen. Abb. 3 zeigt die erhöhte Verfügbarkeit im Vergleich zu der Anzahl der vom Angreifer kontrollierten Kanten beispielhaft. In diesem Fall brauchen wir vier parallele Spannbäume, um eine höhere Erfolgsrate als Virtual Overlays wie MCON zu erreichen. Tab. 2 deutet an, dass die vierfachen Routingkosten für Greedy Embeddings die Kosten in MCON übersteigen. Jedoch bleibt die Stabilisierung um ein Vielfaches effizienter. Demnach erreicht unser neuer Algorithmus eine hohe Verfügbarkeit und Effizienz.

Die Adressen in Prefix Embedding erlauben jedoch die Rekonstuktion der Spannbäume und damit großer Teile des sozialen Graphen. Ferner geben sie die Identität des Empfängers preis. Um dies zu verhindern, randomisieren wir zum einen die Elemente des Adressvektors. Zum anderen geben Knoten statt ihrer Adresse nur eine anonyme Rückadresse preis.

Diese wird durch Auffüllen des Vektors auf eine konstante Länge und das Hashen der Vektorelemente gebildet. Knoten behalten die Möglichkeit zu routen, da sie durch Hashen der Nachbaradressen gemeinsame Adressprefixe feststellen können. Jedoch werden weitere Informationen über die Adresse verborgen und Sender und Empfänger werden beweisbar anonymisiert. So erreichen wir Vertraulichkeit zusätzlich zu Effizienz und Verfügbarkeit.

Des Routingalgorithmus $\mathbf{R}_{content}$ nutzt die (anonyme) Adressen als Grundlage für ein strukturiertes Overlay. Nachbarn in diesem Overlay können über ihre Adressen in den unterliegenden Greedy Embeddings kommunizieren. Dadurch wird der Tunnelaufbau vermieden und die uniforme Lastenverteilung des strukturierten Overlays kann zum Speichern und Aufrufen von Inhalten genutzt werden. Auf diese Art erreichen wir Effizienz im Sinne von geringer Kommunikationkomplexität und fairer Lastverteilung.

Gemeinsam ermöglichen die obigen Beiträge den Nachrichtenaustausch und das Teilen von Inhalten in einem F2F Overlay. VOUTE ist effizient, resistent gegenüber Denial-of-Service-Angriffen und schützt die Kommunikationsdaten von Teilnehmern.

## Literaturverzeichnis

[Cl01] Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hong, Theodore: Freenet: A Distributed Anonymous Information Storage and Retrieval System. In: Designing Privacy Enhancing Technologies. 2001.

[Cl10] Clarke, Ian; Sandberg, Oskar; Toseland, Matthew; Verendel, Vilhelm: Private Communication through a Network of Trusted Connections: The Dark Freenet. Network, 2010.

[CS14] Conrad, Bernd; Shirazi, Fatemeh: A Survey on Tor and I2P. In: ICIMP. 2014.

[CW07] Crosby, Scott A; Wallach, Dan S: An Analysis of BitTorrent's Two Kademlia-based DHTs. Bericht, Technical Report TR07-04, Rice University, 2007.

[DMS04] Dingledine, Roger; Mathewson, Nick; Syverson, Paul: Tor: The Second-generation Onion Router. Bericht, DTIC Document, 2004.

[EG11] Evans, Nathan S; Grothoff, Christian: R5N: Randomized Recursive Routing for Restricted-route Networks. In: NSS. 2011.

[HRS13] Hoefer, Andreas; Roos, Stefanie; Strufe, Thorsten: Greedy Embedding, Routing and Content Addressing for Darknets. In: NetSys. 2013.

[Is10] Isdal, Tomas; Piatek, Michael; Krishnamurthy, Arvind; Anderson, Thomas: Privacy-preserving P2P Data Sharing with ONESWARM. In: ACM SIGCOMM Computer Communication Review. Jgg. 40, 2010.

[Kl07] Kleinberg, Robert: Geographic Routing using Hyperbolic Space. In: INFOCOM. 2007.

[LSP82] Lamport, Leslie; Shostak, Robert; Pease, Marshall: The Byzantine Generals Problem. TOPLAS, 4(3), 1982.

[MCB12] Mittal, Prateek; Caesar, Matthew; Borisov, Nikita: X-Vine: Secure and Pseudonymous Routing in DHTs Using Social Networks. In: NDSS. 2012.

[Po05] Pouwelse, Johan A.; Garbacki, Pawel; Epema, Dick H. J.; Sips, Henk J.: The BitTorrent P2P File-Sharing System: Measurements and Analysis. In: IPTPS. 2005.

[Po06] Popescu, Bogdan: Safe and Private Data Sharing with Turtle: Friends Team-up and Beat the System. In: Security Protocols. 2006.

[PR04] Papadimitriou, Christos H; Ratajczak, David: On a Conjecture Related to Geometric Routing. In: Algorithmic Aspects of Wireless Sensor Networks. 2004.

[RBS16] Roos, Stefanie; Beck, Martin; Strufe, Thorsten: Anonymous Addresses for Efficient and Resilient Routing in F2F Overlays. In: INFOCOM. 2016.

[Rh03] Rhea, Sean; Geels, Dennis; Roscoe, Timothy; Kubiatowicz, John: Handling Churn in a DHT. Computer Science, 2003.

[RNS15] Roos, Stefanie; Nguyen, Giang T; Strufe, Thorsten: Integrating Churn into the Formal Analysis of Routing Algorithms. In: NetSys. 2015.

[Ro14a] Roos, Stefanie; Schiller, Benjamin; Hacker, Stefan; Strufe, Thorsten: Measuring Freenet in the Wild: Censorship-resilience under Observation. In: PETS. 2014.

[Ro14b] Roos, Stefanie; Wang, Liang; Strufe, Thorsten; Kangasharju, Jussi: Enhancing Compact Routing in CCN with Prefix Embedding and Topology-aware Hashing. In: MobiArch. 2014.

[Ro17] Roos, Stefanie; Byrenheid, Martin; Deusser, Clemens; Strufe, Thorsten: BD-CAT: Balanced Dynamic Content Addressing in Trees. In: INFOCOM. 2017.

[RS13] Roos, Stefanie; Strufe, Thorsten: A Contribution to Analyzing and Enhancing Darknet Routing. In: INFOCOM. 2013.

[RS15] Roos, Stefanie; Strufe, Thorsten: On the Impossibility of Efficient Self-Stabilization in Virtual Overlays with Churn. In: INFOCOM. 2015.

[RS16] Roos, Stefanie; Strufe, Thorsten: Dealing with Dead Ends-Efficient Routing in Darknets. TOMPECS, 1(1), 2016.

[St01] Stoica, Ion; Morris, Robert; Karger, David; Kaashoek, M Frans; Balakrishnan, Hari: Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications. ACM SIGCOMM Computer Communication Review, 31(4), 2001.

[Va09] Vasserman, Eugene; Jansen, Rob; Tyra, James; Hopper, Nicholas; Kim, Yongdae: Membership-concealing Overlay Networks. In: CCS. 2009.

**Stefanie Roos** forscht im Bereich Datenschutz und verteilte Systeme, bevorzugt sogar Datenschutz in oder durch verteilten Systeme. Insbesondere beschäftigt sie sich mit dem Zusammenhang zwischen Datenschutz, Verfügbarkeit und Performance. Sie ist bekannt für ihre Arbeit an Friend-to-Friend Overlays. Der Einfluss ihrer Arbeit zeigt sich in zahlreichen Veröffentlichungen in Konferenzen wie INFOCOM und PETS sowie der praktischen Umsetzung der von ihr erdachten Protokolle in reellen Systemen wie Freenet. Momentan ist Stefanie ein Post-doctoral Fellow an der University of Waterloo, Kanada, wo sie zusammen mit Ian Goldberg an Performancesteigerungen des Anonymisierungdienstes Tor sowie des verteilten Transaktionsnetzwerk Ripple arbeitet. Im Juli 2016 erhielt sie ihren Doktortitel (Dr. rer. nat., Note: summa cum laude) von der Technischen Universität Dresden für die Arbeit ‘Analyzing and Enhancing Routing Protocols for Friend-to-Friend Overlays’, betreut von Thorsten Strufe.