Anonymität und Mehrwegeübertragung

Raphael Wigoutschnigg

Alpen-Adria-Universität Klagenfurt
Raphael.Wigoutschnigg@aau.at

Zusammenfassung

Die meisten Anonymisierungsprotokolle basieren darauf, einen einzelnen Kommunikationskanal zwischen Sender und Empfänger aufzubauen. In dieser Arbeit wird der Einfluss von Mehrwegeübertragung (mehrere Kommunikationskanäle) auf die Anonymitätseigenschaften von Sender und Empfänger untersucht. Hierfür wird ein exemplarisches Protokoll mittels Simulationen analysiert. Es wird gezeigt, dass Mehrwegeübertragung gewinnbringend zum Schutz des Empfängers eingesetzt werden kann. Zusätzlich werden potentiell gefährliche Designentscheidungen bei der Verwendung von Mehrwegeübertragung identifiziert.

1 Einleitung

In Zeiten massiver Überwachung einerseits durch Geheimdienste, andererseits durch private Firmen rückt das Thema der Privatsphäre immer mehr in das Zentrum des Interesses der Benutzer digitaler Kommunikationsmedien. Zum Schutz der Privatsphäre werden immer häufiger Systeme zur anonymen Kommunikation eingesetzt (z.B. Tor [DiMS04]). Je nach Anwendungsfall ist es wünschenswert, den Sender (Sender-Anonymität), den Empfänger (Empfänger-Anonymität) oder lediglich die Beziehung zwischen Sender und Empfänger (Sender-Empfänger-Zuordenbarkeit) geheim zu halten (vgl. [PfHa10]).

Der Fokus dieser Arbeit liegt auf der Analyse des Einflusses von Mehrwegeübertragung auf die Anonymitätseigenschaften der Kommunikationspartner. Hierfür wird exemplarisch ein Protokoll (Branch and Bound-Protokoll [RSWK12]) betrachtet, welches speziell den Schutz des Empfängers zum Ziel hat. Die Angabe des Protokolls erfolgt auf einer konzeptuellen Ebene. Es werden daher keine Paketdefinitionen oder weitere Details besprochen. Zudem werden Eigenschaften des Protokolls (z.B. verwendete Schlüssel), welche für die Analysen nicht relevant sind, nicht oder nur oberflächlich behandelt.

Dieser Artikel ist in fünf weitere Abschnitte unterteilt. In Abschnitt 2 werden grundlegende Begriffe vorgestellt. Abschnitt 3 beschreibt das Crowds-System, auf welchem das Branch and Bound-System (Abschnitt 4) aufbaut. In Abschnitt 5 wird das Branch and Bound-System analysiert und der Einfluss von Mehrwegeübertragung diskutiert. Abschnitt 6 enthält eine Zusammenfassung der Ergebnisse des Artikels und beschreibt weitere Probleme, welche durch das im Rahmen dieser Arbeit analysierte System nicht abgedeckt werden können.

2 Grundlegende Begriffe

Im Rahmen dieser Arbeit sind speziell die Begriffe *Anonymitätsmenge*, *Anoymitätsgrad* und *Gesamtwahrscheinlichkeit* von Bedeutung. Diese werden in diesem Abschnitt besprochen, um das Verständnis für den zentralen Teil der Arbeit zu erleichtern.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 82-92.

Anonymitätsmenge: Nach Pfitzmann und Hansen [PfHa10] besteht die Anonymitätsmenge aus all jenen Subjekten (hier idR. als Netzwerkknoten oder kurz Knoten bezeichnet), welche an einer Aktion beteiligt sein können. Die Anonymitätsmenge hängt somit, abgesehen vom vorhandenen System, auch vom jeweiligen Angreifer und dessen Fähigkeiten ab.

Anonymitätgrad: Der Anonymitätsgrad (Engl. degree of anonymity) gibt an, mit welcher Wahrscheinlichkeit eine Entscheidung (dh. die Identifizierung eines Subjekts) des Angreifers korrekt ist. Reiter und Rubin geben in ihrer Arbeit zudem verschiedene Ausprägungen des Anonymitätsgrades an, welche eine Grobeinteilung von Systemen erlauben [ReRu98]. Sie unterscheiden hierbei zwischen den Stufen *Exposed* (sichere Identifizierung), *Possible Innocence* (keine sichere Identifizierung), *Probable Innocence* (korrekte Identifizierung maximal mit Wahrscheinlichkeit $1/2$) und *Beyond Suspicion* (Identifizierung ist nur durch pures Raten möglich). Zusätzlich wird noch der Begriff *Absolute Privacy* eingeführt. Dieser Anonymitätsgrad wird erreicht, wenn ein Angreifer keine Entscheidung treffen kann. Beispielsweise ist dies der Fall, wenn der Angreifer nicht entscheiden kann, ob überhaupt kommuniziert wurde.

Gesamtwahrscheinlichkeit: Neben dem Anonymitätsgrad ist auch die Gesamtwahrscheinlichkeit für eine korrekte Identifizierung ein wichtiger Begriff. Die Gesamtwahrscheinlichkeit sagt somit aus, mit welcher Wahrscheinlichkeit das gesuchte Subjekt identifiziert wird.

Zudem ist es notwendig, den Angreifer zu definieren, weil andernfalls weder eine Anonymitätsmenge noch ein Anonymitätsgrad, sei es für den Sender sowie den Empfänger, bestimmt werden kann. In dieser Arbeit wird ein interner Angreifer angenommen, welcher k der vorhandenen n Netzwerkknoten unter seiner Kontrolle hat. Der Angreifer kann alle von diesen Knoten verarbeiteten Daten lesen und mit allen kontrollierten Knoten vertraulich kommunizieren. Zudem ist der Angreifer berechenmäßig beschränkt. Diese Anforderung ist notwendig, weil andernfalls jegliche auf asymmetrischer Kryptographie basierende Kommunikation entschlüsselt werden kann.

3 Crowds-Protokoll

Das Crowds-Protokoll wurde von Reiter und Rubin im Jahr 1998 vorgestellt [ReRu98]. Im Gegensatz zu den bis zu diesem Zeitpunkt bekannten Verfahren wie dem Mixnet-System [Chau81], Onion Routing [GoRS96] sowie dem erst später vorgestellten Tor-System [DiMS04], verwenden Reiter und Rubin einen zufälligen Verbindungsaufbau. Kann bei vielen Systemen der Sender die für die Kommunikation benötigten Zwischenknoten selbst aussuchen, ist dies im Crowds-System nicht mehr möglich.

3.1 Verbindungsaufbau

Das Anonymisierungsnetzwerk besteht aus n Knoten, die als Jondos (vom englischen Begriff John Doe) bezeichnet werden. Der Sender ist zudem selbst ein Teil des Anonymisierungsnetzwerks, also ein Jondo. Zusätzlich kommunizieren die Jondos paarweise verschlüsselt, wodurch ein Außenstehender die übermittelten Daten nicht lesen kann. Um eine Verbindung zum Empfänger aufzubauen, werden folgende Schritte durchgeführt:

1. Der Sender wählt einen zufällig ausgewählten Jondo aus, baut zu diesem eine Verbindung

auf und sendet ihm die Identität des Empfängers E. Wählt sich der Sender selbst aus (er ist auch ein Jondo), so baut er keine Verbindung auf und verfährt selbst mit Schritt 2.

2. Der Jondo, zu dem eine Verbindung aufgebaut wurde, entscheidet zufällig, ob er die Nachricht zum Empfänger (Wahrscheinlichkeit $1 - p_f < 0.5$) oder zu einem ebenfalls zufällig ausgewählten Jondo (Wahrscheinlichkeit $p_f > 0.5$) sendet. Die Wahrscheinlichkeit p_f ist global vorgegeben und jedem Jondo bekannt. Alle weiteren Jondos, zu denen eine Verbindung aufgebaut wird, verfahren analog.

Durch diesen Ablauf entsteht ein virtueller Kanal zwischen dem Sender und dem Empfänger. Das Crowds-Protokoll kann somit wie eine Zufallsbewegung (Engl. random walk) durch den zugrunde liegenden vollständigen Kommunikationsgraphen gesehen werden. Durch diesen virtuellen Kanal können die beiden Kommunikationspartner Daten zum jeweils anderen senden, ohne dass der Empfänger den Sender kennt.

3.2 Sicherheitsanalyse

Das Crowds-Protokoll wird gegenüber einem internen Angreifer, der eine Menge an Jondos unter seiner Kontrolle hat, analysiert. Da das Crowds-Protokoll gegenüber einem globalen Angreifer, der alle übermittelten Daten lesen kann, keinen Schutz bietet, wird dieser Angreifer nicht weiter betrachtet.

3.2.1 Empfängeranonymität

Das von Reiter und Rubin vorgestellte Protokoll bietet gegenüber einem internen Angreifer keinen Schutz des Empfängers. Da jeder Jondo den Empfänger kennen muss, um im Bedarfsfall zu diesem eine Verbindung aufbauen zu können (Terminierung des Verbindungsaufbaus), kennt ein Angreifer, der einen Jondo des Kanals kontrolliert, automatisch auch den Empfänger. Die Chance, dass bei n Jondos, k Angreifern und dem Parameter $p_f > 0.5$ zumindest ein Angreifer Teil des virtuellen Kanals ist, liegt bei $\frac{k}{n-p_f(n-k)}$. Diese Wahrscheinlichkeit entspricht somit der Gesamtwahrscheinlichkeit für den Angriff. Die Entscheidungssicherheit ist hierbei jedoch durchwegs 1, weil im Falle einer Festlegung durch den Angreifer dieser in keinem Fall einen Fehler begeht. Somit gilt der Empfänger im Crowds-Protokoll als *Exposed*.

3.2.2 Senderanonymität

Im Gegensatz zum Empfänger ist der Sender durch das Protokoll vor der zweifelsfreien Identifizierung geschützt. Wird zu einem Jondo eine Verbindung aufgebaut, so kann dieser Jondo nicht entscheiden, ob dieser Aufbau durch den Schritt 1 oder den Schritt 2 des Protokolls zustande gekommen ist. Mit anderen Worten kann der Jondo nicht sicher entscheiden, ob sein Vorgänger der Sender ist oder nur ein weiterer Zwischenknoten. Falls ein Angreifer mehrere Jondos eines virtuellen Kanals kontrolliert, wird dem Angreifer die Möglichkeit zugestanden, eindeutig zu entscheiden, welcher der kontrollierten Jondos als erster im Crowds-Kanal vorkommt. Die Wahrscheinlichkeit liegt bei $\frac{n-p_f(n-k-1)}{n}$ (Entscheidungssicherheit), dass zumindest ein Angreifer Teil des Kanals und der Vorgänger des ersten vom Angreifer kontrollierten Jondos der Sender ist. Die Gesamtwahrscheinlichkeit für die korrekte Identifizierung entspricht $\frac{k(n-n\cdot p_f+k\cdot p_f+p_f)}{n^2-p_f\cdot n(n-k)}$. Abhängig vom Parameter p_f kann somit der Anonymitätsgrad *Probable Innocence* erreicht werden.

Gegenüber einem betrügerischen Empfänger entspricht die Entscheidungssicherheit dem Wert

$1/(n-k)$. Dies bedeutet, dass der Empfänger lediglich raten kann, welcher der nicht unter seiner Kontrolle stehenden Knoten der Sender ist. Der Anonymitätsgrad *Beyond Suspicion* ist somit erreicht. Für den Fall, dass jeder mögliche Empfänger ein Angreifer ist, nimmt die Gesamtwahrscheinlichkeit zudem den selben Wert an, weil der Angreifer in jedem Fall eine Entscheidung treffen kann (einer der kontrollierten Empfänger erhält die Nachricht).

4 Branch and Bound-Protokoll

Um die Auswirkung von Mehrwegeübertragung auf die Anonymitätseigenschaften zu untersuchen, wird das Branch and Bound-Protokoll analysiert, welches in diesem Abschnitt in seiner Grundstruktur vorgestellt wird [RSWK12]. Beim Branch and Bound-Protokoll baut der Sender eine virtuelle Verbindung zu einem Empfänger auf, indem er einen in Ebenen unterteilten Kommunikationsgraphen und keinen einzelnen Kommunikationskanal aufbaut. Ziel dieses Protokolls ist es, den Empfänger durch Sackgassen im Kommunikationsgraphen zu schützen. Für dieses Protokoll werden in Abschnitt 5 Analyseergebnisse vorgestellt, welche den Einfluss der Mehrwegeübertragung auf die Anonymität des Senders und des Empfängers zeigen.

4.1 Verbindungsaufbau

Das Netzwerk besteht aus n Knoten. Der Sender und der Empfänger sind Teil davon.

1. Der Sender wählt ganze Zahlen $e > 1$, $b > 1$ (Branch-Wert) und $l > 1$ (Bound-Wert), welche die Struktur des erzeugten Netzwerks beeinflussen.
2. Der Sender baut einen Kommunikationsgraphen auf, der aus $e + 1$ Ebenen besteht. Die Ebene i besteht aus den Knoten der Menge F_i. Zudem besitzt jede Ebene (abgesehen von der Ebene 0) eine Teilmenge an Knoten $B_i \subseteq F_i$ mit $|B_i| = l$. Die Ebene 0 besteht nur aus dem Sender $B_0 = F_0 = \{I\}$. Der Empfänger ist Teil der letzten Ebene ($E \in B_e$). Die Knoten aus den Mengen $F_i \setminus B_i$ werden als Sackgassen-Knoten bezeichnet. Zudem gilt $B_1 = F_1$ damit der Sender weniger Crowds-Verbindungen aufbauen muss (vgl. Abschnitt 5.3).
3. Der Sender baut zu jedem Knoten aus der Menge B_1 zwei eigenständige Crowds-Verbindungen auf und teilt den Knoten der Menge B_1 die Identitäten ihrer b Nachfolgeknoten in der Ebene 2 mit. Die Knoten der Menge B_2 sind jeweils Endpunkt zweier Verbindungen, besitzen somit je zwei Vorgänger in der Ebene 1.
4. Der Sender sendet durch den bisher aufgebauten Kommunikationsgraphen den Knoten der Ebene i (verschlüsselte) Daten, die sie dazu veranlassen Verbindungen zu b Knoten der Ebene $i + 1$ aufzubauen (siehe Abschnitt 4.2).

Durch diesen Aufbau entsteht ein Kommunikationsgraph wie in Abbildung 1 dargestellt.

4.2 Übertragung von Daten

Um Daten durch den Kommunikationsgraphen zu transportieren (z.B. zum Aufbau des Graphen) verfolgt das Branch and Bound-System folgenden Ablauf. Der Sender verschlüsselt die Daten mit dem öffentlichen Schlüssel des Empfängers und leitet diese Daten an alle seine Nachfolger weiter. Erhält ein Knoten ein Datenpaket, so entschlüsselt er dieses und überprüft ob das Resultat dem erwarteten Redundanzschema (z.B. Verwendung eines geeigneten kryptographischen Hashwertes) entspricht. Ist dies der Fall, so ist der jeweilige Knoten der Empfänger dieser Daten. In jedem Fall leitet er das Paket zu all seinen Nachfolgern weiter (falls vorhanden).

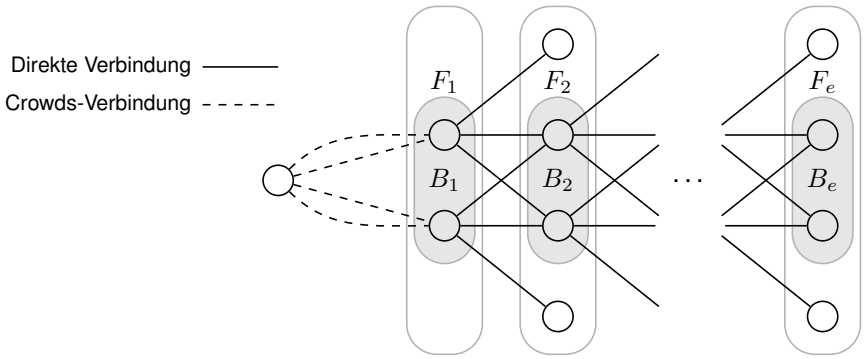


Abb. 1: Aufbau des Kommunikationsgraphen ($b = 3, l = 2$)

Mehrfach erhaltene Pakete werden von den Knoten nicht weitergeleitet, weil andernfalls die Menge an Paketen von Ebene zu Ebene verdoppelt wird (jeder Knoten hat zwei Vorgänger in der Vorgängerebene), was ein exponentielles Wachstum der Nachrichten zur Folge hätte.

Um Antwortdaten zu senden, werden diese mit einem vom Sender beim Aufbau des Kommunikationsgraphen übermittelten öffentlichen Schlüssel verschlüsselt und an alle Vorgänger der Vorgängerebene gesendet. Die Knoten, die Antwortdaten erhalten, leiten diese ebenfalls an ihre Vorgänger weiter, wobei Duplikate gelöscht werden. Das Löschen von Duplikaten hat auch hier den Grund, dass es zu keinem exponentiellen Wachstum der Nachrichten kommt.

4.3 Kommunikationsaufwand

Mit dem Aufbau eines Kommunikationsgraphen ist naturgemäß ein hoher Kommunikationsaufwand verbunden. Ein Datentransfer zu einem Knoten durch einen Kommunikationsgraphen mit $r + 1$ Ebenen, ergibt einen Aufwand von ungefähr $r \cdot b \cdot l$ Nachrichtenübertragungen. Im Vergleich zu einem System, welches nur einen Kanal aufbaut (kurz: 1-Kanal-System) ist der Aufwand nennenswert höher. Bei einem 1-Kanal-System mit $r+1$ beteiligten Knoten werden r Übertragungen benötigt, womit abhängig von den Parametern b und l ein nennenswerter Mehraufwand betrieben werden muss. Weniger stark wird durch diesen Aufbau die Latenz bei der Übertragung beeinflusst. Für die Latenz ist nur der schnellste Weg vom Sender durch die Ebenen zum Empfänger relevant. Dieser besteht ebenfalls aus r Verbindungen (eine davon ist eine Crowds-Verbindung).

5 Analyse

In diesem Abschnitt wird das Branch and Bound-Protokoll anhand von Simulationen analysiert. Die Simulationsmethode wird in Abschnitt 5.1 vorgestellt. Wichtige Analyseergebnisse werden in Teilabschnitt 5.2 sowie Anpassungen zur Verbesserung der Anonymitätseigenschaften in Teilabschnitt 5.3 diskutiert. Abschließend wird das Branch and Bound-Protokoll mit einem idealisierten 1-Kanal-System verglichen um den Einfluss von Mehrwegeübertragung bewerten zu können.

5.1 Methode

Das Branch and Bound-Protokoll wird mittels Simulationen analysiert. Hierfür wird anhand der Protokolldefinition der Aufbau des Kommunikationsgraphen nachgestellt. Daraufhin werden zwei Angreifer (jeweils interne Angreifer, welche k der n Knoten unter ihrer Kontrolle ha-

ben) simuliert. Ein Angreifer versucht die Identität des Senders, der andere die des Empfängers offenzulegen.

Zur Identifizierung des Senders wird der Predecessor-Angriff (vgl. [WALS04, WALS02]) verwendet. Der Angriff läuft folgend ab:

1. Der Angreifer identifiziert alle Vorgänger der von ihm kontrollierten Knoten, welche Teil der vom Sender aufgebauten Crowds-Verbindungen sind. Die Knoten der Menge $F_i, i = 1, \ldots, e$ werden ignoriert, weil diese nichts zu dem Angriff beitragen können. Knoten der Mengen $F_i, i > 1$ können den Sender nicht identifizieren. Knoten der Menge F_1 haben einen zufällig ausgewählten Jondo als Vorgänger (dies kann auch der Sender sein). Da der letzte Jondo des Kanals jedoch zufällig ausgewählt wurde, hat ein Angreifer hiermit keine bessere Chance als er es durch pures Raten hätte.
2. Der Angreifer identifiziert die Vorgänger der im Punkt 1 ausgewählten Knoten und bestimmt die Häufigkeit des Auftretens der identifizierten Vorgänger.
3. Der Angreifer wählt den Knoten mit der maximalen Häufigkeit als Sender aus. Wurden mehrere Knoten maximal oft (dh. gleich oft) identifiziert, so wählt der Angreifer einen dieser Knoten per Zufall aus.

Dieses Prozedere wird daraufhin wiederholt und es wird gezählt wie oft

- der Angreifer überhaupt eine Entscheidung getroffen hat (dh. ein Angreifer Teil einer Crowds-Verbindung war). Dieser Wert wird als n_p bezeichnet. Das Subskript p steht hier für den Begriff *potentiell*.
- der Angreifer den Sender korrekt bestimmt hat. Dies wird als n_k bezeichnet.

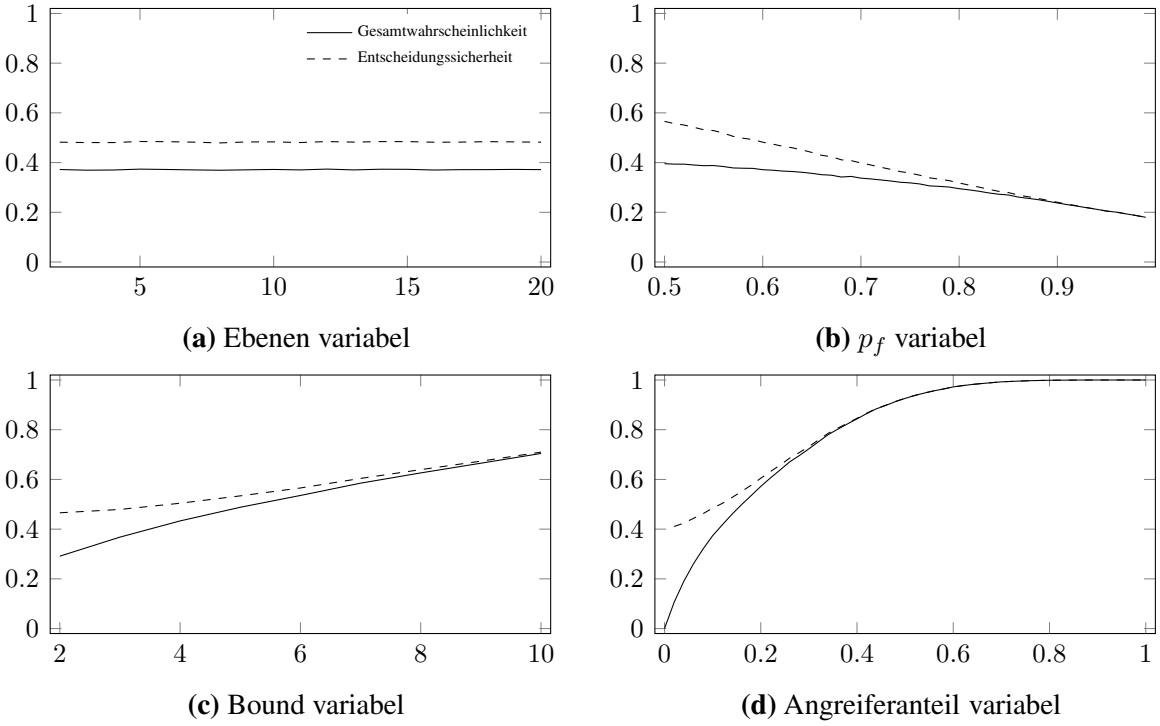
Schließlich werden die Werte $p_G = n_k/N$ und $p_E = n_k/n_p$ bestimmt. Der Wert p_G gibt die geschätzte Gesamtwahrscheinlichkeit für einen erfolgreichen Angriff an (dh. der relative Anteil der korrekten Entscheidungen). Der Wert p_E entspricht der geschätzten Entscheidungssicherheit (dh. der Wahrscheinlichkeit, dass eine getroffene Entscheidung korrekt ist). In $N - n_p$ Fällen entscheidet der Angreifer nicht, was beispielsweise dann der Fall ist, wenn er von der Kommunikation nichts erfährt (z.B. erhält der Angreifer keine weiterzuleitenden Nachrichten).

Die Identifizierung des Empfängers geschieht sehr ähnlich. Die Simulation unterscheidet sich lediglich darin, wie der Angreifer den Empfänger versucht zu identifizieren. In diesem Anwendungsfall erhält der Angreifer zudem die Möglichkeit die Reihenfolge der beobachteten Ebenen zu bestimmen. Dies bedeutet, dass der Angreifer entscheiden kann, welche Knoten zu der aus seiner Sicht letzten Ebene gehören (dies sind somit Nachfolger von kontrollierten Knoten der vorletzten bekannten Ebene). Der Angreifer wählt nun einen derjenigen Knoten der letzten identifizierten Ebene als Empfänger aus, zu dem die meisten Verbindungen aufgebaut wurden. Die Wahrscheinlichkeiten p_G und p_E werden analog bestimmt.

5.2 Ergebnisse

Für die Analysen wurden jeweils $N = 10^6$ Durchläufe getätigt. Die Größe des Netzwerkes wurde mit $n = 1000$ festgelegt. Zudem wurden die Standardparameter $p_f = 0.6$, $e = b = l = 5$ sowie 10% Angreiferanteil (entspricht $k = 100$ Angreifern) gewählt. In den Auswertungen ist jeweils die Gesamtwahrscheinlichkeit sowie die Entscheidungssicherheit angegeben (y-Achse). Für die Analysen wurde jeweils ein Parameter variabel gehalten. Die restlichen Parameter wurden mit den Standardwerten belegt. Somit zeigen die Auswertungen lediglich den Einfluss bei

Veränderung exakt eines Parameters.



(a) Ebenen variabel

(b) p_f variabel

(c) Bound variabel

(d) Angreiferanteil variabel

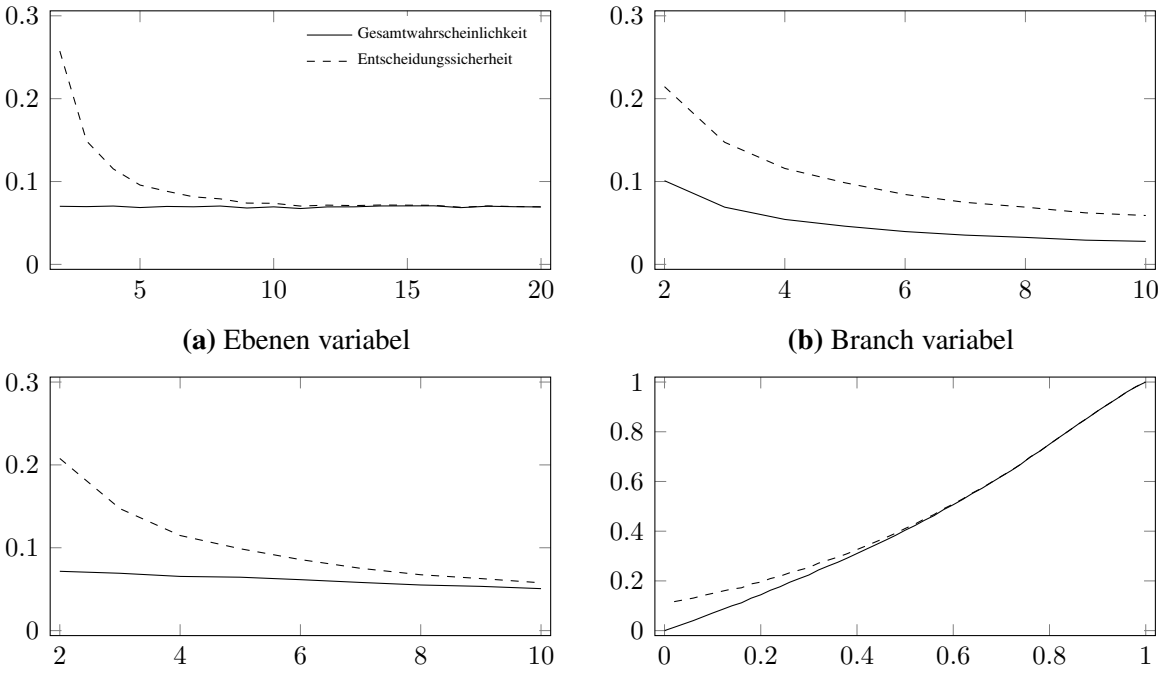
Abb. 2: Senderanonymität

Die Analysen ergaben, dass der Sender durch dieses System schlecht geschützt ist (siehe Abbildung 2). Durch die Anwendung des Predecessor-Angriffs und der mehrmaligen Verwendung von Crowds-Verbindungen ergibt sich eine hohe Chance für den Angreifer den Sender zu identifizieren. Speziell eine Erhöhung des Parameters l (Größe der Menge B_i) impliziert eine Verschlechterung für den Sender, weil dieser in diesem Fall mehr Crowds-Verbindungen aufbauen muss (zu jedem Knoten der Menge B_1 zwei Verbindungen).

Anhand der Analysen in Abbildung 3 ist erkennbar, dass auch der Empfänger durch diesen Aufbau des Systems abhängig vom Angreiferanteil k/n schlecht geschützt ist. Dadurch, dass der Empfänger immer Teil der letzten Ebene ist und der Angreifer einen Knoten aus der aus seiner Sicht letzten Ebene identifiziert, hat er eine gute Chance den Empfänger zu bestimmen. Eine Erhöhung der Ebenenanzahl bringt hier keine Verbesserung. Der Grund ist, dass die Chance, die letzte Ebene zu identifizieren, unabhängig von der Anzahl der Ebenen ist.

5.3 Anpassungen

Wie die Analysen gezeigt haben, ist der Empfänger durch seine Positionierung in der letzten Ebene vergleichsweise leicht zu identifizieren, auch wenn das Netzwerk aus vielen Ebenen besteht. Um den Empfänger somit besser zu schützen, ist diese Eigenschaft aufzugeben und der Empfänger in einer zufällig ausgewählten Ebene (Ebene 2 bis r) unterzubringen. Durch diese Anpassung verbessert sich der Schutz des Empfängers merkbar. Es ist zu beachten, dass die Ebene 1 ausgelassen werden muss, weil im Falle einer Positionierung in dieser Ebene die Anonymitätseigenschaften des Empfängers verschlechtert werden, auch wenn es mehr potentielle Ebenen gibt, in denen sich der Empfänger befinden kann. Dies wird dadurch erklärt, dass



(a) Ebenen variabel

(b) Branch variabel

(c) Bound variabel

(d) Angreiferanteil variabel

Abb. 3: Empfängeranonymität

die Knoten der Ebene 1 (und somit auch der Empfänger) in diesem Fall Ziel zweier Crowds-Verbindungen sind. Da die Crowds-Verbindungen aus mehreren Jondos bestehen, die alle den Endpunkt kennen, steigt die Chance, dass der Empfänger, sollte er in der Ebene 1 sein, identifiziert werden kann. Eine weitere Verbesserung der Anonymitätseigenschaften des Empfängers entsteht dann, wenn jeder Knoten nur einen Vorgänger in der Vorgängerebene besitzt (gilt auch für die aufgebauten Crowds-Verbindungen). Durch die geringere Anzahl an Kommunikationskanälen sinkt die Chance, dass der Angreifer den Empfänger identifizieren kann. Durch dieses Vorgehen besteht jedoch das Problem, dass beim Ausfall einzelner wichtiger Knoten, die Daten nicht mehr zum Empfänger übermittelt werden können. Im Originalsystem stellte dies durch die stärkere Verknüpfung der Ebenen ein geringeres Problem dar. Der resultierende Kommunikationsgraph ist in Abbildung 4 dargestellt.

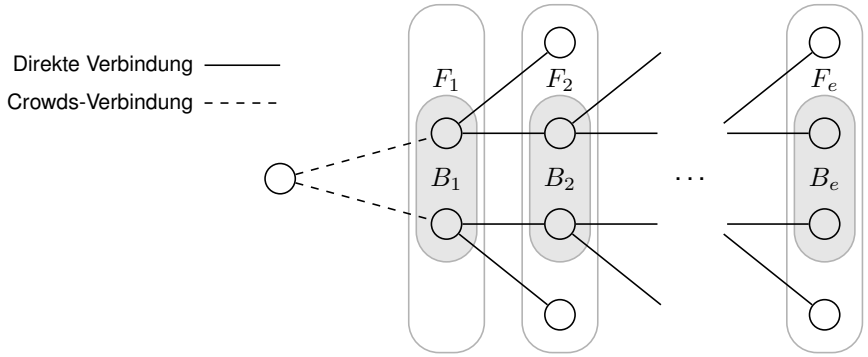


Abb. 4: Aufbau des Kommunikationsgraphen (einfache Verbindungen)

Der Schutz des Senders kann zudem auch verbessert werden, indem der Aufbau des Netzwerkes geändert wird (Reduktion der vom Sender aufgebauten Crowds-Verbindungen). Durch die Verwendung von eigens ausgewählten Eingangsknoten kann der Schutz des Senders erhöht werden. Speziell sinkt in diesem System die Gesamtwahrscheinlichkeit für einen erfolgreichen Angriff. Eingangsknoten sind Knoten, zu denen der Sender eine Verbindung aufbaut und welche den Verbindungsaufbau im Namen des Senders tätigen und somit wie Stellvertreter fungieren (siehe Abbildung 5). Vergleichbar ist dies mit dem Tor sowie Onion Routing-System, bei denen der Client eine einzelne Verbindung zu einem Onion Router aufbaut, welcher daraufhin den weiteren Kanalaufbau selbstständig erledigt. In diesem Modell können die Analysen aus dem Crowds-System herangezogen werden, weil nur eine Crowds-Verbindung verwendet wird.

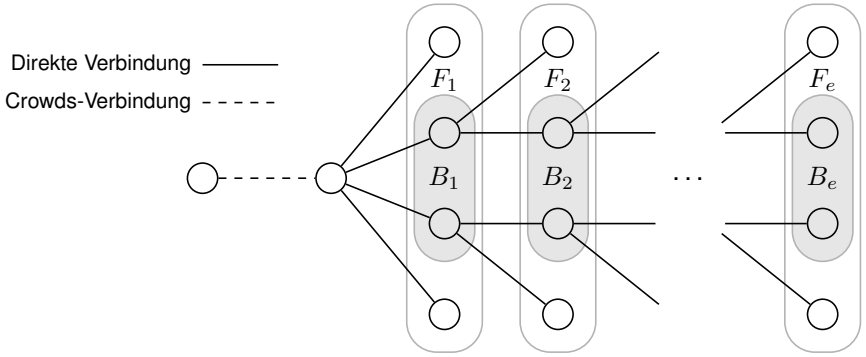


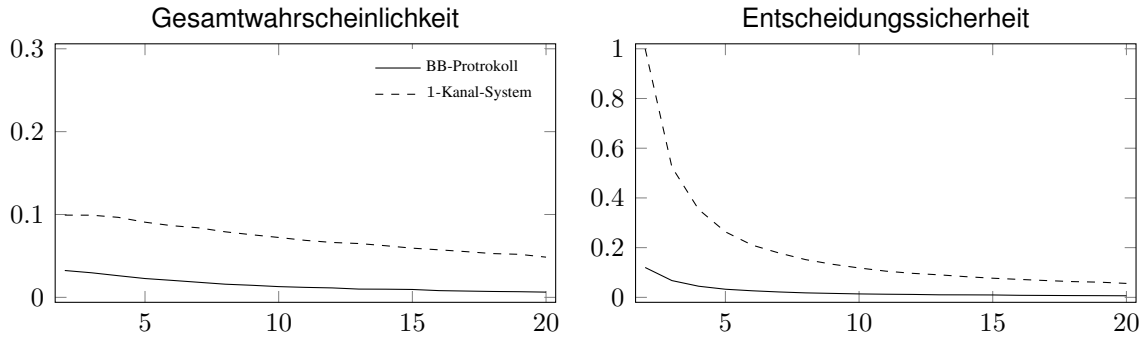
Abb. 5: Aufbau des Kommunikationsgraphen (Eingangsknoten, einfache Verbindungen)

5.4 Vergleich mit 1-Kanal-Systemen

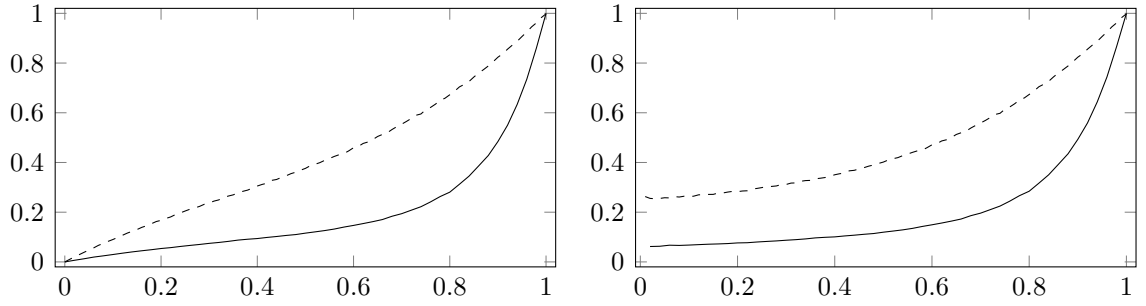
Um den Einfluss von Mehrwegeübertragung bewerten zu können, wird das Branch and Bound-Systeme mit einem idealisierten 1-Kanal-System vergleichen. Zum Vergleich wird das 1-Kanal-System mit dem angepassten Branch and Bound-System (einfache Verbindungen, Empfänger in einer zufällig ausgewählten Ebenen, vgl. Abschnitt 5.3) gegenübergestellt. Das 1-Kanal-System besteht aus so vielen Zwischenknoten wie das Branch and Bound-Systeme Ebenen hat. Durch diese Festlegung besitzen beide Systeme somit eine ähnliche Länge (Anzahl Verbindungen auf dem Weg vom Sender zum Empfänger), womit die Latenz vergleichbar ist. Die gleiche Länge kann nicht erreicht werden, weil durch die Verwendung der Crowds-Verbindungen zwischen Sender und Ebene 1 die effektive Länge des Kanals nicht vom Sender exakt festlegbar ist. Zudem kann im 1-Kanal-System der Empfänger ein beliebiger Knoten des aufgebauten Kanals sein (vgl. angepasstes Branch and Bound-System). In Abbildung 6 sind die Auswertungen bezüglich des Empfängers angegeben. Speziell ist der Vorteil des Branch and Bound-Protokolls zu erwähnen, wenn der Angreiferanteil hoch ist.

6 Fazit

Die Ergebnisse zeigen anhand des Branch and Bound-Protokolls, dass der Schutz der Identität des Empfängers durchaus durch Verwendung von Mehrwegeübertragung gestärkt werden kann (vgl. Abbildung 6). Dieser erhöhte Schutz schlägt sich jedoch negativ auf den Kommunikationsaufwand nieder. Die Analysen haben zudem auch wichtige Hinweise ergeben, welche Topologien potentielle Gefahren für Sender und Empfänger darstellen. Hier ist beispielsweise das Ergebnis zu erwähnen, dass durch eine Reduktion der Anzahl der Verbindungen zwischen den einzelnen Ebenen ein besserer Schutz des Empfängers erreicht werden kann.



(a) Ebenenanzahl variabel



(b) Angreiferanteil variabel

Abb. 6: Empfängeranonymität (Vergleich mit 1-Kanal-Systemen)

Im Gegensatz zum Empfänger ist es jedoch ungleich schwerer, den Sender zu schützen, weil dieser durch seine exponierte Lage im Kommunikationsgraph besonders leicht identifiziert werden kann. Hierbei ist grundsätzlich nach der Devise „Weniger ist mehr“ zu verfahren. Je mehr Verbindungen vom Sender aufgebaut werden, desto leichter ist der Predecessor-Angriff anzuwenden [DaKä13, WALS04, WALS02]. Somit bringt die Mehrwegeübertragung für den Schutz des Senders keine Verbesserungen.

Zudem bietet die Mehrwegeübertragung keinen Schutz vor Angreifern, die langfristige Analysen anstellen können. Diese Angreifer können den Verbindungsaufbau (z.B. Aufbau des Kommunikationsgraphen) eines Senders viele Male beobachten und somit die potentiellen Empfänger (Empfänger-Anonymitätsmenge) einschränken. Diese langfristigen Angriffe stellen jedoch viele Anonymisierungsprotokolle vor Probleme [AgKe03, DaSe04, KeAP03, JWJS+13]. Als Gegenmaßnahmen werden oft künstlich Daten (Dummy-Traffic) versendet bzw. Verbindungen aufgebaut (jeweils zu zufällig ausgewählten Empfängern) um den Angreifer zu verwirren. Dieses Vorgehen stößt jedoch auch an seine Grenzen [BeLa03, DaTr13, AgKe03]. Lediglich Verfahren, welche die Zuordnung zwischen Nachrichten bzw. zwischen Nachrichten und dem Sender bzw. Empfänger verhindern, bieten gegen diese Angriffe einen Schutz, sind jedoch häufig praktisch nicht einsetzbar [BeDo03].

Literatur

[AgKe03] D. Agrawal, D. Kesdogan: Measuring Anonymity: The Disclosure Attack. In: *IEEE security & privacy*, 1, 6 (2003), 27–34, .

[BeDo03] A. Beimel, S. Dolev: Buses for Anonymous Message Delivery. In: *J. Cryptology*, 16, 1 (2003), 25–39.

[BeLa03] O. Berthold, H. Langos: Dummy Traffic Against Long Term Intersection Attacks. *In: R. Dingledine, P. Syverson (Hrsg.), Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, Springer-Verlag, Berlin, Heidelberg (2003), 110–128.

[Chau81] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: *Communications of the ACM*, 24, 2 (1981), 84–90.

[DaKä13] G. Danezis, E. Käsper: The Dangers of Composing Anonymous Channels. *In: M. Kirchner, D. Ghosal (Hrsg.), Information Hiding*, Springer-Verlag (2013), *Lecture Notes in Computer Science*, Bd. 7692, 191–206.

[DaSe04] G. Danezis, A. Serjantov: Statistical disclosure or intersection attacks on anonymity systems. *In: Proceedings of the 6th international conference on Information Hiding*, IH'04, Springer-Verlag, Berlin, Heidelberg (2004), 293–308.

[DaTr13] G. Danezis, C. Troncoso: You Cannot Hide for Long: De-Anonymization of Real-World Dynamic Behaviour. *In: Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2013)*, ACM (2013).

[DiMS04] R. Dingledine, N. Mathewson, P. Syverson: Tor: The Second-Generation Onion Router. *In: Proceedings of the 13th USENIX Security Symposium* (2004), 303–320.

[GoRS96] D. Goldschlag, M. Reed, P. Syverson: Hiding Routing Information. *In: Information Hiding*, Springer-Verlag (1996), 137–150.

[JWJS+13] A. Johnson, C. Wacek, R. Jansen, M. Sherr, P. Syverson: Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. *In: 20th ACM conference on Computer and Communications Security (CCS 2013)* (2013).

[KeAP03] D. Kesdogan, D. Agrawal, S. Penz: Limits of Anonymity in Open Environments. *In: Revised Papers from the 5th International Workshop on Information Hiding*, IH '02, Springer-Verlag, London (2003), 53–69.

[PfHa10] A. Pfitzmann, M. Hansen: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (2010), v0.34.

[ReRu98] M. Reiter, A. Rubin: Crowds: Anonymity for Web Transactions. In: *ACM Transactions on Information and System Security*, 1 (1998), 66–92.

[RSWK12] S. Rass, P. Schartner, R. Wigoutschnigg, C. Kollmitzer: Anonymous Communication by Branch-and-Bound. *In: Proceedings of the 7th International Conference on Availability, Reliability and Security (AReS 2012)*, IEEE, IEEE Computer Society: Conference Publishing Services, Prague, Czech Republic (2012).

[WALS02] M. Wright, M. Adler, B. N. Levine, C. Shields: An Analysis of the Degradation of Anonymous Protocols. *In: Proceedings of the Network and Distributed Security Symposium – NDSS '02*, IEEE (2002).

[WALS04] M. Wright, M. Adler, B. N. Levine, C. Shields: The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems. In: *ACM Transactions on Information and System Security*, 4, 7 (2004), 489–522.