Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

SS 2009

Seminararbeit

Internet Mapping: from Art to Sience

Peer-to-Peer Seminar Ausarbeitung

Patrick Hornecker

24. Juli 2009

Betreut durch Prof. Dr. Schindelhauer

Inhaltsverzeichnis

1 Einleitung **2**

2 Archipelago **3**

3 Die Messungen **4**
3.1 IP Topologie 4
3.2 DNS 4
3.3 Router-Level Karten 5
3.4 Karten der Autonomen Systeme Struktur 5
3.5 Autonome System Router Karten 6

4 Ausblick **6**

1 Einleitung

Im heutigen privaten, sowie im Geschäftsleben spielt das Internet immer mehr eine tragende Rolle und es kann nur noch in wenigen Bereichen darauf verzichtet werden. Da das Internet allerdings eine dynamische Struktur ist, kennt niemand die genauen Strukturen, die diesem globalen Netzwerk zugrunde liegen. Diese Strukturen sind aber von Interesse, wenn es darum geht die vorhandenen Schwachstellen, Flaschenhälse oder mögliche Angriffspunkte in diesem System zu finden.
Die *Cooperative Association for Internet Data Analysis* (CAIDA) setzt genau an diesem Punkt an und versucht, mit einer selbst entwickelten Software, den Aufbau des Systems zu ermitteln und zu verstehen um daraus intuitiv zu lesende Karten des Netzwerkes zu erstellen. Eben dieses Vorhaben wird in dem Paper „Internet Mapping: from Art to Sience“[1] von Kimberley Claffy, Young Hyun, Ken Keys, Marina Fomenkov und Dimitri Krioukov erläutert. Die darin beschriebene Software nennt sich *Archipelago* und bietet verschiedene Möglichkeiten der Messung an. Im ersten Teil wird vor allem diese Software und deren Komponenten besprochen. Im folgenden Abschnitt werden die verschiedenen Messverfahren für die verschiedenen Karten erläutert. Im letzten Teil des Papers wird noch ein kleiner Ausblick auf zukünftige Entwicklungen im Bereich von CAIDA gegeben.

2 Archipelago

Wie bereits in der Einleitung erwähnt ist *Archipelago* (Ark) die neueste Software, die von CAIDA entwickelt wurde. Das Programm ist deren neueste Version einer aktiven Vermessungs-Struktur. Der große Vorteil von Ark liegt im Bereich des schnellen und einfachen Entwickelns neuer Module und Prototypen. Um dies zu ermöglichen werden dynamische Skriptsprachen, wie zum Beispiel *Ruby* genutzt und vorgefertigte APIs und Dienste angeboten.
Herz und Motor von Ark ist eine Software, welche auf den Namen *scamper* hört. *Scamper* kümmert sich um das effiziente Ausführen von parallelisiertem *traceroute* und Ping-Messungen, sowie um andere Arten von Messungen wie *alias resolution*. Das Tool unterstützt sowohl IPv4, sowie IPv6 *traceroute* und Ping-Messungen. In *scamper* ist *traceroute* auf Basis von TCP, UDP und ICMP implementiert.
Ark bietet die Möglichkeit dynamische Messungen durchzuführen. Das heißt, dass die Messungen nicht nur bei einer von vornherein bekannten Menge an Zielen stattfindet, sondern dass während der Messungen herausgefunden wird, welche Ziele zu messen sind. Des Weiteren legt Ark sehr viel Wert auf koordinierte Messungen. Um diesen Punkt zu garantieren, nutzt Ark das *tupel-space* Model. *Tupel-space* ist ein verteilter Speicher auf den jeder zugreifen und in den jeder schreiben kann. Diese Eigenschaften werden mit der Tatsache kombiniert, dass die Operationen die ausgeführt werden können sehr einfach anzuwenden sind. Wenn Daten im *tupel-space* gespeichert wI couldn't open file name 'lit.aux' erden, werden diese als Arrays bestehend aus Strings und Integern gespeichert. Um ein Tupel zu erhalten muss der Client diesen nur per Pattern Matching abfragen. Durch diese Eigenschaften von *tupel-space* ist es Ark möglich, dynamische Tests durchzuführen und auch komplexe Messungen in einzelne Teilmessungen aufzuteilen und Zwischenergebnisse im *tupel-space* abzuspeichern. Auch die Erweiterbarkeit von Ark ist durch dieses Model gegeben, da der Nutzer, welcher einen neuen Dienst implementieren will, einfach nur einen Dienst zur Messung entwickeln und die Ergebnisse als Tupel zurück geben muss.
Da Ark ein System ist, das auf verteilte Messungen setzt, sind momentan mehrere Monitore weltweilt aktiv. Nach dem Stand vom Dezember 2008 gibt es insgesamt 31 Monitore, wovon 12 in Nordamerika, zwei in Süd-Afrika, neun in Europa, einer in Afrika, fünf in Asien und zwei in Australien stehen. Sechs der 31 Monitore sind momentan fähig neben den normalen IPv4 auch IPv6 Messungen durchzuführen. Auch die Zahl der IPv6-Monitore soll in der Zukunft steigen. Es sollen in der nahen Zukunft noch weitere Monitore aufgestellt werden, um die Messungen zu verbessern. Erwähnenswert ist, dass die Monitore momentan alle in akademischen Institutionen stehen. Allerdings werden

die Internet Service Provider immer mehr zu interessanten Partnern, welche das Wissen, das aus den Messungen gewonnen wird, auch für sich nutzen könnnen.

3 Die Messungen

Im folgenden Abschnitt werden die verschiedenen Messungen selbst besprochen und es wird jeweils erklärt, wie diese durchgeführt werden und wie die visuellen Darstellungen der einzelnen Messergebnisse zu Stande kommen. Im behandelten Paper werden insgesamt fünf verschiedene Arten von Darstellungen beschrieben. Diese sind eine grobe Darstellung der IP Topologie, eine Karte der momentanen DNS Infrastruktur, eine Karte die nur Router darstellt, eine Darstellung auf dem Level der Autonomen Systeme, sowie eine Karte die die Darstellung der Router und der Autonomen Systeme kombiniert.

3.1 IP Topologie

Bei dieser Art der zu erstellenden Karte werden Messungen zu dynamisch generierten Listen von IP-Adressen in routbaren /24 Netzwerken durchgeführt. Um dieses Vorhaben möglichst effizient zu bewältigen, werden die Ark-Monitore, welche die Messungen ausführen, in verschiedene Teams eingeteilt und die dynamischen Messungen unter den Teammitgliedern verteilt. Durch diese Aufgabenverteilung ist es möglich *traceroute*-Messungen in allen routbaren /24 Netzwerken, in relativ kurzer Zeit durchzuführen. Das heißt, dass ein Team von 13 Monitoren für 7.4 Millionen /24 Netz circa 2 Tage benötigt. Zum Zeitpunkt des Verfassens des Papers waren drei Monitor-Teams aktiv, welche zufällig Ziele innerhalb der /24 Netze gemessen haben. Durch das zufällige Messen von Zielen innerhalb der Netze wird zum einen der auftretende Datenverkehr verteilt und zum anderen werden eher Lücken in den Messungen verhindert, wenn zum Beispiel ein bestimmtes Subnetz nicht erreichbar ist. Das Ergebnis dieser Messungen ist für Forscher frei zugänglich und dient als Grundlage für andere Messungen.

3.2 DNS

Mit den aus dem vorhergehenden Absatz erhaltenen Daten werden DNS-lookups durchgeführt. Durch dieses Vorgehen können wiederrum neue Daten gewonnen werden. Zum einen eine Abbildung von IP auf Hostname und zum anderen Informationen über den Datenverkehr, der bei diesen Lookups generiert wird. Mit dem ersten Datensatz der Hostnamen können Informationen die in den Routernamen gespeichert sind, wie geographische

Lage, Link Kapazitäten, Router Typ oder Netzwerknamen gewonnen werden. Durch den zweiten Datensatz ist es möglich, Informationen bezüglich der DNS-Strukturen zu erhalten. So kann man zum Beispiel herausfinden, wie es mit der Unterstützung von IPv6 seitens der DNS-Server aussieht. Durch die große Anzahl der gemessenen IP-Adressen ist es somit möglich, viele Informationen über diese wichtige Schicht des Internets zu gewinnen.

3.3 Router-Level Karten

Auch hier werden die Daten genutzt, welche mit dem *traceroute*-Verfahren gewonnen wurden. Um aus diesen einzelnen IP-Adressen eine Karte zu erstellen, müssen diese einem Router zugeordnet werden. Dieses Verfahren wird *alias-resolution* genannt. CAIDA arbeitet in diesem Gebiet hauptsächlich mit zwei Methoden: zum einen das selbst entwickelte *iffinder* Tool, zum anderen den *Analytical and Probebased Alias Resolver*.
Iffinder sendet UDP-Testpakete an alle oder eine Teilmenge der IP-Adressen und kann aus den Daten im Header der Antwortpakete schliessen zu welchem Router die Adresse zugehörig ist.
ARPA hingegen überprüft die Struktur einer Menge von IP-Adressen aus den *traceroute*-Daten. Hierbei werden die IP-Adressen einfach mit normalen Schemas von Adressverteilungen verglichen. CAIDA hat das vorhandene ARPA Tool noch erweitert und verbessert, sowie weitere Heuristiken hinzugefügt und nennt seine Fassung *karpa*.
Um nun eine Karte der verschiedenen Router-Level zu erstellen, sind mehrere Durchläufe der beiden Tools mit den vorhandenen Daten notwendig. Nach diesen Durchläufen werden die benötigten Informationen erhalten, um eben diese Karten zu erstellen. So können nun IPv4-Adressen identifiziert werden, welche zum selben Router gehören. Mit Hilfe dieser Informationen kann nun eine Karte erstellt werden, welche die verschiedenen Router und Links visualisiert und somit die vorhandenen IPv4 Daten wesentlich besser darstellen.

3.4 Karten der Autonomen Systeme Struktur

Um eine Karte zu erstellen, auf welcher die verschiedenen vorhandenen Autonomen Systeme im Internet dargestellt werden, werden wieder die Daten der *traceroute*-Messungen verwendet. Diese werden mit Routing Tabellen des *Border Gateway Protocols* verglichen. Diese Routing Tabellen wurden von einer Software namens *Route View* ermittelt. Beim vergleichen der zwei Datensätze werden die IP-Adressen mit den Einträgen in der Routing Tabelle abgeglichen. Die IP-Adresse wird dann dem Autonomen System zugeordnet,

welches den längsten passenden Präfix besitzt. Sollten zwei IP-Adressen, die nur ein Hop auseinander liegen, in zwei verschiedenen Autonome Systeme abgebildet werden, so wird dies als Link zwischen diesen beiden Systemen interpretiert. Durch diese Links kann ein Graph erstellt werden, welcher eben die Verbindungen der einzelnen Autonomen Systeme repräsentiert und somit eine Darstellung der Struktur der Autonomen Systeme ist.
Allerdings ist der Graph in diesem Zustand noch ungewichtet und somit wenig aussagekräftig. Um ihn intuitiv lesbarer zu machen, werden die Kanten und Knoten des Graphs noch mit Annotationen versehen. Die Kanten-Annotationen beschreiben die Beziehung zwischen den Autonomen Systemen (zum Beispiel Peer-to-Peer, Anbieter und Kunde). Die Informationen an den Knoten beschreiben wiederrum den Typ des jeweiligen Systems.

3.5 Autonome System Router Karten

Bei dieser Art der Darstellung werden bereits genannte Karten der Router und die der Autonomen Systeme kombiniert. Die Schwierigkeit bei dieser Art von Karte besteht darin, dass die *traceroute*-Daten keinerlei Informationen darüber enthalten, welcher Router physikalisch zu welchen Autonomen System zuzuordnen ist. Diese Zuordnung ist keine einfach zu erledigende Aufgabe.
Es besteht die Möglichkeit die Router-ID den IP's der Autonomen Systeme zuzuordnen. Allerdings ist eine solche Zuweisung nicht unbedingt eindeutig. Zum Zeitpunkt der Veröffentlichung des Papers wurde zum erstellen dieser Karte eine Heuristik genutzt, welche zum einen die Daten der Ark-Monitore und zum anderen die Methodik nutzt, welche schon eingesetzt wurde um einzelne IP's den Autonomen Systemen zuzuweisen. In diesem Fall werden einfach zwei IP-Adressen, die miteinander verbunden sind, überprüft und somit eine Zuteilung vorgenommen. Auch bei dieser Art der Darstellung werden die Kanten und Knoten wieder mit relevanten Meta-Daten versehen.

4 Ausblick

Für die Zukunft ist, wie schon erwähnt, geplant weitere IPv6 Ark-Monitore zu installieren. Des Weiteren will man die Daten, die durch die Messungen gewonnen wurden, weiterhin der Forschergemeinschaft zur Verfügung stellen und die Auswahl an Analysetools erweitern. Es sollen auch neue Tools zur Visualisierung der Ergebnisse entwickelt und eine neue Ad-hoc Messanlage für IPv4 Messungen in Betrieb genommen werden.

Literatur

[1] Ken Keys Marina Fomenkov Dimitri Krioukov Kimberly Claffy, Young Hyun. Internet mapping: From art to sience, 2008.