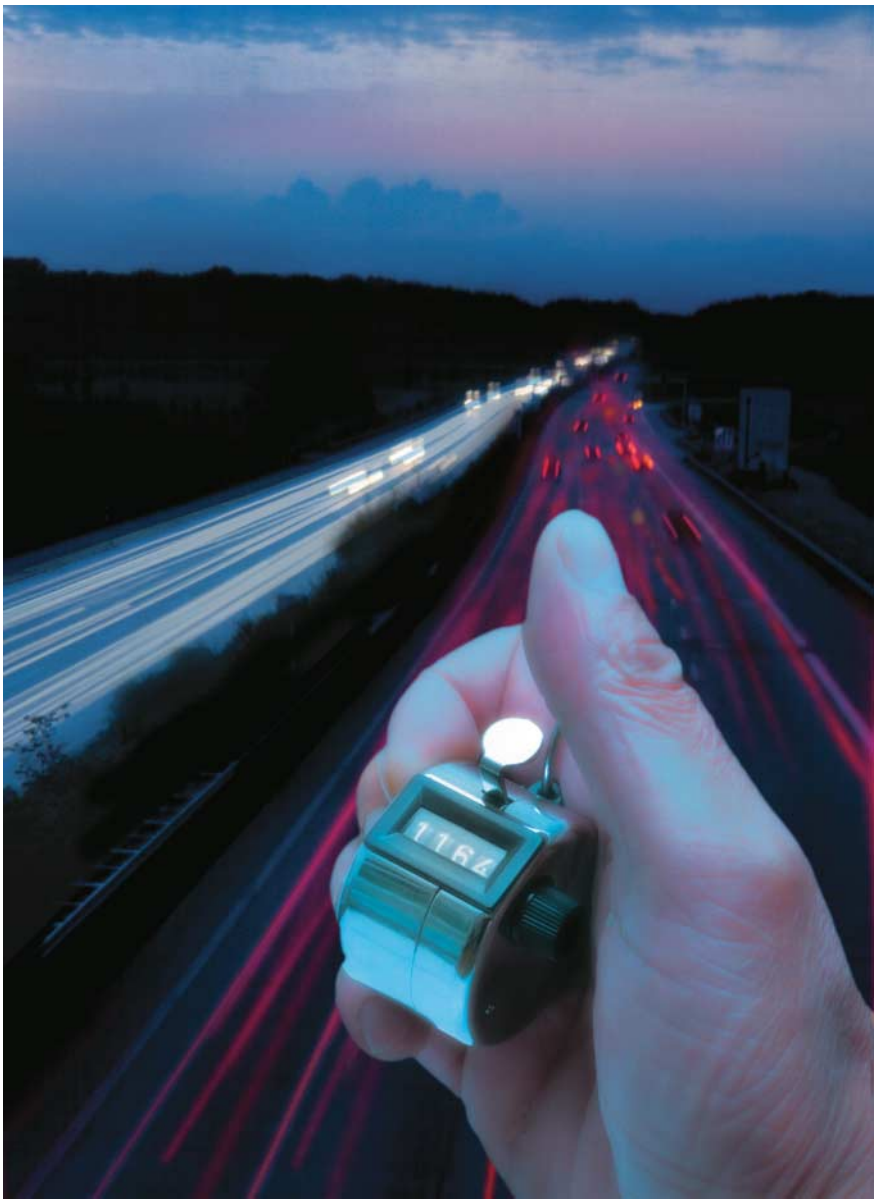


IP-Datenverkehr messen und analysieren

Die Route als Ziel

Dominique Petersen, Sebastian Schmidt, Norbert Pohlmann

Berechnen lassen sich die komplexen Internet-Datenströme nicht. An strategischen Punkten des Netzes platzierte „Drohnen" können jedoch die Verfügbarkeit von Services messen, Routen visualisieren und dadurch helfen, Angriffe oder Störungen wie den DE-CIX-Ausfall im Juni schneller zu erkennen.

Nicht nur die ununterbrochene Verfügbarkeit des Internet gilt heutzutage als selbstverständlich, sondern auch seine Allgegenwart. Es steht überall bereit, sei es am privaten DSL-Anschluss, im Hotel oder via Mobilfunk. Die übertragenen Informationen scheinen immer einen optimalen Weg durch das weltumspannende Netz zu finden. Und trotz gelegentlicher Ausfälle wichtiger Routen sind die meisten Server ständig erreichbar.

Jedes durchs Internet transportierte Datenpaket trägt eine Ziel-IP-Adresse und hat damit einen eindeutigen Empfänger. Damit die Pakete am Bestimmungsort ankommen, muss jeder Router, den die Pakete passieren, wissen, wie er mit ihnen verfahren und wohin er sie weiterleiten soll. Dazu baut er sogenannte Routingtabellen auf. Die Wegewahl erfolgt anhand weltweit eindeutiger, hierarchischer Netzadressen. Bei den meisten kleineren Routern geschieht dieser Aufbau automatisch nach dem Einschalten des Gerätes.

Router auf Provider-Ebene sind leistungsfähige Netzwerkkomponenten, die viele Gigabit/s transportieren. Für einen hohen Durchsatz muss die Bearbeitungszeit pro Paket (Latenz) minimal sein. Optimierungspotenzial besteht vor allem bei der Entscheidung, auf welcher Übertragungsleitung der Router ein eingehendes Paket weiterleiten soll. Es geht darum, Pakete über den Weg mit den geringsten „Kosten" zum Ziel zu bringen. Mögliche Metriken sind die „Hops" (Zahl der Router, die das Paket passiert), finanzielle Kosten, Verlässlichkeit, Durchsatz und Verzögerung der jeweiligen Verbindung.

Informationen über den Informationsfluss

Beim statischen Routing bleiben die Tabellen in den Vermittlungsknoten über längere Zeit unverändert. Bei der adaptiven Variante passen die Router ihre Entscheidungen laufend an den Zustand des Netzes an. Für die Wegewahl sind Veränderungen der Topologie oder der Auslastung einer Leitung entscheidend. Um den momentanen Netzzustand bei der Routingwahl berücksichtigen zu können, ist ein Informationsaustausch zwischen den beteiligten Knoten notwendig.

Netze unter einheitlicher Verwaltung (etwa einer großen Firma, eines Internet-Providers oder einer Hochschule) sind zu „autonomen Systemen" (AS)

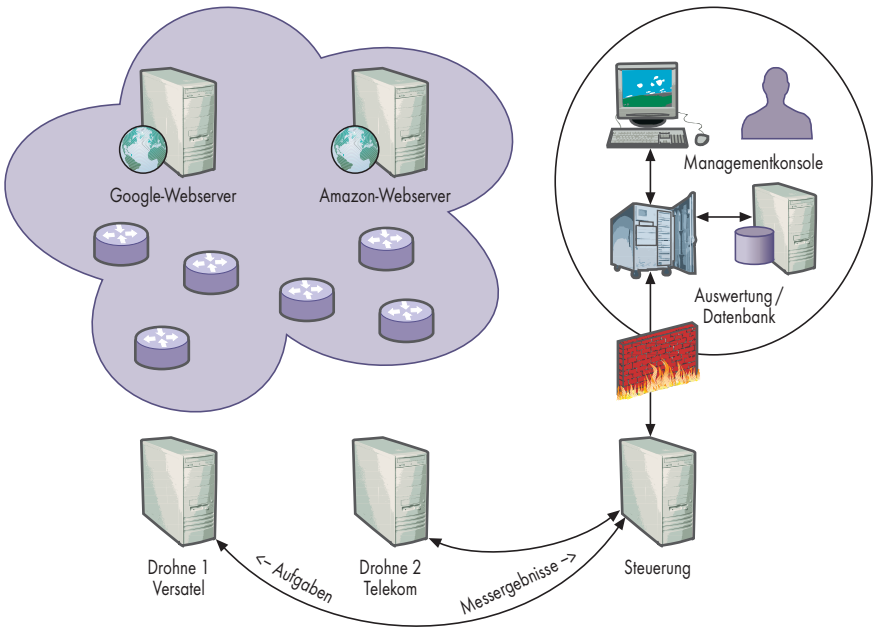
zusammengefasst. Ein AS-Betreiber lässt sich von seiner regional zuständigen Vergabestelle (etwa RIPE in Europa) einen IP-Adressbereich für sein Netz zuteilen. Als eindeutige Kennzeichnung erhält das AS eine Nummer, die gleich mehrfach als Schlüssel im weltweiten Routing zwischen den AS dient.

Zunächst repräsentiert die AS-Nummer die Gesamtheit aller Netze im Verantwortungsbereich eines Providers. Das können die Netze sein, die er selbst für seine Server benötigt, aber auch Netze und Adressblöcke für Kunden, die kein eigenes AS benötigen. Unter der AS-Nummer lassen sich IP-Subnetze eines Netzbetreibers zusammenfassen. Das vereinfacht vor allem das Routing auf oberster Ebene, also zwischen AS. Zwar muss nicht jedes den Weg für alle einzelnen IP-Subnetze kennen, aber jedes muss bei Bedarf abfragen können, zu welchem AS die gewünschte IP-Adresse gehört, um die Daten dorthin übertragen zu können.

Ein AS kann aus vielen Netzen bestehen, die über interne Router, sogenannte Interior Gateways (IG), miteinander verbunden sind. Exterior Gateways (EG) hingegen verbinden unterschiedliche AS miteinander. Beide verwenden unterschiedliche Protokolle. Ein Interior Gateway Protocol (IGP) muss lediglich Pakete so schnell wie möglich von der Quelle zum Ziel befördern – auch in großen internen Netzen mit komplizierter Topologie.

Als Exterior Gateway Protocol (EGP) dient derzeit praktisch allein das Border Gateway Protocol (BGP). Beim Datentransport von einem zum anderen AS müssen Router besondere Regeln beachten – nicht nur technische, sondern auch politische, wirtschaftliche oder sicherheitsbezogene. Manch ein Unternehmen kann oder will sein Netz nicht zum Transportieren von Daten zwischen fremden AS zur Verfügung stellen, obwohl es auf dem kürzesten Weg zwischen den beiden fremden Systemen liegt. Andererseits ist die Firma vielleicht bereit, Transitverkehr für ihre Nachbarn oder bestimmte andere AS zu übernehmen, falls die dafür bezahlen. Gerade in diesem Fall stellen Telekommunikationsgesellschaften einander ihre Übertragungsdienste gerne zur Verfügung.

Andere Beispiele für besondere Regeln sind, dass der eigene Datenverkehr nie durch bestimmte AS fließen soll, etwa dass vom Pentagon ausgehender Datenverkehr niemals in den Iran gelangen darf. Die nötigen Regeln und Maßnahmen konfiguriert ein Administrator normalerweise manuell oder halbautomatisiert in jedem BGP-Router, da sie nicht Teil des eigentlichen Protokolls sind. Eine Vorstellung, wie komplex Routen allein von großen Firmen in Deutschland sind, vermittelt eine Karte der Internet-Infrastruktur unter www.internet-sicherheit.de (siehe *iX*-Link).



In verschiedenen Internet-Zugangsnetzen verteilte Drohnen gewähren Einblicke in Routing-Vorgänge und Service-Qualität (Abb. 1).

Internet-Verfügbarkeits-System

Zum Beobachten und Auswerten von Veränderungen im so kritischen Routing hat das Institut für Internet-Sicherheit das Internet-Verfügbarkeits-System (IVS) entwickelt: Sogenannte Drohnen sind an strategischen Punkten im Internet platziert und sammeln Informationen über die Verfügbarkeit ausgewählter Server (Abb. 1). Eine Drohne besteht im Kern aus einer in C++ geschriebenen Software, die periodisch Server anfragt und die Verbindungsqualität misst. Sie läuft derzeit auf jeder üblichen Linux-Distribution. Besondere Anforderungen an die Hardware bestehen nicht, da keine komplexen Analyseprozesse auf den Drohnen laufen.

Drohnen können verschiedene Kriterien der Internet-Verfügbarkeit überwachen, darunter die Erreichbarkeit wichtiger Webseiten, DNS-Server, E-Mail-Dienste oder eben das Routing. Sie messen periodisch Dienstgüteparameter wie Quality of Service, Bandbreite oder Paketverlustrate. Die Drohnen senden ihre Messwerte an ein zentrales Auswertungssystem, das die Daten aufbereitet und analysiert. Zum Konfigurieren steht dem Administrator ein zentrales Management-Interface auf einem Server im Institut für Internet-Sicherheit zur Verfügung.

iX-TRACT

- Eine grafische Darstellung von Internet-Routen erleichtert den Überblick über die Vorgänge beim Datentransport.
- Je mehr an strategisch günstigen Punkten platzierte Messrechner, sogenannte Drohnen, Teile des Internet-Datenverkehrs aufzeichnen, desto genauer wird das Gesamtbild.
- Die Messergebnisse der Drohnen-Software, die die Verbindungsqualität zwischen Teilnetzen repräsentieren, lassen sich für Angriffsalarme oder Optimierungen der Infrastruktur nutzen.

Sicheres Routing

Ändert sich die Infrastruktur eines AS, kann das auch Änderungen am Internet-Routing nach sich ziehen. Das teilt ein BGP-Router den Pendants in anderen AS über Update-Nachrichten mit. „Route Withdrawals“ und „Route Advertisements“ entfernen Routen oder fügen sie hinzu. Der derzeitigen BGP-Implementierung fehlen Mechanismen, mit denen Router überprüfen können, von wem derlei Updates wirklich stammen und ob sie legitim sind. So kommt es immer wieder vor, dass Routen wegen Konfigurationsfehlern gelöscht werden oder ins Nichts führen.

Selbst Szenarien, in denen böswillige Hacker Datenströme über ihre eigenen Router lenken, um Inhalte zu manipulieren oder mitzulesen, sind denkbar. Zwei populäre Beispiele für BGP-Fehlkonfigurationen ereigneten sich 2008 bei der Pakistani Telekom und 2010 beim Internet-Provider IDC China (siehe *iX*-Links).

Im ersten Fall wollte Pakistani Telekom den Zugriff auf YouTube lediglich für Pakistan sperren und verbreitete eine Route, die Pakete an YouTube ins Nichts lenkte. Diese Route verbreitete sich jedoch im ganzen Internet und sperrte YouTube somit für alle Benutzer.

Im zweiten Fall erklärte sich der chinesische ISP durch einen Konfigurationsfehler für das Routing von rund 37 000 IP-Netzen zuständig. Anfragen von Internetnutzern, bei denen diese falschen Routen als die kürzesten erschienen, landeten in China, wo sie vermutlich unbeachtet versickerten.

Eine mögliche Lösung für diese Probleme wäre Secure BGP, das mittels Public-Key-Infrastruktur sicherstellen soll, dass BGP-Router überprüfen können, ob empfangene Routen-Updates authentisch sind. Bisher konnte sich S-BGP allerdings nicht durchsetzen.

Über einen Controller fragen die Drohnen in regelmäßigen Abständen nach, ob neue Aufträge für sie vorliegen. Er dient außerdem als Ansprechpartner für die Auslieferung der gesammelten Messdaten. Da die Drohnen von sich aus aktiv Server abfragen, ist ihre Platzierung und Nutzung unabhängig von Dritten.

Intern besteht eine Drohne aus mehreren Modulen, darunter einem Plug-in für HTTP-Requests und für die Traceroute-Funktion. Des Weiteren kann das System durch Zeitmessungen feststellen, wie lange einzelne Pakete unterwegs waren, und dadurch auf eine mögliche Auslastung der Strecke schließen.

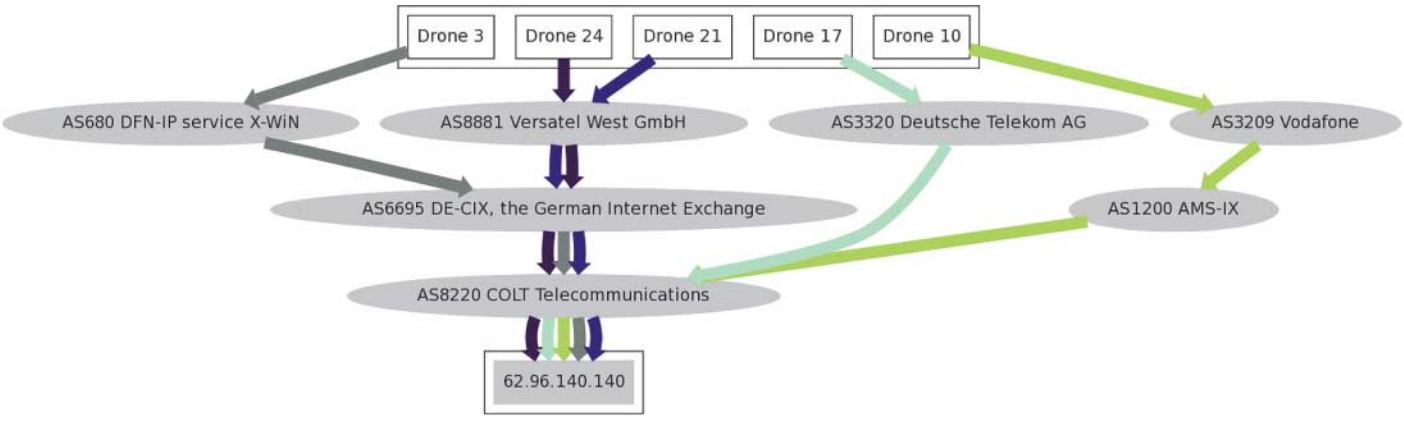
Das Internet-Verfügbarkeits-System ist seit einigen Jahren als Forschungsprojekt in Betrieb. Zwar wären die Drohnen auch geeignet, im Auftrag von Unternehmen die Funktion von deren Servern und Diensten zu überwachen, aber dafür sind spezialisierte Monitoring-Werkzeuge wie Nagios besser geeignet. Das IVS dient vielmehr dazu, die Verfügbarkeit eigener oder fremder Server von verschiedenen Punkten im Internet aus zu beobachten.

Ein Webseitenbetreiber möchte zum Beispiel wissen, wie es um die Verbindungen zwischen verschiedenen Anschluss-Providern und seinen Servern bestellt und wie gut seine Dienstleistung für die Kunden erreichbar ist. Mithilfe der Routing- und Qualitätsinformationen könnte er die Verfügbarkeit optimieren. Eine ausreichende Zahl von Messdaten vorausgesetzt, lassen sich die Routen visualisieren sowie Vergleiche von DSL-Providern untereinander oder zwischen Anschlüssen eines Providers in verschiedenen Regionen anstellen. So ließe sich ermitteln, wo ein Provider sein Anschlussnetz ausbauen müsste, um einen einheitlichen Qualitätsstandard bei allen Kunden zu erreichen. Vergleiche zwischen Providern könnten zudem für das Marketing von Interesse sein.

Da die Drohnen-Software wenig Ansprüche an die Hardware stellt (Mindestvoraussetzungen: 200 MHz, 16 MByte RAM), läuft sie auch auf handelsüblichen DSL-Routern, für die es Linux-Distributionen wie OpenWrt oder DD-WRT gibt. Für die breite Verteilung solcher Drohnen ist das essenziell, da DSL-Router in privaten Haushalten meist kleine All-in-One-Geräte sind und weil es dort selten andere geeignete Hardware gibt, die rund um die Uhr läuft. Die in den folgenden Abschnitten vorgestellten Messergebnisse basieren auf den Messungen solcher Drohnen auf DSL-Routern in privaten Haushalten, die in unterschiedlichen Provider-Netzen platziert sind.

Routen im grafischen Überblick

Ein zentraler IVS-Server sammelt die Traceroute-Daten, die sich anschließend auswerten und visualisieren lassen (siehe Abbildungen). Jeweils aufeinanderfolgende Router eines Traceroute-Ergebnisses sind in den Graphen als benachbarte Knoten miteinander verbunden. Router, die einen Timeout erzeugten, tauchen in den Grafiken nicht auf. Router mit der gleichen IP-Adresse oder AS-Nummer sind zu einem Knoten zusammengefasst. Die Dicke der Kanten zwischen den Routern stellt die Anzahl der einzelnen ursprünglichen Traceroute-Graphen dar, die diese Verbindung nutzen. Das zeigt, welche



Datenfluss zwischen mehreren IVS-Drohnen und dem Webserver von Xing (Abb. 2)

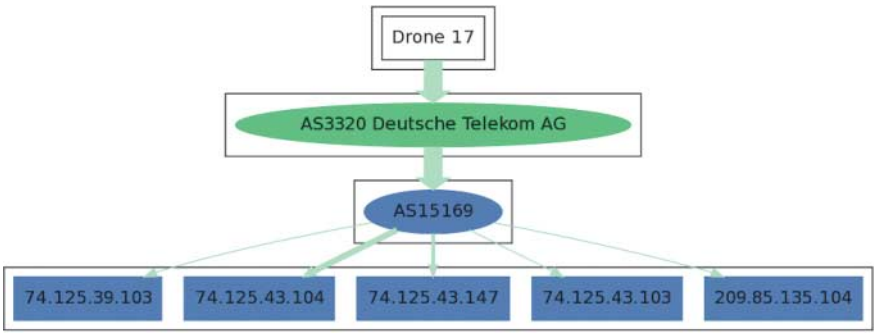
Routen häufiger in Benutzung sind als andere.

Grundsätzlich können Datenpakete jeden möglichen Weg nehmen. Fallen Verbindungen aus oder sind überlastet, können die Router laufend Anpassungen vornehmen und Pakete umleiten. Dieses dynamische Routing kann Nachteile haben. Es ist allgemein bekannt, dass unverschlüsselte E-Mails wie eine Postkarte anzusehen sind, die jeder lesen kann, der Zugriff auf eines der Systeme hat, die die E-Mail transportieren. Auf diese Weise lassen sich Firmengeheimnisse deutscher Unternehmen theoretisch auf Routern in Ländern wie China, Russland oder auch den USA abgreifen, die im Verdacht stehen, intensive Industriespionage zu betreiben. Viele Unternehmen ignorieren das Risiko und übertragen Nachrichten trotzdem immer noch unverschlüsselt. Zum Glück für die einheimische Industrie entfaltet das Internet seine Dynamik nur selten in vollem Umfang, eine E-Mail von Hamburg nach München nimmt also selten einen Weg über New York oder Moskau.

Zwischen dem Routing innerhalb autonomer Systeme und zwischen autonomen Systemen bestehen entscheidende Unterschiede. AS-intern kommen Algorithmen zum Einsatz, die sehr schnell auf Lastveränderungen von Routern und aktuelle Gegebenheiten reagieren. Routen ändern sich daher innerhalb eines AS ständig.

Zwischen unterschiedlichen AS sind die BGP-Routen dagegen nahezu konstant. Manchmal tritt über Tage oder Wochen keine einzige Änderung auf (Abb. 2).

Da es üblicherweise Priorität hat, Pakete möglichst schnell ans Ziel zu transportieren, dürfte die Bedrohung durch Mitlesen unverschlüsselter Pakete nicht allzu groß sein. Trotzdem gibt es keinen Grund, auf verschlüsselte Kommunikation zu verzichten.



Verteilung von Suchanfragen auf mehrere Google-Server (Abb. 3)

Webapplikationen wie die Suchmaschine Google, die mehrere Milliarden Suchanfragen täglich bewältigt, benötigen ganze Serverfarmen zum Abwickeln der Anfragen. Das dabei eingesetzte Load Balancing verteilt sie auf die Systeme (Abb. 3).

Load Balancing bei Google

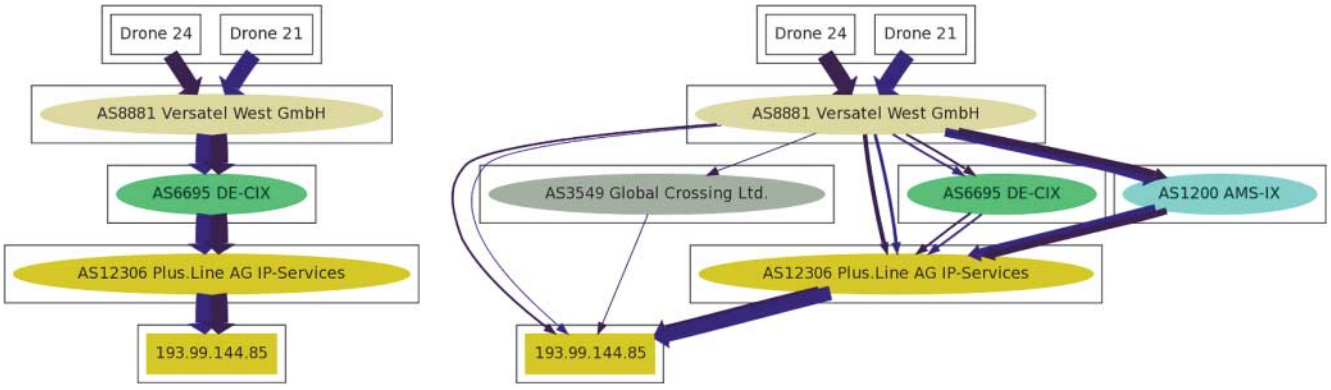
In diesem Fall lieferte die Traceroute-Daten eine IVS-Drohne im Telekom-Netz, das direkt mit Googles autonomem System 15 169 verbunden ist. Das Domain Name System ermittelt zum Namen www.google.de von der geografischen Position des Anfragenden abhängige IP-Adressen, verteilt die Anfragen so auf verschiedene physische Cluster und verringert damit unter anderem die „Round Trip Time“ (RTT, auch „Ping-Zeit“ genannt) der Verbindungen. Der angesprochene Cluster nutzt außerdem ein Hardware-Load-Balancing, das der Graph nicht zeigt [1]. Auf diese Weise läuft der Datenverkehr zwischen den autonomen Systemen fast aller großen deutschen Provider zu Google meist ohne Umweg durch andere AS, und die durchschnittliche Anzahl der Hops liegt bei nur acht.

Angriffe und Ausfälle im Blick

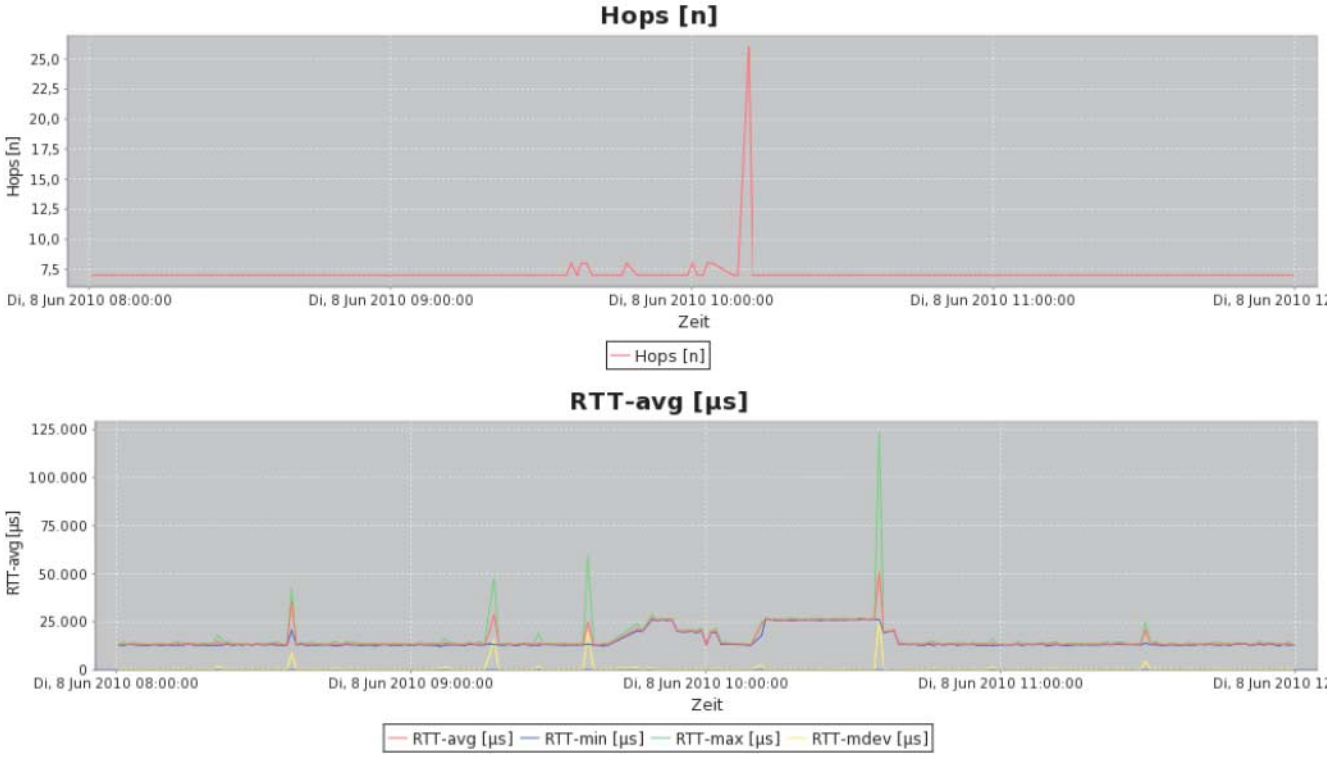
Eine wachsende Bedrohung für Internet-Dienstleister sind „Distributed Denial of Service Attacks“, kurz DDoS-Angriffe, die mithilfe großer Bot-Netze stattfinden und Onlinepräsenzen beeinträchtigen oder sogar blockieren. Die Gründe solcher Angriffe sind vielfältig. Manche Täter erpressen auf diese Weise Firmen, die bei einem Ausfall ihrer Services viel Geld verlieren würden, andere blockieren aus politischen Motiven Webseiten von Regierungen oder Parteien.

Nicht nur am jeweiligen Ziel richten solche Angriffe großen Schaden an. Auch andere Systeme können von der Paketflut betroffen sein, wenn Router unter der Last ihren Dienst versagen und Pakete verwerfen müssen.

Die Last des Angriffs verteilt sich aufseiten der angreifenden Systeme breit, fällt dort kaum auf und lässt sich gut handhaben, weil es sehr viele verschiedene mögliche Routen zum Ziel gibt. Doch die Auswahl an Routen schrumpft zum Ziel hin. Dort gibt es in



Der Weg der Datenpakete zwischen dem Versatel-Netz und www.heise.de vor dem und während des DE-CIX-Ausfalls im Juni 2010 (Abb. 4 und 5)



Nach dem DE-CIX-Ausfall stiegen die Anzahl der Hops zwischen dem Versatel-Netz und www.heise.de sowie die Round Trip Time aufgrund der massiven Routen-Änderungen (Abb. 6 und 7).

vielen Fällen weniger starke Hardware, die den Paketstrom in solchen Extremfällen nicht mehr handhaben kann. Die vorgestellte Visualisierungs-Technik kann dazu beitragen, die Auswirkungen eines solchen Angriffs und die der Gegenmaßnahmen sichtbar zu machen, um bei deren Koordination zu unterstützen.

Eingreifen kann das Internet-Verfügbarkeits-System jedoch nicht, da es sich um ein passives Messinstrument handelt. Theoretisch möglich wäre aber das automatisierte Erkennen beginnender DDoS-Angriffe. Ein Algorithmus, der die Drohnen für diesen Zweck geeignet platziert, befindet sich noch im Forschungsstadium.

Nicht nur durch einen DDoS-Angriff kann die Qualität der Verbindungen drastisch sinken, sondern auch wegen einer schlichten Panne. Am Morgen des 8. Juni 2010 etwa fiel aufgrund eines Switch-Fehlers für rund eine halbe Stunde der Datenaustausch (das „Peering“) zwischen am DE-CIX angeschlossenen Providern aus. Die mussten ihren Verkehr über andere Peering-Knoten weiterleiten (Abb. 4 und 5).

Das IVS kann die Folgen eines solchen Ausfalls darstellen. Administratoren könnten mit diesem Werkzeug somit rechtzeitig herausfinden, dass Ausfälle und schlechte Verbindungsqualität ihren Ursprung nicht im eigenen Netz hatten, sondern extern (Abb. 6 und 7).

Fazit und Ausblick

Die vom Internet-Verfügbarkeits-System ermittelten Messwerte sind auch für Forschung und Lehre interessant, da sie veranschaulichen, wie das Internet funktioniert und wie es auf Unregelmäßigkeiten reagiert. Schon 12 Drohnen haben während eines Tests innerhalb eines einzigen Monats bei einer Überwachung von 14 Domains bereits 2495 Router aus 188 unterschiedlichen autonomen Systemen erkannt. In einer Woche (an einem einzelnen Tag) verzeichneten sie Pakete aus immerhin noch 1277 (699) Routern und 122 (54) AS.

In Zukunft soll das IVS die wichtigsten Dienste und deren Anbieter im Blick haben, bei einer stark vergrößerten Anzahl von Drohnen. Zunächst soll sich das IVS auf das deutsche Internet konzentrieren. Es überwacht aber auch im Ausland gehostete Dienste, sofern diese wichtig für deutsche Nutzer sind. Mithilfe einer ständigen Routenüberwachung kann es zudem Routing-Störungen sofort erkennen – etwa wenn mal wieder ein großer Internet-Austauschknoten ausfällt. (un)

DOMINIQUE PETERSEN

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der FH Gelsenkirchen und betreut dort seit Januar 2007 den Bereich der Internet-Frühwarnsysteme als Projektleiter.

SEBASTIAN SCHMIDT

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit und dort seit August 2008 in der Forschung tätig.

PROF. DR. NORBERT POHLMANN

ist geschäftsführender Direktor des Instituts für Internet-Sicherheit und Professor an der FH Gelsenkirchen im Fachbereich Informatik und zuständig für den Master-Studiengang „Internet-Sicherheit“.

Literatur

[1] Luiz André Barroso, Jeffrey Dean, Urs Hölzle; Web Search for a Planet: The Google Cluster Architecture; IEEE Micro March-April 2003, S. 22–28

www.ix.de/ix1008096