Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

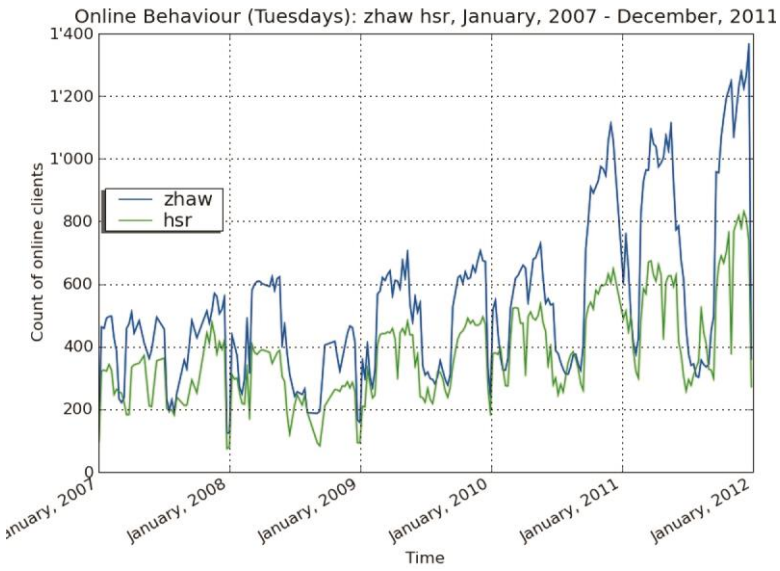
InIT Institut für angewandte
Informationstechnologie

Überwachung von Computernetzen

Diplomierende
David Halter
Thomas Strebel

Dozierende
Bernhard Tellenbach
Adrian Roth

Das Internet hat sich in den letzten Jahren zu einem riesigen komplexen Gebilde entwickelt, dessen rasches Wachstum neue Herausforderungen an die Wissenschaft stellt. Um ein reibungsloses Funktionieren weiterhin zu gewährleisten, müssen Informationen zur Auslastung, Sicherheit und dem zeitlichen Verlauf gesammelt werden. Diese werden mit Cisco NetFlow gespeichert und von Flowbox, einem primär von der ETH entwickelten Framework zur Analyse von Flowdaten, verarbeitet.
Das Ziel dieser Arbeit ist die Entwicklung zweier Module für dieses Framework. Im ersten geht es um die Detektion von Network Address Translators. Dies ist immer dann zentral, wenn es um Analysen geht, bei denen Werte, die pro Host erfasst werden, in die Auswertungsstatistik einfliessen. Hier verfälscht ein NAT die Auswertung, da sich hinter einem NAT, welches als einzelner Host in den Daten erscheint, mehrere reale Hosts verstecken können.
Im zweiten Modul wird das Onlinezeitverhalten von Hosts betrachtet und anhand dessen Statistiken aufgestellt. Es geht darum, zentrale Fragestellungen der Internetnutzung zu beantworten, wie beispielsweise die zeitliche Veränderung der in einem Netzwerk aktiven Hosts. Anhand der gefundenen Resultate können Empfehlungen gemacht werden, wie sich die Benutzer verhalten sollen, um Energie zu sparen. Abschliessend werden die Nutzungs- und Weiterentwicklungsmöglichkeiten der beiden Module diskutiert.



Um den Verlauf der Anzahl Hosts in verschiedenen Netzen festzustellen, wurden die Netzwerkdaten über neun Jahre jeden Dienstag Nachmittag verarbeitet.
Im Jahresverlauf sehen die Daten der ZHAW und der Hochschule Rapperswil (HSR) Daten sehr ähnlich aus. So lassen sich darin die folgenden Strukturen erkennen: Weihnachten, Semesterpausen und die Assessmentprüfungen.