Traffic-Analyse in (Software-Defined) Networks

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Prof. Dr. Torsten Braun

In Computernetzwerken steigt das Verkehrsaufkommen stetig an. In dieser Datenmenge sind fehlerhafte oder unerlaubte Verbindungen nur schwierig zu erkennen. Das Projekt befasst sich mit der Umsetzung einer Applikation zur Visualisierung von Verkehrsdaten. Die Darstellungen sollen die Analyse und den chronologischen Vergleich von Netzwerkflüssen erleichtern.

Einleitung

Bestehende Netzwerk-Analyse-Tools konzentrieren sich in den meisten Fällen auf die statistische Auswertung und Darstellung von Verbindungsdaten. Diese Arbeit hat zum Ziel, ein Netzwerk und dessen Verbindungen in einer Applikation als Graph darzustellen. Zu den Herausforderungen bei der Visualisierung von Verbindungsdaten gehören die grosse Datenmenge und die Verfügbarkeit von Testdaten. Die umfangreichen Daten sollen schnell verarbeitet werden und es muss eine übersichtliche Darstellungsmöglichkeit für die Verbindungen gefunden werden.

Methode und Konzept

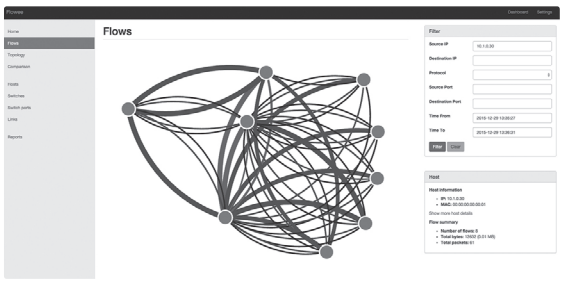
Auf Basis einer Voranalyse zu Datenquellen, Datenspeicherung und Applikationsframeworks wird die Applikation wie folgt umgesetzt:
Als Datenquelle wird ein Mininet mit ONOS als SDN-Controller eingesetzt. Über das REST API des Controllers werden die Flow-Daten periodisch abgefragt und in eine relationale Datenbank gespeichert. Die aggregierten Daten werden anschliessend in der Web-Applikation als SVG-Graph (d3.js) dargestellt. Die Web-Applikation wurde auf Basis des Web-Frameworks Symfony implementiert.
Dank SDN ist es möglich, verschiedene Szenarien einfach zu simulieren und die Applikation auf oben erwähnte Herausforderungen zu prüfen. Anhand der Simulationen können die Datenbank-Abfragen und die Visualisierungen getestet und damit schrittweise optimiert werden.

Resultat

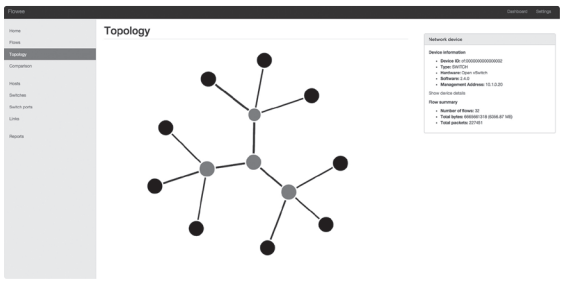
Mit Flowee ist es möglich sowohl das Netzwerk als auch den darin fliessenden Verkehr darzustellen. Dank Flowee können Verkehrs-Metadaten, im Gegensatz zu bestehenden, meist textbasierten Tools, visuell sichtbar gemacht werden. Bei der Analyse von Netzwerkprotokollen kann die Visualisierung Aufschluss über deren Funktionsweise im Netzwerk bieten.
Mittels Aggregation und Filterung ist es gelungen, die Verbindungsdaten so darzustellen, dass ein interpretierbarer Graph entsteht. Mit dieser Darstellung lassen sich unter anderem auch störende oder unerlaubte Verbindungen identifizieren. So können auch bei grossen Datenmengen sicherheitsrelevante Ereignisse erkannt werden.
Mit dem realisierten Datenmodell werden auch komplexe Fragestellungen beantwortet und es können zusätzliche Informationen aus den Flussdaten gewonnen werden. Flowee implementiert zum Beispiel einen Algorithmus, der es erlaubt die Auslastung eines Netzwerk Ports anhand von Flow-Daten zu berechnen.
Die Gegenüberstellung zweier Graphen erlaubt zudem visuelle Vergleiche.

Franziska Corradi

Simon Krenger



Flow-Darstellung



Topologie-Darstellung