



## Verkehrscharakterisierung anhand von Flow-Eigenschaften

### Motivation

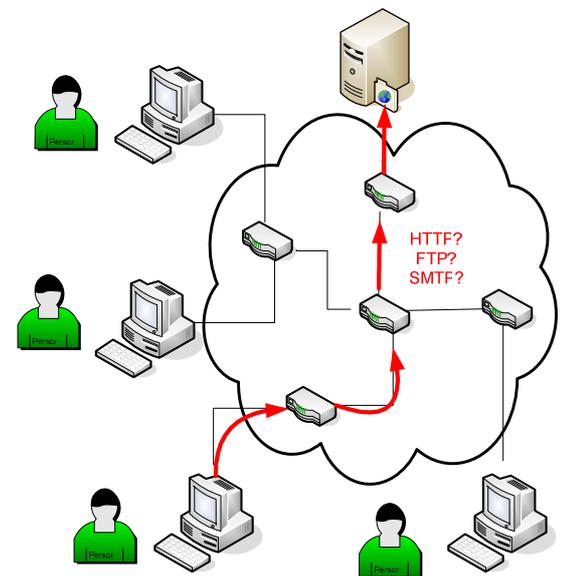
War es früher möglich verschiedene Anwendungen anhand von Portnummern zu identifizieren, kann dieses Vorgehen heute zu Problemen führen. In vielen Netzwerken werden Ports unerwünschter oder unbekannter Dienste gefiltert. Anwendungen gehen deshalb vermehrt dazu über, ihre Ports dynamisch festzulegen (z.B. Skype). Auch werden offene Ports, die eigentlich für bestimmte Dienste reserviert sind (z.B. Port 80 für http), von anderen Anwendungen zum Transportieren ihrer Daten „missbraucht“.

Um im Netzwerkverkehr dennoch Protokolle und Anwendungen identifizieren zu können muss der Verkehr genauer betrachtet werden. Eine Möglichkeit ist, das Verhalten von Verkehrsströmen (Flows) zu untersuchen und mit dem bekannter Dienste oder Anwendungen zu vergleichen. Charakteristisch können zum Beispiel die zeitliche Abfolge und die Größe der ausgetauschten Nachrichten sein.

### Aufgabenstellung

Im Rahmen der Diplom- oder Studienarbeit soll zunächst das Verhalten verschiedener Protokolle und Anwendungen anhand von Messdaten untersucht werden um herauszufinden, welche Eigenschaften für die Verkehrscharakterisierung geeignet sind. Anschließend ist ein Verfahren zu entwickeln, mit dem Protokolle und Anwendungen unterschieden und identifiziert werden können. Das Verfahren soll als neues Modul in ein bestehendes Verkehrsmess- und analysesystem integriert werden.

Der Umfang der Arbeit richtet sich danach, ob ein sie als Studien-/ Bachelor- oder Diplom-/Masterarbeit vergeben wird.



### Voraussetzungen

C/C++ oder Java-Kenntnisse  
Grundlegende Kenntnisse über statistische Methoden empfohlen

