Technische Universität München
**Lehrstuhl für**
**Netzarchitekturen & Netzdienste**
Prof. Dr. Georg Carle

15.3.2013

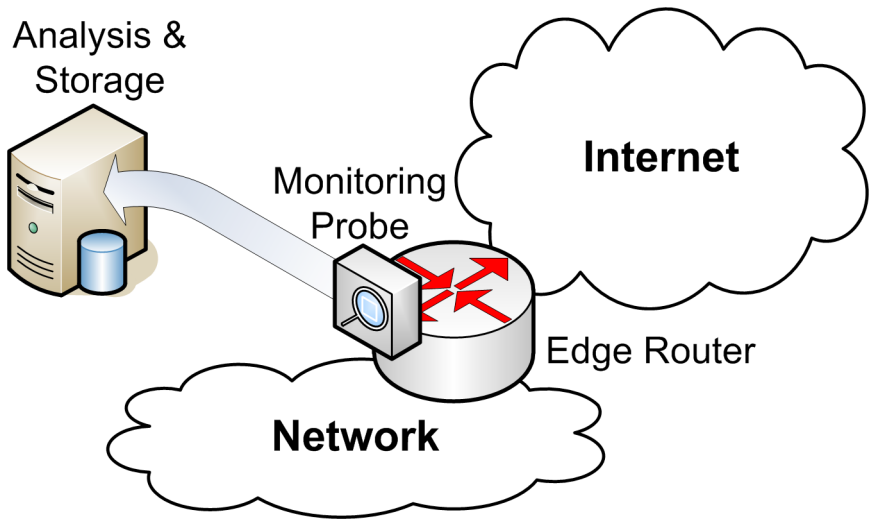
# Diplom-/ Bachelor-/ Masterarbeit/SEP

# Anomalie-Erkennung in Hochgeschwindigkeitsnetzen

## Beschreibung

IT-Verkehrsnetzwerkinfrastrukturen spielen heute eine zentrale Rolle bei der weltweiten Kommunikation und haben nicht nur eine wichtige wirtschaftliche Bedeutung. Der fortwährend steigende digitale Informationsaustausch erfordert eine stetig wachsende Bandbreite im Bereich der optischen Übertragungstechnik.

Um die Sicherheit und Robustheit dieser Hochgeschwindigkeitsnetze zu erhöhen, muss der umfangreiche Datenverkehr möglichst in Echtzeit untersucht werden. Durch Analyse von an zentralen Infrastrukturkomponenten, wie an Edge Routern beobachteten Daten erfolgt eine Erkennung von Anomalien. Diese weisen auf eventuell vorhandene Fehlkonfigurationen und Bedrohung im Netzwerk hin. Allgegenwärtige Angriffe z.B. durch Botnetze, Trojaner oder Scanattacken sollen auf die Weise frühzeitig enttarnt werden.




## Aufgabenstellung

Im Rahmen der Arbeit sollen unter Berücksichtigung der hohen Datenraten von bis zu 100 GBit/s geeignete Algorithmen angewandt werden, welche eine folgende parallelisierte Echtzeitanalyse ermöglichen. Hierfür sind Erkennungsalgorithmen und zugehörige Parameter zu finden, die auf Basis von erhobenen Flow- oder Paketdaten Anomalien feststellen und eine möglichst geringe Fehlerkennungsrate aufweisen. Um dies zu erreichen, sollen zu Beginn Bedrohungsszenarien in Hochgeschwindigkeitsnetzen identifiziert und beschrieben werden, um abschließend darzustellen, in welchem Umfang eine zeitnahe Detektion möglich ist.

Der Umfang der Arbeit richtet sich nach dem Typ (BA/SEP oder MA/DA) und kann in mehrere Arbeiten aufgeteilt werden.

## Infos & Kontakt

Simon Stauber <stauber@net.in.tum.de> Tel.: 289-18011
Lothar Braun <braun@net.in.tum.de> Tel.: 289-18010