Sarthak **Grover**

Network Security and Machine Learning Expert

☐ (+91) 79821 30021
✉ sgrover@protonmail.ch
☐ groversarthak   Ⓢ shahifaqeer
⌂ https://sarthakgrover.github.io

Education

MA (PhD Incomplete) in Computer Science   *Princeton, New Jersey, USA*
Princeton University   *Apr. 2016*
- Received research assistance for work on Network Performance Analysis and Home Network Security.
- Awarded STEM Chateaubriand Fellowship by the Embassy of France for work on the Internet of Things (2016).
- Advisor: Prof. Nick Feamster
- GPA: 3.8/4.0

BTech and MTech in Electronics and Communication Engineering   *Roorkee, INDIA*
Indian Institute of Technology, Roorkee   *Dec. 2010*
- Specialization in Wireless Communication.
- Thesis: Performance Evaluation of Cross-Layer Wireless Body Area Networks.
- GPA: 8.06/10.00

Skills

Programming	Python v2.7, v3.3 – v3.7, iPython v7.8, Scala v2.11, Java v12.0, PostgreSQL, C/C++, R, Matlab, Node.js
Analytics	Pandas v0.13 – v0.23, Scikit-Learn v0.21, Tensorflow v1.14.0 – v2.0.0, Apache Spark, Numpy, Scipy, Matplotlib
Networking	Wireshark/Tshark v2.0, Iperf v2.0 – v3.7, Nmap v7.8, Scapy v2.4, Urllib3, Requests, Beautiful Soup 4, Networkx
Tools	PyCharm, PyLint, IntelliJ IDEA SBT, Eclipse, Git, Linux, Adobe Photoshop, Corel Draw, MS Office, LaTeX

Work Experience

Sugandhaa Co., Ltd.   *New Delhi, INDIA*
Manager and Freelance Researcher   *Apr. 2018 - Present*
- Leading a family-owned business. Responsible for inventory, account management, and conducting sales.
- Proficient in interacting directly with customers and managing daily finances to ensure smooth business operations.
- **Network anomaly detection:** Designed and implemented an anomaly detection algorithm for NetFlow records.   [Link]
- Used machine learning to extract and transform packet features and detect anomalous behavior in real-time.
- Successfully identified port scans and DoS activity using statistical, information-theoretic, and clustering-based approaches.
- **CDN performance analysis:** Conducted website measurements and tested performance of web page load times.   [Link]
- Developed a scalable rule-based CDN estimation algorithm for websites using xcache, whois, parsing, and DNS information.
- Revealed that for some websites, performance can be substantially improved using CDNs offered by their own ASNs.
- **Coursework:** Awarded certificate for Neural Networks and Deep Learning by deeplearning.ai on Coursera.   [Link]
- Awarded certificate for Functional Programming Principles in Scala by EPFL on Coursera.   [Link]

Princeton University   *Princeton, NJ, USA*
Graduate Research Assistant   *Jan. 2015 - Sep. 2017*
- Advisers: Prof. Nick Feamster (University of Chicago) and Dr. Roya Ensafi (University of Michigan)
- **Identifying Internet of Things (IoTs):** Captured and analyzed packets from various IoT devices in the lab.   [Link]
- Used machine learning to extract and transform (FFT, PCA, MMT, KDE) volumetric and distribution features from packet headers.
- Used clustering (kmeans, Spectral, MeanShift, DBSCAN) to identify IoTs, and distinguish activity and background traffic.
- Built an IoT behavior monitor and demonstrated that it successfully detects DDoS attack anomalies using DBSCAN.   [Link]
- **Real-time IoT query system:** Developed a filtering algorithm to discard non-IoT network traffic using DNS queries.   [Link]
- Implemented an exploratory ETL pipeline in PySpark to extract packet header features and cluster IoT network traffic.
- **Internet of Unpatched Things:** Tested multiple IoT devices in the lab and exposed their vulnerabilities.   [Link]
- Found that PixStar's digital photo frame was susceptible to eavesdroppers and fails to encrypt photographs, and the Nest thermostat exposed private location information of nearest weather stations to the ISP (now patched).
- **Broadband traffic analysis:** Analyzed usage behavior of customers offered higher speed broadband without their knowledge.
- Found that difference in traffic demand was higher for moderate users as compared to high-volume subscribers.   [Link]
- Presented at PAM (Mar 2016), CableLabs (Jul 2016), and FCC (Oct 2016).   [Link]
- **Teaching Assistant:** Developed material for Fog Networks and the Internet of Things, Coursera MOOC.   [Link]

Comcast   *Philadelphia, PA, USA*
Research Intern   *May. 2016 - Aug. 2016*
- Advisers: Jason Livingood (VP, Comcast) and Nirmal Mody (Manager, Comcast)
- Customer Owned and Managed (COAM) Internet of Things (IoT) security: Used DPI to study connectivity, security, and privacy of a subset of Comcast smart homes. Developed a script to search for PII in unencrypted IoT data.
- Used DNS queries to filter smart homes. Identified a misconfigured XBOX for one subscriber by correlating IoT packet captures.

Georgia Institute of Technology
Graduate Research Assistant

Atlanta, GA, USA
Aug. 2012 - Dec. 2014

- Advisers: Prof. Nick Feamster (University of Chicago) and Prof. Renata Teixeira (INRIA Paris)
- **Home network analysis:** Analyzed active and passive network traces from multiple homes to study network availability and reliability in various countries, popular devices and infrastructure in homes, and traffic usage with time. [Link]
- Discovered most home traffic is exchanged to a small number of domains, and home network usage differs based on the device.
- Analyzed prevalence and persistence of traceroutes to a variety of Internet destinations from the perspective of access points.
- **SAZO:** Built and deployed a blacklist based malware identification and notification system on the home router. [Link]
- Used bloom-filters to index malicious IPs and perform quick look-ups on packet headers before redirecting traffic to DPI boxes.
- **Facade:** Built and deployed an HTTP pluggable transport protocol to avoid censorship and detection for Tor. [Link]
- Responsibilities included parallelizing code, implementing framing buffers, and unit testing the system in a team of 6 students.
- **QoS control using SDN:** Identified application and used SDNs to program appropriate rate shaper and control network flow.
- Identified traffic using a DNS classifier and demonstrated ad-block for the whole home using FlowQoS at the access point. [Link]

INRIA
Research Engineer

Paris, FRANCE
May. 2014 - Sep. 2014

- Advisers: Prof. Renata Teixeira (INRIA Paris) and Dr. Christian Kreibich (ICSI Berkley).
- Browserlab: Home network diagnosis for performance bottleneck detection: Tested uplink and downlink broadband performance between devices, gateways, and online servers to detect if the bottleneck is in the local wireless network or at the edge router.

LIP6, UPMC
Research Engineer

Paris, FRANCE
Jun. 2013 - Sep. 2013

- Adviser: Prof. Renata Teixeira (INRIA Paris).
- Home network troubleshooting platform using Fathom and BISmark: Programmed active traceroute test on bismark router and analyzed latency and throughput performance from routers.

North Carolina State University
Research Associate

Raleigh, NC, USA
Dec. 2011 - Apr. 2012

- Adviser: Prof. Injong Rhee (VP - IoT, Google).
- Indoor Localization for Samsung Smartphones using Radio: Implemented FM/AM transceiver systems on GNURadio to utilize the time difference in RDS information for performing accurate indoor localization on smart phones.

Indian Institute of Science
Junior Research Fellow

Bangalore, INDIA
Apr. 2011 - Dec. 2011

- Adviser: Prof. Anurag Kumar (Director, IISc Bangalore).
- WSNs for Societal Needs and Disaster Management: Prepared work-plan proposal for submission to the Department of Science and Technology (DST), Govt of India.
- Computed closed-formed expressions for network reliability for regular hexagonal network topology.
- Evaluated information-theoretic bounds on network reliability for random hybrid network topology.

University of New South Wales
Practicum Exchange

Sydney, AUSTRALIA
May. 2009 – Aug. 2009

- Adviser: Prof. Vijay Sivaraman (UNSW)
- Wireless Body Area Networks for Athlete Monitoring: Analyzed time-series experimental data collected from wireless bio-medical sensors. Developed encounter based model to capture user mobility, and generate synthetic network topologies. [Link]
- Modeled the evolution of connectivity with time, and computed correlation of connectivity using Cholesky decomposition.
- Evaluated the connectivity model using Kolmogorov-Smirnov (K-S) test. Publication awarded Best Paper at WiMob 2010.

Selected Publications

A Case Study of Traffic Demand Response to Broadband Service-Plan Upgrades
    Sarthak Grover, Roya Ensafi, and Nick Feamster
    Proceedings of 17th International Conference on Passive and Active Measurement (PAM), 2016, Heraklion, Greece

The Internet of Unpatched Things
    Sarthak Grover and Nick Feamster
    Proceedings of FTC PrivacyCon, 2016, Washington, DC, USA

Facade: High-Throughput, Deniable Censorship Circumvention Using Web Search
    Ben Jones, Sam Burnett, Nick Feamster, Sean Donovan, Sarthak Grover, Sathya Gunasekaran, and Karim Habak
    4th USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2014, San Diego, CA, USA

Panoptes: Detecting Malware Activity in Home Networks
    Sarthak Grover and Nick Feamster
    HomeSys: Workshop on Design, Technology, Systems and Applications for the Home (UbiComp), 2013, Zurich, Switzerland

Peeking Behind the NAT: An Empirical Study of Home Networks
    Sarthak Grover, Mi Seon Park, Srikanth Sundaresan, Sam Burnett, Hyojoon Kim, Bharath Ravi, and Nick Feamster
    Proceedings of the ACM Internet Measurement Conference (IMC), 2013, Barcelona, Spain