Sivaramakrishnan Ramanathan

http://sivaram.me
satyaman@usc.edu

Research Interests

My research focuses on using partial observations for effective network protection and management.

Education

University of Southern California, Ph.D., Computer Science 2016-Present
Advisors: Dr. Jelena Mirkovic and Dr. Minlan Yu

University of Southern California, M.S., Computer Science 2014-2016
Specialization: Computer Networking

BMS College of Engineering, B.S., Computer Science 2010-2014
GPA: 9.2/10

Work Experience

Facebook	**BGP compiler for Facebook datacenter** *Intern with Ying Zhang*	**Summer** 2020
ICSI	**Quantifying the impact of blocklisting** *Intern with Sadia Afroz*	Summer 2019
AT&T Labs Research	**Enabling machine learning in switches** *Intern with Balachander Krishnamurthy and Yaron Kanza*	Summer 2018
AT&T Labs Research	**Prober for measuring propagation delays** *Intern with Balachander Krishnamurthy and Yaron Kanza*	Summer 2017

Conference Publications

[1] Quantifying the Impact of Blocklisting in the Age of Address Reuse
Sivaramakrishnan Ramanathan, Anushah Hossain, Jelena Mirkovic, Minlan Yu and Sadia Afroz.
Proceedings of ACM Internet Measurement Conference (IMC), 2020.
Acceptance Rate: 53/216 (24.5%)

[2] PINT: Probabilistic In-band Network Telemetry
Ran Ben Basat, **Sivaramakrishnan Ramanathan**, Yuliang Li, Gianni Antichi, Minlan Yu, and Michael Mitzenmacher.
ACM SIGCOMM, 2020.
Acceptance Rate: 54/250 (21.6%)

[3] BLAG: Improving the Accuracy of Blacklists.
Sivaramakrishnan Ramanathan, Jelena Mirkovic and Minlan Yu.
Proceedings of Network and Distributed System Security Symposium (NDSS), 2020.
Acceptance Rate: 88/506 (17.4%)

[4] SENSS Against Volumetric DDoS Attacks.
Sivaramakrishnan Ramanathan, Jelena Mirkovic, Minlan Yu and Ying Zhang.
Proceedings of Annual Computer Security Applications Conference (ACSAC), 2018.
Acceptance Rate: 60/299 (20.1%)

[5] SDProber: A Software Defined Prober for SDN.
Sivaramakrishnan Ramanathan, Yaron Kanza and Balachander Krishnamurthy.
Proceedings of the Symposium on SDN Research (SOSR), 2018.
Acceptance Rate: 18/63 (28.5%)

Workshop Publications

[6] Enabling SDN Experimentation in Network Testbeds.
Sivaramakrishnan Ramanathan, Jelena Mirkovic, Pravein G. Kannan, Chan Mun Choon and Keith Sklower.
Proceedings of the ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDNNFV), 2017.

Professional Activities

- Reviewer for IEEE Transactions on Networking (2016)
- Reviewer for IEEE Transactions on Network and Service Management (2018)
- Reviewer for IEEE Communications Letters (2020)
- Shadow PC member of Internet Measurement Conference (2018)

Teaching Experience

- CS570: Analysis of Algorithms — Teaching Assistant (Fall 2018)
- CS570: Analysis of Algorithms — Teaching Assistant (Spring 2019)

Awards

- Best presentation at ISI Graduate Student Symposium (2018).
- Student travel grant awardee for attending Operating Systems Design and Implementation (2018).

Research Experience

University of Southern California, Research Assistant — Los Angeles, 2016-Present

- Software Defined Security Service | SENSS
  SENSS [4] is a collaborative framework against volumetric DDoS attacks which allows victims to request help from ISPs in an automated and secure manner. SENSS provides simple and generic programmable interfaces that allow victims to build custom detection and mitigation approaches against a variety of attacks.
- Blacklist Aggregator | BLAG
  Blacklists contain addresses of known offenders, which can be used as a layer of defense. But blacklists are inaccurate, capture only a limited number of offenders and are reactive. BLAG [3] is a blacklist aggregation framework that uses a recommendation system to detect misclassifications in blacklists and predict malicious addresses based on historical blacklist data from 157 blacklists. BLAG also selectively identifies to expand some IP addresses into prefixes to proactively list malicious addresses.

AT&T Labs Research, Intern NYC, Summer 2017
Mentors: Dr. Yaron Kanza and Dr. Balachander Krishnamurthy

- SDProber
  Proactive delay measurements in networks aim to detect congested links. Ideally, congested links should be detected as early as possible, without interfering with the network traffic. SDProber is a new delay measurement tool that uses probe packets taking a random walk in the network. SDProber [5] finds a trade-off between detection time and bandwidth utilization of measurements by changing the probabilities that govern the random walk.

AT&T Labs Research, Intern NYC, Summer 2018
Mentors: Dr. Yaron Kanza and Dr. Balachander Krishnamurthy

- A Framework for ML-Based
  Machine learning can be powerful in predicting network events, which can help network operators to take proactive decisions. However, modern switches are limited in operations that would allow machine learning in them. We propose a framework, which performs real-time prediction of network events (such as microbursts or link utilization) in switches. Our framework uses offline learning to understand scenarios leading to a particular network event, translates the learned model to a DFA and finally compile it to a switch using P4.

International Computer Science Institute (ICSI), Intern UC Berkeley, Summer 2019
Mentor: Dr. Sadia Afroz

- Quantifying the impact of blacklisting
  Blocklists, consisting of known malicious IP addresses, can be used as a simple method to block malicious traffic. However, blocklists can potentially lead to unjust blocking of legitimate users due to IP address reuse, where more users could be blocked than intended. IP addresses can be reused either at the same time (Network Address Translation) or over time (dynamic addressing). In this work [5], we propose two new techniques to identify reused addresses. We built a crawler using the BitTorrent Distributed Hash Table to detect NATed addresses and use the RIPE Atlas measurement logs to detect dynamically allocated address spaces. We then analyze 151 publicly available IPv4 blocklists to show the implications of reused addresses and find that 53–60% of blocklists contain reused addresses having about 30.6K–45.1K listings of reused addresses. We also find that reused addresses can potentially affect as many as 78 legitimate users for as many as 44 days.