+1 404 786-1767
sahiti@jhu.edu
b-sahiti.github.io

Sahiti Bommareddy

Education

2019– now **Ph.D., Computer Science**, *Johns Hopkins University*, Baltimore, USA
Advisor: Professor Yair Amir (https://www.cs.jhu.edu/~yairamir/)

2017–2019 **M.S., Computer Science**, *Duke University*, Durham, NC

2007–2011 **B.Tech, Electronics and Communication Engineering**, *Jawaharlal Nehru Technological University*, Hyderabad, India

Research and Publications

My research areas is dependability, resiliency, and security of distributed systems and networks. My primary research focuses on designing and developing systems needed for building resilient critical infrastructure that should remain operational in face of faults, attacks, and intrusions.

Real-Time Byzantine Resilience: Many sectors of society depend on critical infrastructure such as the power grid, making them essential to the functioning of society. Supervisory Control and Data Acquisition (SCADA) systems provide automated control and remote monitoring of such infrastructure. In the world of increasing cyber threats, a compromise in SCADA component can put power grid resilience at risk by irreparably damaging grid infrastructure or by causing significant disruptions. Byzantine Resilient solutions for critical infrastructure is challenging due to several rigid factors including strict real-time requirements, continuous availability with long system life, solution cost and seamless integration into existing infrastructure. The strict requirements drive the need to develop new architectures, protocols and evaluations techniques that go beyond existing Byzantine fault tolerant solutions (based on state machine replication). The publications in this area are:

Real-Time Byzantine Resilience for Power Grid Substations, 41st International Symposium on Reliable Distributed Systems 2022. URL:https://www.dsn.jhu.edu/papers/RealTime.pdf

Real-Time Byzantine Resilient Power Grid Infrastructure: Evaluation and Trade-offs, Accepted, International Workshop on Explainability of Real-time Systems and their Analysis at the IEEE Real-Time Systems Symposium (RTSS 2022)

Severe Impact Resilience: The joint threats of increasingly frequent severe natural disasters and follow-on sophisticated malicious cyberattacks are becoming increasingly realistic and seriously threaten critical infrastructure systems. This novel threat model and the impact of such threats on critical infrastructure are not well understood. The research focuses on defining the threat model, developing a framework to assess the impact of novel compound threats on critical infrastructure with the aim to develop severe impact resilient systems. Hence, the research focuses on making resilient architectures more dynamic and flexible to withstand severe impact events. The research also investigates the impact of such threats on other critical infrastructure. Modernization and increasing inter-dependency among critical infrastructures reinforces the need for studying and designing severe impact resilient systems. The publication in this area is:

Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems, in 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Baltimore, MD, June 2022, pp. 72-79. URL:https://ieeexplore.ieee.org/abstract/document/9833853

Systems: Open Source Software Releases

Spire: Spire is an open-source intrusion-tolerant Supervisory Control And Data Acquisition (SCADA) system for the power grid. It is designed to withstand attacks and compromises at both the system level and the network level, while meeting the timeliness requirements of power grid monitoring and control systems (on the order of 100-200ms update latency).

In the latest release of Version 1.3 in December 2021, I optimized latency of the system in single site configuration to around 30ms i.e., 3x latency performance improvement and added a Machine Learning-based network intrusion detection system. Currently, I am working on applying the intrusion-tolerance principles to achieve Byzantine resilience in power grid substations that have exact real-time constraints on latency (4 milliseconds) among other rigid design constraints. This system is delivered for test bed deployment at Pacific Northwest National Labs (PNNL), Siemens, General Electric and Hitachi Energy.

Web page: https://www.dsn.jhu.edu/spire/

Spines: Many applications including critical infrastructure require high demanding combinations of latency, reliability, resilience, and processing even in presence of malicious actors at network level. To support such applications, new overlay dissemination protocols are developed and used to provide the necessary timeliness and reliability. Spines is a generic messaging infrastructure, that provides automatic reconfiguration and network flexibility required for research and production deployments.
Contributed to the latest version 5.5 of the Spines released in December 2020. It includes the cryptography and needed algorithm support for Byzantine resilient critical infrastructure SCADA systems.

Web page: http://www.spines.org

Teaching Experience

Spring 2022	Advanced Distributed Systems (JHU EN.601.717), *Special Help*
Fall 2021	Distributed Systems (JHU EN.601.417/617), *Special Help*
Spring 2021	Software for Resilient Communities (JHU EN.601.310), *Special Help*
Fall 2020	Intermediate Programming (JHU EN.601.220), *Special Help*
Fall 2019	Distributed Systems (JHU EN.601.417/617), *Teaching Assistant*
Spring 2019	Introduction to Artificial Intelligence (Duke CS270), *Teaching Assistant*

Industry Experience

Specialized in application load analysis, performance evaluation, network performance analysis, root cause analysis and performance optimization.

Jan 2013 – Dec 2015 **Aktrix Technologies Pvt Ltd**, *Co-Founder and Software Engineer*, Hyderabad,India

Led the performance engineering team on multiple client projects.

Ensured application performance Service-Level-Agreement(SLA) by identifying and resolving performance bottlenecks.

Initiated and led development of on an automated performance monitoring system to enable machine learning-based analysis tool, that reduced cost and time spent on RCA of performance degradation and bottleneck identification by 2x to 5x in each of the issue instances.

May 2011 – Nov 2012 **Deloitte**, *Performance Engineering Analyst*, Hyderabad,India

Reduced application transaction latency to bring it within the SLA window by identifying performance bottlenecks.

Received *Applause Award* in recognition of my application performance optimization efforts at Deloitte for both optimization and performing Root Cause Analysis (RCA) with traffic profiling, CPU, and memory utilization analysis in production environment.

Ensured guaranteed performance (backed by SLAs) in geo-distributed systems.

Technical Skills

Languages	Python, C, Java, SQL
Tools & Frameworks	Kubernetes, LoadRunner, HP Performance Center, Mininet, Spark, MongoDB
Systems	*NIX (CentOS, Ubuntu, Kali), Windows
Dev Tools	Vim, Git, VS Code, Eclipse, PyCharm

Additional Projects

Tweet Irony Detection: Implemented Irony Detection in tweets by modeling features from Context, Behavioural and Word embeddings. Explored a number of classifiers and improved F1-score by nearly 10% compared to Baseline.

Loosely Coupled Key-Value Store with Fault Tolerance: Built a sharded, replicated key-value store that utilizes the Raft consensus protocol. The objective of this project was to study the tradeoffs offered by the CAP theorem and implications of data distribution schemes. The prototype built was Consistent, but not Available, under a network partition.

Fair Decision Making using Privacy-Protected Data: This research investigates if fairness and privacy are fundamentally incompatible, and if there exists some differentially private mechanism which can preserve fairness, or if fairness can only be preserved in some cases. This project extends previous work by exploring new privacy mechanisms, and by designing a new fairness metric. Different privacy preserving mechanisms are explored to reduce error and increase fairness while preserving privacy.

Cracking a Home Router: Evaluated the security vulnerabilities of a home router – compromised the router using several known methods, such as password cracking, DoS attacks, Evil twin exploit, SYN flood and MITM attacks. This helped in understanding the security vulnerabilities to which a networked system can be exposed. The successful attacks were demonstrated and identified.

Performance Evaluation of Fat-Tree: The fat-tree topology is one of the most commonly used network topologies. This project builds a fat-tree on the Mininet network emulator, and compares its performance with a standard tree topology. The impact of application distribution, scheduling schemes and topology on performance SLAs and Bandwidth Utilization based on traffic profile varied from 0.5x - 3x.