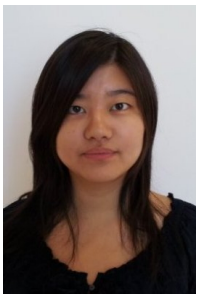
DREXEL UNIVERSITY
Cybersecurity Institute

Research project profile: **network anomaly detection**

Investigators	Tingshan Huang	Ph.D.		Akamai
	Ni An	Ph.D. student	Dept. of ECE	Drexel University
	Harish Sethu	Associate Professor	Dept. of ECE	Drexel University
	Naga Kandasamy	Associate Professor	Dept. of ECE	Drexel University
	Matthew C. Stamm	Assistant Professor	Dept. of ECE	Drexel University
	Steven Weber	Professor	Dept. of ECE	Drexel University


T. Huang


N. An


H. Sethu


N. Kandasamy


M. Stamm


S. Weber

Research summary: The goal of this research project is to better understand the fundamental issues in detecting anomalies in a network, and to apply that understanding to the design of improved network anomaly detection mechanisms, algorithms, and protocols.

The work of Tingshan Huang, Harish Sethu, Naga Kandasamy, and Matthew Stamm is on dimensionality reduction techniques for low-cost online performance monitoring and anomaly detection.

The work of Ni An and Steven Weber is on the performance overhead tradeoff of distributed principal component analysis via data partitioning. Data partitioning is desirable or even necessary when the network data used to infer the presence or absence of anomalies cannot be gathered into a single location. Performing network anomaly detection on partitioned data involves first compressing the information stored at each local site (e.g., using principal component analysis), and then sending the compressed signatures to a central data fusion center. The focus of this work is to analytically characterize the relationship between the controls (including the number of sites and the level of compression) and the resulting performance (including the quality of the reconstructed data and the amount of network bandwidth consumed).

Publications related to this research project include:

[1] Ni An and Steven Weber. On the performance overhead tradeoff of distributed principal component analysis via data partitioning. *submitted for inclusion in the proceedings of the 50th Conference on Information Sciences and Systems (CISS) (under review)*, Princeton, NJ, March 2016.

[2] T. Huang, H. Sethu, and N. Kandasamy. A fast algorithm for detecting anomalous changes in network traffic. *Proceedings of the 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[3] T. Huang, N. Kandasamy, and H. Sethu. Anomaly detection in computer systems using compressed measurements. *Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Gaithersburg, MD, November 2015.

This research is partially supported by the following grants:

[1] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Computing Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[2] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.