# "Transfer Learning for Malware Detection"

*Sachin Shetty, PhD*
*Associate Professor*
*Department of Modeling, Simulation and Visualization Engineering*
*Virginia Modeling, Analysis and Simulation Center*
*Center of Cyber Security Education and Research*
*Old Dominion University*

## ABSTRACT

Machine learning techniques have been employed in detecting occurrence of malicious attack and classification of malware families. Most machine techniques for malware detection are effective in building classifiers in the presence of labeled dataset. The availability of labeled dataset also hinges on the assumption that we can build predictive models of dynamic threats based on prior models of adversarial behavior. At the same time it is time consuming and impractical to generate labeled dataset.

In the Department of Defense funded Center of Excellence in Cybersecurity, we are developing techniques that builds on existing models of adversarial behavior to extend to environments characterized by diversity of systems, networks and users. In this talk, I will present the transfer learning technique to detect malware. Transfer learning utilizes labeled data in a source domain to help to train better models in the target domain with insufficient or no labels. To the best of our knowledge, this is the first effort to use a feature-based transfer learning technique to detect malware. The premise of the technique is to find a common latent feature subspace for the source and target domain by minimizing the difference between the data distributions while preserving the original discriminative data far apart. The technique can project the source and target data onto the new latent subspace. Furthermore, this technique can be used with any type of classifier on the transformed source data and does not need labeled target data. We evaluated the technique on publicly available datasets and results demonstrate the effectiveness of transfer learning to detect malware.

## SPEAKER BIO

Dr. Sachin Shetty received his PhD in Modeling and Simulation from the Old Dominion University in 2007. He is an Associate Professor in the Modeling, Simulation and Visualization Engineering at Old Dominion University. He also holds a joint appointment with the Virginia Modeling, Analysis and Simulation and Center and the newly founded Center for Cybersecurity Education and Research. Prior to joining Old Dominion University, he was an Associate Professor with the Electrical and Computer Engineering Department at Tennessee State University. He was also the associate director of the Tennessee Interdisciplinary Graduate Engineering Research Institute and directed the Cyber Security laboratory at Tennessee State University. He also holds a dual appointment as an Engineer at the Naval Surface Warfare Center, Crane Indiana. His research interests lie at the intersection of computer networking, network security and machine learning. His laboratory conducts cloud and mobile security research and has received over $10 million in funding from National Science Foundation, Air Office of Scientific Research, Air Force Research Lab, Office of Naval Research, Department of Homeland Security, and Boeing. He is a co-principal investigator on the Department of Homeland Security National Center of Excellence, the Critical Infrastructure Resilience Institute (CIRI), Department of Defense, Center of Excellence in Cybersecurity, and Department of Energy, Cyber Resilient Energy Delivery Consortium (CREDC). He has authored and coauthored over 80 research articles in journals and conference proceedings and two books. He is recipient of DHS Scientific Leadership Award and has been inducted in Tennessee State University's million dollar club. He has served on the technical program committee for ACM CCS, IEEE Infocom, IEEE ICDCN, and IEEE ICCCN. He is an Associate Editor for International Journal of Computer Networks.