Seminar

Using Deep Learning in Identifying Network Intrusions

Dr. Rajeev Agrawal, Information Technology Laboratory
US Army Engineer Research and Development Center

April 8, 2019
10:00 - 10:50 am
209 Computer Science Building



Deep Learning algorithms have been very successful in computer vision, natural language processing, and speech recognition. However, there is a big challenge in applying it in cyber security domain due to non-availability of 'real' cybersecurity data. Many researchers have tried using synthetic data such as KDD-NSL or newer UNSW-NB15 network intrusion datasets, however, it is difficult to determine the performance of the proposed research on a dataset captured from an experimental network. The DoD's High Performance Computing Modernization Program (HPCMP) operates Defense Research Engineering network (DREN), which has multiple security software and hardware tools installed across the network. A variety of cybersecurity logs are captured using these tools. We use a TensorFlow based framework to analyze DREN's Bro alert data generated under Cybersecurity Environment for Detection, Analysis and Reporting (CEDAR) project. These alerts are marked as bad or normal by the cybersecurity analysts and used as ground truths. This labeled data is used to measure the performance of our approach in identifying network intrusions. We are able to achieve high level accuracy by tuning hyper-parameters used in any deep learning approach. In this presentation, we will discuss the results of our approach which harnesses the power of HPC systems to train our proposed model.

Bio: Dr. Rajeev Agrawal joined Cyber Engineering and Analysis branch (CEAB), Information Technology Laboratory in 2016. He is the Data Science lead of the High Performance Computing Architecture (HPC) for Cyber Situational Awareness (HACSAW) Project. The goal of this project is to analyze the cybersecurity data captured across Defense Research and Engineering Network (DREN). He is also a member of the HPC-based deep learning project team and exploring deep learning applicability in cybersecurity domain.

Dr. Agrawal received his Ph.D. in Computer Science with minor in Engineering from Wayne State University in 2009. Prior to joining ITL, he was an Associate Professor in the Department of Computer Systems Technology at North Carolina A&T State University.

Dr. Agrawal's research interests include Deep Learning, Cyber Security, SCADA/ICS, Machine Learning and Pattern Recognition. He has published more than 80 technical papers and book chapters in refereed conferences and journals in these areas. He was selected a Data Science Fellow by the National Consortium of Data Science (NCDS) in 2014. His research has been funded by NSF, US Army, John Deere, ACM, RedHat, National Consortium of Data Science and Michigan State University.

CO-SPONSORED BY COMPUTER SCIENCE DEPARTMENT AND THE CENTER FOR SMART LIVING

MISSOURI S&T