Application of Belief Propagation for Detecting advanced persistent threats (APT’s)
Peter Chin, Boston University

We propose a new graph-theoretic framework based on belief propagation to detect the attacks and demonstrate that our detector has high accuracy while the incurred false positive and false negative rates are low using an anonymized dataset publicly released by Los Alamos National Lab (LANL) that includes two months of DNS logs collected at LANL with 20 simulated APT attacks overlaid onto it. We then apply our techniques to real-world web proxy logs collected at the border of a large enterprise network. We show the effectiveness of our techniques by identifying hundreds of suspicious domains contacted by enterprise hosts overlooked by state-of-the-art security products. Through careful manual investigation, we confirm that a large fraction of detected domains are used for malicious purposes.