Cross-Platforms Cybercrime Detection on Inter-connected Heterogeneous Networks

LEAD PI: LIANG ZHAO

Criminal Network Analysis

SUMMARY

Cybercrime can be particularly diffuse, incorporating multiple entities and platforms over time, which makes detection of complex cybercrime difficult. This project aims to develop methods and tools for processing and connecting digital evidence across multiple platforms so that dispersed cybercrimes can be reliably detected.

PROBLEM STATEMENT

A large amount of research effort has been devoted to cybercrime detection and prevention for different platforms and social networks as they are typically highly vulnerable to cross-platform cybercrimes. This is because many cybercrimes can be disguised as benign activities in each separate platform, but can only be detected as malicious by jointly modeling and exploring multi-networks. To address this open problem, this project will investigate and develop a framework for cross-platform cybercrime detection by using cross-references and links across different social networks.

APPROACH

There are three research thrusts of our proposed project: First, to comprehensively capture, identify, and connect users and their activities with potential cybercrime purposes, we will first develop methods that can construct and characterize the attributed heterogeneous information cross-networks. Second, we will detect cybercrime in the constructed network, by devising the techniques for cross-platform cybercrime detection via multi-network node embedding and classification. Third, we aim to establish the cross-platform cybercrime system by integrating and deploying the cross-network construction and cybercrime detection methods developed in the above objectives.

ANTICIPATED IMPACT FOR DHS

This project will significantly advance the overarching homeland security mission of securing cyberspace, specifically advancing towards the goal of combating cybercrime. More specifically, this project will advance CINA's mission and DHS operations towards: 1) developing transformative techniques for detection of sophisticated criminal activities in heterogeneous and multiple networks, 2) cross-platform cybercrime activity pathway identification and tracking, 3) focusing on crucial crime topics that involve multi- or cyber-physical-networks such as human trafficking in spatial network and darknets, social engineering in social media, and online activism networks. The software tool developed by this project will be generalizable and able to handle various sophisticated crime activities potentially of interest to different components of DHS including FEMA, TSA, CBP, Secret Service, and USCIS.