

BorderSafe: Cross-Jurisdictional Information Sharing, Analysis, and Visualization

Siddharth Kaza¹, Byron Marshall¹, Jennifer Xu¹, Alan G. Wang¹, Hemanth Gowda¹, Homa Atabakhsh¹, Tim Petersen², Chuck Violette², and Hsinchun Chen¹

¹ Department of Management Information Systems, University of Arizona, Tucson, Arizona
{skaza,byronm,jxu,ganghoma,hchen}@eller.arizona.edu
heman@email.arizona.edu

² Tucson Police Department, Tucson, Arizona
{tim.petersen,chuck.violette}@tucsonaz.gov

Project Background

The BorderSafe project funded by Department of Homeland Security (DHS) and the Corporation for National Research Initiatives (CNRI) aims to develop, foster, and leverage information sharing between law enforcement agencies for border safety and national security. The partners in the project include the Artificial Intelligence (AI) Lab at the University of Arizona, Tucson Police Department (TPD), Pima County Sheriff's Department (PCSD), Tucson Customs and Border Protection (CBP), San Diego Automated Regional Justice Information System (ARJIS), and the San Diego Supercomputer Center (SDSC). We describe the three major areas of research in the BorderSafe project at the AI Lab, University of Arizona.

Criminal Activity Network Analysis

A criminal activity network (CAN) is a network of interconnected people (often known criminals), vehicles, and locations based on law enforcement records. These networks aid in identifying suspicious individuals, vehicles, and locations based on data from multiple tiers of law enforcement agencies. Cross-jurisdictional information sharing and triangulation can help generate better investigative leads and strengthen legal cases against criminals. In the BorderSafe project, CANs are used to explore the criminal links of individuals and vehicles based on local police and border crossing records. The analysis has provided valuable results for law enforcement.

Critical Infrastructure Protection

Homeland security concerns include protecting critical infrastructures like power plants, water treatment plants, airports etc. Incidents that might pose threat to infrastructures are recorded in local law enforcement datasets. Analysis of these incidents can be used to set up alerts for individuals and vehicles involved in

2 Siddharth Kaza¹, Byron Marshall¹, Jennifer Xu¹, Alan G. Wang¹, Hemanth Gowda¹, Homa Atabakhsh¹, Tim Petersen², Chuck Violette², and Hsinchun Chen¹

suspicious activity around critical infrastructures. The locations of critical infrastructures and police incidents are geo-coded using the state plane coordinate system used by ESRITM. The AI Lab's Spatio-Temporal visualizer is used to analyze and plot the incidents around the critical infrastructure.

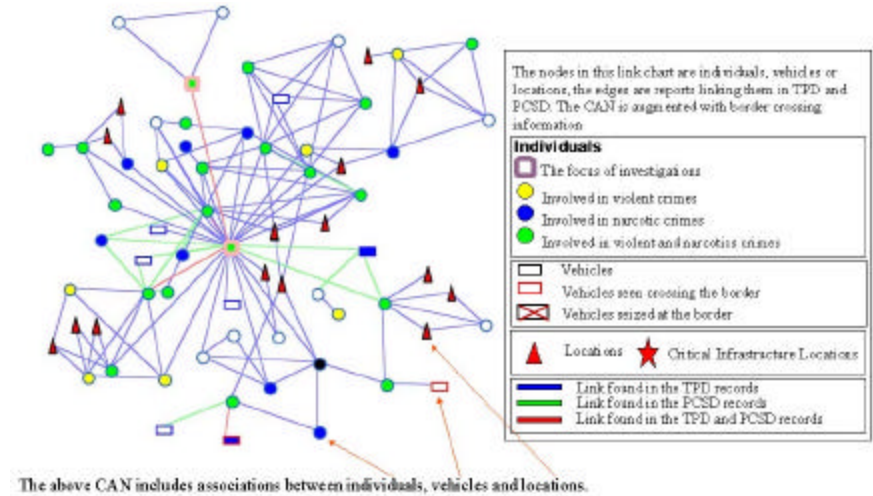


Fig. 1. An example Criminal Activity Network

Deception Detection

In law enforcement it is critical to penetrate identity concealment attempts as quickly and as effectively as possible. Our research goal is to create algorithms that automatically analyze law enforcement datasets to produce a ranked list of different individual identity entries that are likely to represent the same individual, and to tag each identity record with an estimate of the probability that it represents an active attempt at identity concealment. We have conducted a case study on real concealment cases identified by a police detective and developed a taxonomy of identity concealment. Probability-based detection algorithms, such as record linkage and Bayesian network, are currently being developed.