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

Hsinchun Chen, Homa Atabakhsh, Siddharth Kaza, Byron Marshall, Jennifer Xu, G. Alan Wang
Department of Management Information Systems
University of Arizona
Tucson, AZ
1-520-621-2165
{hchen, homa, skaza, byronm, jxu, gang}@eller.arizona.edu

Tim Petersen, Chuck Violette
Tucson Police Department
270 S. Stone Ave.
Tucson, AZ
1-520-791-4444
{tim.petersen,chuck.violette}@tucsonaz.gov

Categories and Subject Descriptors
H.4.2 [**Information Systems Applications**]: Types of Systems – *Decision support.*

General Terms
Algorithms, Design, Legal Aspects

Keywords
Criminal network analysis, critical infrastructure protection, deception detection

1. INTRODUCTION
Information sharing and knowledge management have become a major focus in Digital Government research. The "COPLINK BorderSafe Research and Testbed" project funded by NSF KDD program and the BorderSafe project funded by Department of Homeland Security (DHS) and the Corporation for National Research Initiatives (CNRI) aim to develop, foster, and leverage inter-agency information sharing. The partners involved in the projects include the Artificial Intelligence (AI) Lab at the University of Arizona, Tucson Police Department (TPD), Phoenix Police Department (PPD), Pima County Sheriff's Department (PCSD), Tucson Customs and Border Protection (CBP), San Diego Automated Regional Justice Information System (ARJIS), San Diego Supercomputer Center (SDSC), and Knowledge Computing Corporation (KCC).

The goal of the BorderSafe project is to facilitate information analysis and research for border safety and national security. We describe the three major areas of research in the BorderSafe and KDD projects at the AI Lab, University of Arizona.

2. 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. Figure 1 shows an example of a criminal activity network. 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 [2, 4].

3. 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 suspicious activity around critical infrastructures. The locations of critical infrastructures and police incidents are geo-coded using the state plane coordinate system used by ESRI™. The AI Lab's Spatio-Temporal visualizer [1] is used to analyze and plot the incidents around the critical infrastructure.

This research was supported in part by the NSF Digital Government (DG) program: "COPLINK Center: Information and Knowledge Management for Law Enforcement" #9983304, NSF Knowledge Discovery and Dissemination (KDD) program: "COPLINK Border Safe Research and Testbed" #9983304, NSF Information Technology Research (ITR) program: "COPLINK Center for Intelligence and Security Informatics Research - A Crime Data Mining Approach to Developing Border Safe Research" #0326348, and Department of Homeland Security (DHS) and Corporation for National Research Initiatives (CNRI) through the "BorderSafe" initiative #2030002.

DGO '05, May 15–18, 2005, Atlanta, GA, USA.

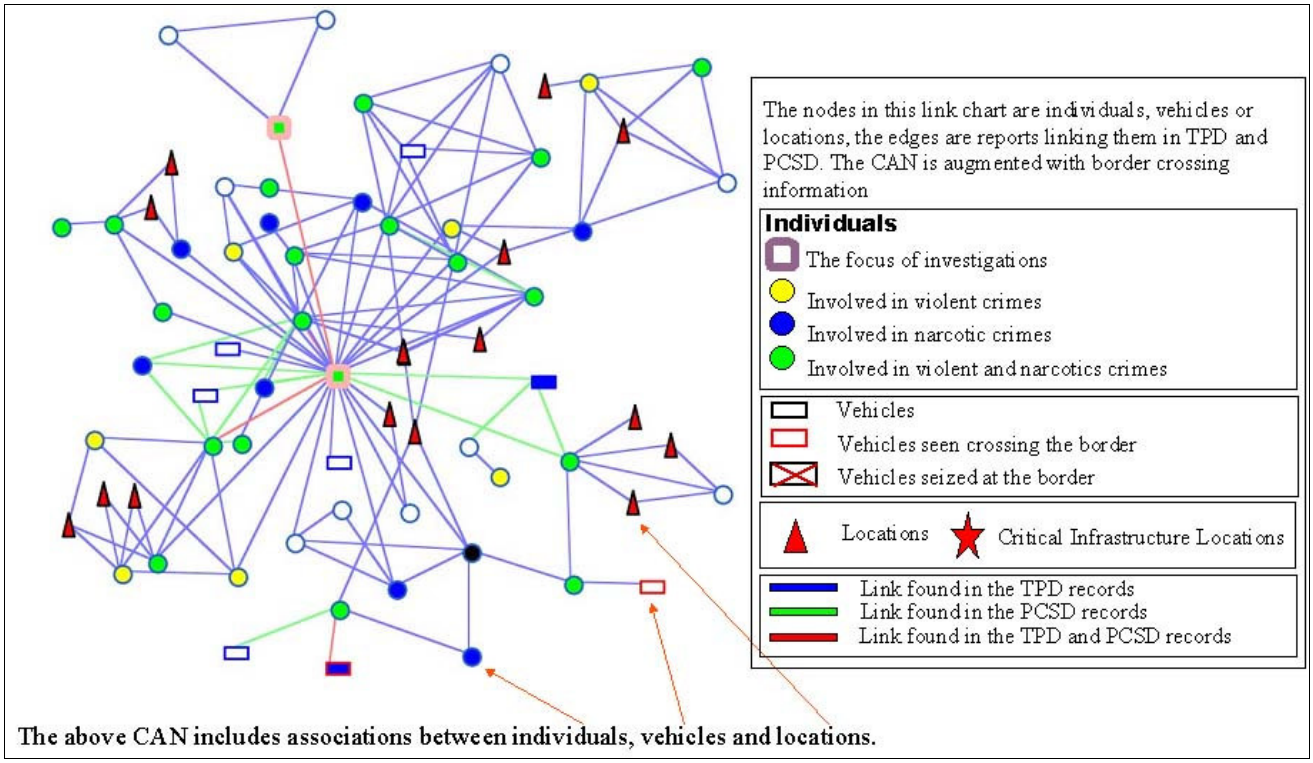

Figure 1. An Example Criminal Activity Network

4. 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 [3] of identity concealment. Probability-based detection algorithms, such as record linkage and Bayesian network, are currently being developed.

5. REFERENCES

[1] Chen, H., Atabakhsh, H., Tseng, C., Marshall, B., Kaza, S., Eggers, S., Gowda, H., Shah, A., Petersen, T. and Violette, C., Visualization in Law Enforcement. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, (Portland, OR, 2005).

[2] Marshall, B., Kaza, S., Xu, J., Atabakhsh, H., Petersen, T., Violette, C. and Chen, H., Cross-Jurisdictional Criminal Activity Networks to Support Border and Transportation Security. In *Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems*, (Washington D.C., 2004).

[3] Wang, G., Chen, H. and Atabakhsh, H. Automatically Detecting Deceptive Criminal Identities. *Communications of the ACM*, *47* (3). 71-76.

[4] Xu, J. and Chen, H. Fighting Organized Crime: Using Shortest-Path Algorithms to Identify Associations in Criminal Networks. *Decision Support Systems*, *38* (3). 473-487.