Coplink Center: Social Network Analysis and Identity Deception Detection for Law Enforcement and Homeland Security
Intelligence and Security Informatics: A Crime Data Mining Approach to Developing Border Safe Research

Hsinchun Chen[1], Homa Atabakhsh[2], Jennifer Jie Xu, Alan Gang Wang, Byron Marshall, Siddharth Kaza, Lu Chunju Tseng, Shauna Eggers, Hemanth Gowda, Tim Petersen*, Chuck Violette*

University of Arizona Dept of Management Information Systems Artificial Intelligence Lab, *Tucson Police Department

ABSTRACT
The goal of the COPLINK project is to develop information and knowledge management systems technologies and methodology appropriate for capturing, accessing, analyzing, visualizing, and sharing law enforcement related information. Continuing our pursuit of this goal, we have developed a framework for creating cross-jurisdictional Criminal Activity Networks for social network analysis, and have constructed a taxonomy of criminal identity resolution problems for detecting intentional identity deception and unintentional identity errors.

Categories and Subject Descriptors
I.2.1 [**Artificial Intelligence**]: Applications and Expert Systems – *law.*

General Terms
Design, Security, Human Factors

Keywords
Data Mining, Social Network Analysis, Identity Matching, Law Enforcement, Homeland Security

1. INTRODUCTION
The goal of the COPLINK project is to develop information and knowledge management systems technologies and methodology appropriate for capturing, accessing, analyzing, visualizing, and sharing law enforcement related information. COPLINK has bridged gaps between law enforcement agencies by allowing secure access by officers of some of the participating agencies. A prototype for COPLINK was initially developed at the University of Arizona's Artificial Intelligence Lab in collaboration with the Tucson Police Department (TPD) and Phoenix Police Department (PPD). COPLINK was developed into a commercial product by Knowledge Computing Corporation (KCC) and deployed in

approximately one hundred law enforcement agencies nationwide.

2. SOCIAL NETWORK ANALYSIS
2.1 Criminal Activity Networks
The security of borders is a critical component of the national strategy for homeland security. The Department of Homeland Security's (DHS) national strategy calls for the creation of "smart borders" where information from local, state, federal, and international sources can be combined to support risk-based management tools for border-management agencies. Security concerns at the border are not independent of law enforcement in border-area jurisdictions because information known by local law enforcement agencies may provide valuable leads useful for securing the border and transportation infrastructure. The combined analysis of law enforcement information and data generated by vehicle license plate readers at the international borders can be used to identify suspicious vehicles at ports of entry. We have developed a framework for effectively integrating such data to create cross-jurisdictional Criminal Activity Networks (CANs) (Figure 1) [Marshall et al. 2004].

2.2 Network Analysis
Criminal network knowledge has important implications for crime investigation and national security. To help law enforcement and intelligence agencies analyze criminal networks, we propose applying the concept space and social network analysis approaches to extract structural patterns automatically from large volumes of data. We have implemented these techniques in a prototype system, which is able to generate network representations from crime data, detect subgroups in a network, extract between-group interaction patterns, and identify central members. Multi-dimensional scaling has also been employed to visualize criminal networks and structural patterns found in them. We conducted a case study with crime investigators from TPD to validate the structural patterns of gang and narcotics criminal enterprises. The results were quite encouraging—the approaches we proposed could detect subgroups, central members, and between-group interaction patterns correctly most of the time. Moreover, our system could extract the overall structure for a network that might help in the development of effective disruptive strategies for criminal networks [Xu & Chen, 2003].
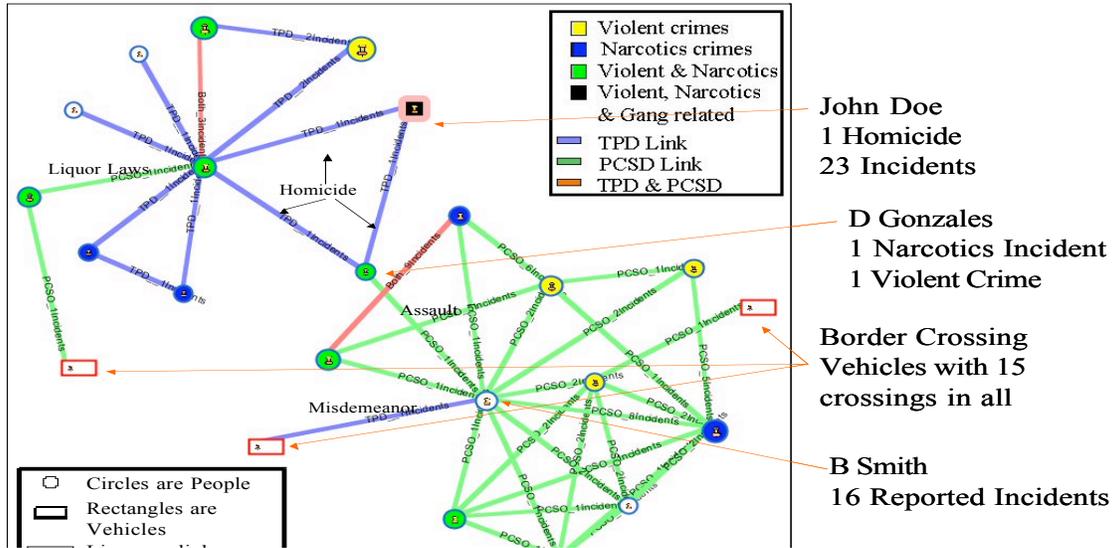
Figure 1. Visualization of a Criminal Activity Network

3. IDENTITY DECEPTION DETECTION

Identity resolution is central to fighting against crime and terrorist activities in various ways. Current information systems and technologies deployed in law enforcement agencies are neither adequate nor effective for identity resolution. We conducted a case study in a local police department (TPD) on problems that produce difficulties in retrieving identity information. Two types of problems, including intentional deception and unintentional errors, were found in real law enforcement records. In most of the cases, altered values looked very similar to the corresponding true values. We found that more than half (55.5%) of the suspects had either a deceptive or an erroneous counterpart existing in the police database system. About 30% of the suspects had used a false identity (i.e., intentional deception), while 42% had similar records due to various types of unintentional errors. Based on these findings, we built a taxonomy of identity problems [Wang et. al 2004].

4. FUTURE RESEARCH

As part of our future research, we plan to explore the characteristics of border crossing activity to better understand their temporal patterns. We will use the mutual information measure to identify vehicles that frequently cross with vehicles having criminal associations. We also plan to study temporal patterns of criminal networks. Over time criminal networks could change in size, organization, structures, member roles and many other characteristics. This would be helpful in predicting the trend and operation of a criminal enterprise. In addition, we plan to develop an automated identity resolution technique that takes our findings on identity problems into account. Techniques that improve identity information retrieval should locate identity information in an approximate rather than exact manner.

5. ACKNOWLEDGEMENTS

6. CONTACT INFORMATION

Artificial Intelligence Lab   http://ai.eller.arizona.edu/

Department of Management Information Systems

McClelland Hall 430
1130 East Helen Street
The University of Arizona
Tucson, Arizona 85721
1 (520) 621-2748

[1]hchen@eller.Arizona.edu, [2]homa@eller.Arizona.edu

7. REFERENCES

[1] Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., Schroeder, J. COPLINK managing law enforcement data and knowledge. *Communications of the ACM*, *46*, (2003), 28-34.

[2] Marshall, B., Kaza, S., Xu, J., Atabakhsh, H., Petersen, T., Violette, C., 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., Atabakhsh, H., Automatically detecting deceptive criminal identities. *Communications of the ACM, 47*, (2004), 70-76.

[4] Xu, J., Chen, H. Untangling criminal networks: A case study. In *Proceedings of the First NSF/NIJ Symposium on Intelligence and Security Informatics (ISI03)*, (2003), 232-248. Berlin: Springer