

Organized Crime Detection in Co-offending Networks

Mohammad A. Tayebi and Uwe Glässer
School of Computing Science
Simon Fraser University
British Columbia, Canada
Email: {tayebi, glaesser}@cs.sfu.ca

Patricia L. Brantingham
School of Criminology
Simon Fraser University
British Columbia, Canada
Email: pbrantin@sfu.ca

Abstract—This paper aims at a conceptual foundation for the development of advanced computational methods for analyzing co-offending networks to identify organized crime structures, that is, any static or dynamic characteristics of a co-offending network that potentially indicate organized crime or refer to criminal organizations. Specifically, we study networks derived from large real-world crime data sets using social network analysis and data mining techniques. Striving for a coherent and consistent framework for defining the problem scope and analysis methods, we propose here a constructive approach that uses mathematical models of crime data and criminal activity as underlying semantic foundation. Organized crime has been defined in a variety of ways, although, so far, there is surprisingly little agreement about its meaning—at least not at a level of detail and precision required for defining this meaning in abstract computational terms.

Keywords-Co-offending networks; Criminal networks; Social network analysis; Community Detection

I. INTRODUCTION

Law enforcement and intelligence agencies have long realized the potential of methodical approaches to analyse *co-offending networks* for addressing practical needs in crime investigation, crime reduction and crime prevention. Co-offending networks link criminal offenders who cooperate in committing crimes together. Co-offending can be expanded to include other types of co-activities associated with criminal activities. This could be observations of individuals of interest when seen together for example. Co-offending network analysis is also a rapidly evolving research theme in computational criminology [4], [2], [7], an emerging interdisciplinary research field promoting the use of computational methods and mathematical models in studies of social phenomena related to crime and other forms of illegal activities such as terrorism [5], [14], [8], [11].

This paper aims at a conceptual foundation for developing advanced computational methods to identify *organized crime structures* in co-offending networks, that is, any static or dynamic characteristics of a co-offending network that potentially indicate organized crime or refer to criminal organizations. Specifically, we study networks derived from large crime data sets using social network analysis and data mining techniques. To devise a coherent and consistent framework for defining the problem scope and analysis

methods, we propose here a constructive approach that uses mathematical models of crime data and criminal activity as underlying semantic foundation. Mathematical precision is essential not only for identifying and extracting network characteristics of interest but also for evaluating the efficacy of the underlying analysis methods and mining techniques by systematic analytical means.

Coming from a computing background, algorithmic methods and discrete mathematics seem perfectly rational choices for representing organized crime structures in terms of co-offending networks—but not so in the social sciences, and more specifically in criminology. This situation leads to an interesting interdisciplinary research problem: Computing as a discipline offers promising methods to tackle a notorious problem intensively studied in criminology but lacks sufficient domain knowledge; criminology, on the contrary, combines practical experience with established theories but lacks advanced computational methods. The work presented here attempts to bridge this gap between empirical and formal approaches by proposing a common conceptual foundation for co-offending networks and organized crime structures.

Starting from a conceptual model of crime phenomena as perceived by the domain experts and documented in the criminology literature, a mathematical representation is gradually derived that serves as precise semantic foundation for devising computational analysis methods. One may view this approach as an iterative modeling process based on three perspectives: Conceptual, Mathematical and Computational. This process is highly non-linear, with feedback loops within and across its phases, progressively establishing the validity and appropriateness of the resulting model (Figure 1).

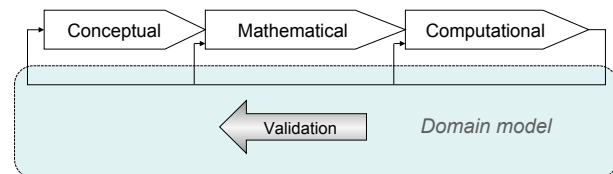


Figure 1. Modeling criminal activity: A highly iterative, non-linear process

Confronted with a bewildering diversity of characteristics referred to in existing definitions related to organized crime

and criminal organizations (see Section 2), the conceptual model itself appears not clearly rendered in the literature—at least not for the purpose considered here. Striving for a definition that is sufficiently general and open, another potential source in question is the criminal code, even though this depends on a specific country. In the Canadian context, for instance, a baseline definition of criminal organization is provided by the Criminal Code of Canada [27, p. 49]:

In Canada a criminal organization is a group, however organized that: (a) is composed of three or more persons in or outside Canada; and (b) has as one of its main purposes or main activities the facilitation or commission of one or more serious offences, that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any one of the persons who constitute the group. The definition further specifies that it excludes a group of three or more persons that has formed randomly for the immediate commission of a single offence. Section 467.1(1) of the Criminal Code of Canada.

The crime data set studied here originates from arrest-data for the Province of British Columbia and comprises several million data records, each of which refers to a reported crime incident. Based on a research memorandum of understanding between ICURS¹ and “E” Division of Royal Canadian Mounted Police (RCMP) and the Ministry of Public Safety and Solicitor General, five years of real-world data was made available for research purposes. This data was retrieved from the RCMP’s Police Information Retrieval System (PIRS), a large database system keeping information for the regions of the Province of British Columbia which are policed by the RCMP (for further details on the data, see also [8]).

Section II discusses related works. Section III explores common characteristics of organized crime and criminal organizations, and Section IV community detection methods in social networks. Next, Section V defines a unified crime data model and explains how the co-offending network model is derived. Section VI then proposes a crime group detection framework. Section VII concludes the paper.

II. RELATED WORKS

With academic and societal awareness of the importance of social networks increasing, law enforcement agencies and intelligence agencies have come to realize the value of detailed knowledge of criminal, or co-offending networks. A co-offending network is a network of offenders who have committed crimes together [17]. Groups and organizations operating within such networks to engage in conspiracies, terrorist activities and crimes like drug trafficking typically operate in a concealed fashion, trying to hide their illegal

activities and often also their associations. In analyzing such activities, investigation does not only focus on individual suspects but also attempts to uncover criminal groups.

Thus, it is important to identify criminal networks in data sources readily available to investigators, such as police arrest data and court data, and study these data using social network analysis methods. In turn, social network analysis can provide useful information about individuals as well. For instance, investigators may identify key players and subject them to closer inspection. Generally, knowledge about co-offending network structures provides a basis for law enforcement agencies to make strategic or tactical decisions. In this section, we review the related studies in co-offending network analysis in general, and then home in on research relevant to locating central actors in co-offending networks.

Several empirical studies that use social network analysis methods to analyze co-offending or terrorist networks have focused on the stability of associations in such networks. Morselli [1] offers a thoughtful general insight into ‘criminal organizational systems’ from a criminal network perspective and applies social network analysis to a number of case studies of criminal groups and organizations. Reiss [17] concludes that the majority of co-offending groups are unstable, and their relationships are short-lived. This is corroborated by McGloin et al. [19] who showed that there is some stability in co-offending relationships over time for frequent offenders but, in general, delinquents do not tend to reuse co-offenders. Reiss et al. [18] also found that co-offenders have many different partners, and are unlikely to commit crimes with the same individuals over time. However, Reiss [17] also states that high frequency offenders are “active recruiters to delinquent groups and can be important targets for law enforcement.” It should be noted that the findings of these works are based on very small datasets: 205 individuals in [18], and 5600 individuals in [19], and may therefore not be representative.

The above studies just analyzed co-offending networks. Smith [22] widened the scope of crime network analysis, enhancing the network by including extra information, particularly for the purpose of criminal intelligence analysis. For example, nodes of the network could be offenders, but also police officers, reports, or anything that can be represented as an entity. Links are associated with labels which denote the type of the relationship between the two entities, such as ‘mentions’ or ‘reported by’. A similar approach was taken by Kaza et al. [23] who explored the use of criminal activity networks to analyze information from law enforcement and other sources to provide value for transportation and border security. The authors defined the criminal activity as a network of interconnected criminals, vehicles, and locations based on law enforcement records, and concluded that including especially vehicular data in criminal activity networks is important, because vehicles can provide new investigative points.

¹The Institute for Canadian Urban Research Studies (ICURS) is a university research centre at Simon Fraser University.

A slightly different take on widening the scope of crime network analysis was taken by Xu et al. [21], who employed the idea of a 'concept space' in order to establish the strength of links between offenders. The frequency of co-offending, but also event and narrative data, were used to construct an undirected but weighted co-offending network. The goal was to identify central members and communities within the network, as well as interactions between communities. By applying cluster analysis in order to detect subgroups within the network they were able to detect overall network structures which could then be used by criminal investigators to further their investigations.

COPLINK [20] was one of the first large scale research projects in crime data mining, and an excellent work in criminal network analysis. It is remarkable in its practicality, being integrated with and used in the workflow of the Tucson Police Department. Xu et al. [14] built on this when they created CrimeNet Explorer, a framework for criminal network knowledge discovery incorporating hierarchical clustering, SNA methods, and multidimensional scaling. The authors further expanded the research in [21] and designed a full-fledged system capable of incorporating outside data, such as phone records and report narratives, in order to establish stronger ties between individual offenders. Their results were compared to the domain knowledge offered by the Tucson Police Department, whose jurisdiction the data came from.

III. WHAT IS ORGANIZED CRIME?

Based on prominent historical research on how organized crime developed in New York City, Block [25] concludes that organized crime was not only more fragmented and chaotic than believed, but also it involved *webs of influence* that linked criminals with those in positions of power in the political and economic world. Block argues that these patterns of affiliation and influence were far more important than any formal structure, since they allowed criminals to maximize opportunities, and should be considered a social system. The social system of organized crime [25]:

... refers to the notion that organized crime is a phenomenon recognizable by reciprocal services performed by professional criminals, politicians, and clients. Organized crime is thus understood to lie in the relationships binding members of the underworld to upperworld institutions and individuals. Organized crime is not a modern, urban, or lower-class phenomenon; it is a historical one whose changes mirror changes in civil society, the political economy. That is why, naturally, organized crime is increasingly taken to represent a series of relationships among professional criminals, upperworld clients and politicians ...

Looking for a quantitative definition used in an attempt to measure organized crime, Van Der Heijden proposes a number of common characteristics [26]:

- 1) *Collaboration of more than two people*
- 2) *Commission of serious criminal offences (suspected)*
- 3) *Determined by the pursuit of profit and/or power*
- 4) *Each having their own appointed tasks*
- 5) *For a prolonged or indefinite period of time*
- 6) *Using some form of discipline and control*
- 7) *Operating across borders*
- 8) *Using violence or other means suitable for intimidation*
- 9) *Using commercial or businesslike structures*
- 10) *Engaged in money laundering*
- 11) *Exerting influence on politics, the media, public administration, judicial authorities, or economy*

According to [26], for any criminal group to be categorized as organized crime it needs to have at least six of the above characteristics, where Items 1, 2, and 3 are obligatory, thus adding three more characteristics.

A major study of organized crime in Holland [28] mentioned great variations in collaborative forms and concluded that "the frameworks need not necessarily exhibit the hierarchic structure or meticulous division of labor often attributed to mafia syndicates. Intersections of social networks with a rudimentary division of labor have also been included as groups in the sub-report on the role of Dutch criminal groups, where they are referred to as cliques. As is demonstrated . . . there can be sizable differences in the cooperation patterns within these cliques and between the cliques and larger networks of people they work with on an incidental basis."

An impressive collection of definitions of organized crime, comprising more than individual 150 entries, has been gathered by von Lampe [3]. In addition to definitions ordered by countries and comments on the problem of how to define organized crime, this collection also includes definitions by prominent individuals and government agencies, for instance such as the Federal Bureau of Investigation (FBI). Not included though are definitions of the term "organized crime group". Given the abstract nature and informal language of these definitions, it is not clear at all how and to what extent one may utilize this resource for defining organized crime in precise computational and/or mathematical terms.

In most cases, existing definitions in the literature on organized crime concentrate on three essential perspectives for characterizing the nature of this form of crime: In the first view, organized crime is primarily about crime. Organized crime is seen as a *specific type* of criminal activity that has certain specific characteristics such as continuity in contrast to irregular criminal behavior. In the second view, organized crime is more related to the *concentration of power*, either in economic or in political structures of the society. And in the third view, the emphasis is on *organized*. That is, the important aspect of organized crime is on how offenders are connected to each other more than what they do.

In this paper, based on the third view, firstly we formalize the meaning of organized crime and criminal organiza-

tions in a coherent and consistent mathematical framework to provide a precise semantic foundation consistent with criminological research, social network analysis and law enforcement operations. This this formal definition aims at bridging the conceptual gap between data level, mining level and interpretation level. Based on this formal definition, we propose a method for detecting the organized crime using co-offending networks which can help law enforcement agencies in detecting and extracting meaningful information about organized crime.

IV. COMMUNITY DETECTION IN SOCIAL NETWORKS

This section addresses the concept of community in social networks and explores community detection methods. Since crime groups in co-offending networks can be categorized as communities in social networks, we need to have a good understanding of communities in social networks and existing methods for their detection before talking about crime groups. Community detection in social networks has attracted a lot of interest and many definitions of the concept of community have been proposed. In social science studies, social networks are considered as basis of social behaviors and activities. Studies of different social networks show that community structure influences information transfer, communication and cooperation. Sense of community is defined as a feeling that members of a group matter to one another and to the group, and a common belief that members' needs will be satisfied through their commitment to be together [30].

A. Community Detection in Static Networks

Usually, algorithms for community detection in static graphs are looking for a 'good' partition of the nodes. This implies that no node is member of more than one community and the main problem is "what does 'good' really mean?". For dealing with this problem some quality measures are defined that give a score to a partition: a good partition is the one which maximizes this quality measure. One of the most commonly used quality measures is modularity [32], and maximizing modularity in a greedy manner is one of the predominant methods for community detection. Modularity Q is defined as

$$Q = \sum_i (e_{ii} - a_i^2) \quad (1)$$

where e_{ij} is the fraction of edges that connect nodes in community i to nodes in community j , and $a_i = \sum_j e_{ij}$. But it has been shown that modularity maximization is an NP complete problem [31], and thus most of the solutions for this problem are based on approximation algorithms.

B. Community Evolution Tracking

In studies of how communities evolve over time, two main approaches have been used: 1) applying temporal information directly in the community detection process,

and 2) tracking communities over a number of snapshots in time. To take into account temporal information, recently, a new type of clustering, called *evolutionary clustering*, that captures the evolutionary process of clusters in time-stamped data was introduced. Chakrabarti et al. [33] address this issue in their paper by proposing a framework called "temporal smoothness". The output of this framework is a sequence of clustering, one for each timestep by considering two distinct aspects: first, it should have low *history quality*, which means it should be similar to the previous clustering in the sequence, and, second, it should have high *snapshot quality* which means it should have high accuracy in clustering of the current arrived data. The evolutionary clustering algorithm takes the similarity matrices M_1, M_2, \dots, M_t and produces the clusterings C_1, C_2, \dots, C_t . Evolutionary clustering uses a cost function to trade off the history quality and the snapshot quality. The cost function consists of two parts comprising snapshot cost and temporal cost:

$$\alpha \cdot SC(C_t, M_t) + (1 - \alpha) \cdot TC(C_{t-1}, C_t) \quad (2)$$

In the cost function snapshot cost measure SC , the quality of clustering C_t at time t , with respect to M_t and temporal cost TC , determines how similar the current clustering C_t is compared with the previous clustering C_{t-1} . For the snapshot and temporal cost, the relation is the smaller the value, the better the quality. The parameter α ($0 < \alpha < 1$) is used to adopt the level of preference to each of the two costs. The temporal smoothness framework attempts to find a clustering C_t that minimizes Eq. (2).

Several evolutionary graph clustering methods [34] have been proposed under the temporal smoothness framework, such as FacetNet [34], which extended the soft clustering algorithm [35] from static graphs to dynamic graphs. Soft clustering means that a node can be assigned to multiple communities at the same time with different participation levels. Having k communities at time t , it is assumed that the similarity m_{ij} is the effect of existence of all k communities. Then m_{ij} is approximated using a mixture model $m_{ij} \approx \sum_{r=1}^k p_r \cdot p_{r \rightarrow i} \cdot p_{r \rightarrow j}$, where p_r is the prior probability of the effect of the r -th community on the similarity m_{ij} , $p_{r \rightarrow i}$ and $p_{r \rightarrow j}$ are the probabilities that an interaction in community r involves nodes v_i and v_j , respectively. This concept can be expressed in matrix form as $W \approx X \Lambda X^T$ where $X \in R^{n \times r}$ is a matrix with $z_{ir} = p_{k \rightarrow i}$ and $\sum_i x_{ik} = 1$.

Another method for identifying relations between communities is constructing the networks for each time step. First, communities are identified within each of these networks, then relationships among communities on subsequent snapshots are recognized. Hence, such an algorithm operates in two steps: 1) static community detection on each snapshot, and 2) applying a matching function to recognize how these static communities evolve over a number of time steps.

V. CRIME DATA MODEL

This section proposes a unified formal model of crime data serving as the semantic framework for defining in a concise and unambiguous way properties of interest in the analysis of crime networks and their constituent entities. Specifically, this model aims at bridging the conceptual gap between data level, mining level and interpretation level, and facilitates separating the description of data from the details of data mining and analysis. By gradually transforming and reducing the unified model to more specific views, the co-offending network model is obtained as one such view.

A. Unified Crime Data Model

Crime data is modeled in the form of a finite graph structure as an attributed tripartite *hypergraph* $\mathcal{H}(\mathcal{N}, \mathcal{E})$ with a set of nodes \mathcal{N} and a set of hyperedges \mathcal{E} . The set \mathcal{N} is partitioned into three subsets, $A = \{a_1, a_2, \dots, a_q\}$, $I = \{i_1, i_2, \dots, i_r\}$ and $R = \{r_1, r_2, \dots, r_s\}$, representing *actors* such as offenders, victims, witnesses, suspects and bystanders; *incidents* referring to crime events of a certain type; and *resources* used in a crime², like mobile phones, tools, vehicles, weapons or bank accounts. A hyperedge e of \mathcal{E} is a non-empty subset of nodes $\{n_1, n_2, \dots, n_p\} \subseteq \mathcal{N}$ such that the following three conditions hold: $|e \cap I| = 1$, $|e \cap A| \geq 1$ and $|e \cap R| \geq 1$.

Each data record in the crime data set uniquely refers to a single crime incident. Thus, for any $e, e' \in \mathcal{E}$ with $e \cap I = e' \cap I$, it follows that $e = e'$. A hyperedge e of \mathcal{H} associates a set of one or more actors $\{a_{i_1}, a_{i_2}, \dots, a_{i_j}\} \subseteq A$ and a set of resources $\{r_{i_1}, r_{i_2}, \dots, r_{i_l}\} \subseteq R$ with a crime incident $i_k \in I$, that is $e = \{i_k, a_{i_1}, a_{i_2}, \dots, a_{i_j}, r_{i_1}, r_{i_2}, \dots, r_{i_l}\}$, as is illustrated in Figure 2.

Finally, with each node $n \in \mathcal{N}$ we associate some finite list of attributes $\langle (\alpha_{n,1}, \beta_{n,1}), (\alpha_{n,2}, \beta_{n,2}), \dots, (\alpha_{n,l}, \beta_{n,l}) \rangle$ where $\alpha_{n,i}$ is a unique identifier and $\beta_{n,i}$ is the value associated with $\alpha_{n,i}$. Attributes of actors, for instance, include the name and address information, while attributes of events include the crime type, the location where, and the time when, this incident occurred, among other data and information.

For analyzing and reasoning about co-offending networks and other specific aspects of crime data that can be described in terms of entities and their relations, the unified crime data model defined by the hypergraph \mathcal{H} is transformed in several steps into simpler graph structures as follows.

From the original graph structure \mathcal{H} , we derive a hypergraph $\mathcal{H}'(\mathcal{N}, \mathcal{E}')$, where \mathcal{N} is identical to the node set of \mathcal{H} and $\mathcal{E}' = \{\{a, i, r\} \mid \exists e \in \mathcal{E} : \{a, i, r\} \subseteq e, a \in A, i \in I, r \in R\}$. Note that \mathcal{H}' has the same attributes as \mathcal{H} . Now, \mathcal{H}' can further be decomposed in a straightforward way into

²Resources do often provide essential clues in criminal investigations. For simplicity, we assume here that R includes a distinguished element *nil* referring to situations in which no specific resource can be identified.

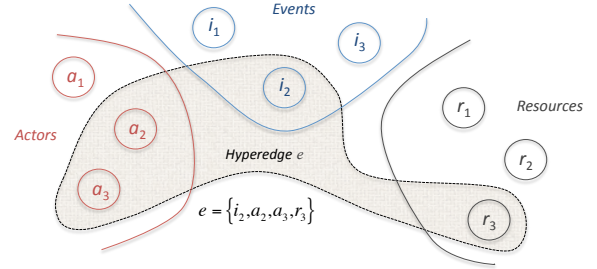


Figure 2. Hyperedge in the crime data model

three *bipartite* graphs that respectively model the relations between actors and incidents (graph AI), actors and resources (graph AR), and incidents and resources (graph IR).

B. Co-offending Network Model

A co-offending network consists of one or more connected components of offenders who have committed crimes together. Co-offending networks constitute a widespread form of social networks that is of considerable interest in crime investigations and in the study of crime. Specifically, this is relevant for law enforcement and criminal justice agencies to better understand organized crime and in evidence-based policy making aiming at crime reduction and prevention.

1) *Co-offending Network*: Starting from the graph AI , we define a co-offending network as a graph $G_O(V_O, E_O)$, where V_O represents the subset of offenders within the set of actors. Two nodes $a_m, a_n \in V_O$ are connected in G_O whenever there is a node $i_k \in I$ of type *crime incident* such that $\{a_m, i_k\}$ and $\{a_n, i_k\}$ are both edges in AI . To indicate multiple co-offenses committed by the same two offenders, a value *strength* is associated with every edge e of E_O , where $strength(e) \in \mathbb{N}$ with $strength(e) \geq 1$.

Assuming k offenders and m crime events ($k, m > 1$), we define a $k \times m$ matrix M such that $m_{uv} = 1$, if offender o_u is involved in event i_v , and “0” otherwise. This way, we can express the co-offending network as a $k \times k$ matrix $N = MM^T$ and therefore have

$$n_{u,v} = \sum_{x=1}^k n_{ux}n_{xv} \quad (3)$$

This matrix links offenders involved in the same crime events. For any two given offenders, the strength of a link is the number of co-offenses. The diagonal of this matrix shows for each offender the number of related crime events.

2) *Probabilistic Co-offending Network*: The crime data studied here is police arrest data containing only partial information of offender collaborations and their social interactions. As co-offenders often try to conceal their connections, one can expect that besides the links based on explicit facts in the crime data additional links can be derived by analyzing

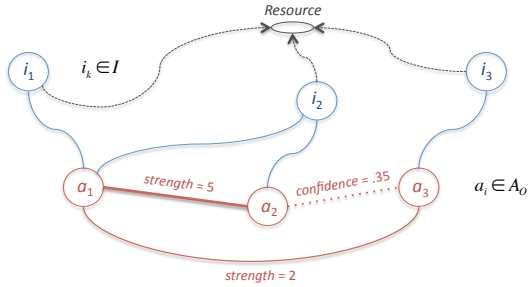


Figure 3. Criminal activity graph with hidden links

and mining the crime data using link prediction methods. Such links, called *hidden links*, are probabilistic in nature as they are based on information that is considered uncertain. Hidden links have an attribute *confidence*, a positive real number in the interval $[0, 1]$, rather than a strength. A confidence value of “0” means that no link exists.

Figure 3 illustrates an example for deriving a hidden link based on a criminal activity graph identifying three offender nodes a_1, a_2, a_3 for which it is known that a_1, a_2 and a_1, a_3 have jointly committed multiple crimes (some of which are not explicitly shown here).

Assume that in all three of the crime incidents i_1, i_2, i_3 a common resource, say a particular vehicle, was used by one of the offenders a_1, a_2, a_3 . From this information, one can derive a hidden link (a_2, a_3) with some probability as stated by the value of the attribute *confidence*.

Our work on co-offending networks ultimately focuses on probabilistic co-offending networks. In this paper, we restrict however on the analysis of explicit links.

VI. CRIME GROUP DETECTION FRAMEWORK

In this section, we propose a framework for detecting criminal groups in co-offending networks. First, we define different types of groups, and then present methods to detect these groups and track their evolution.

Offender Group An offender group is a team of offenders who collaborate in committing crimes. These groups are not necessarily formed as the result of a predefined plan and also they need not be active continuously. Offender group members have generally local clustering within larger loosely connected networks, thus constituting a small group with varying degrees of connection to other larger groups. $C_1^t, C_2^t, \dots, C_n^t$ refers to the n -offender group as part of the network at time t .

Organized Crime Group Offender group and organized crime group differ in scale, reach, type of criminal activity, and motivation. An organized crime group maintains an ongoing activity, involving a continuing criminal conspiracy of several persons motivated by the prospective of economic enrichment. The distinction between organized crime group

and offender group is not clear-cut but organized crime group differ from an offender group in at least three aspects: 1) Group scale and motivation, 2) Time interval of collaboration, and 3) Type of criminal activity.

Organized Crime Group Activity Let $O_1^t, O_2^t, \dots, O_n^t$ be n organized crime groups in the network at time t . We denote the activity of the organized crime group O_i^t with A_i^t . This measure states how active members of a group were inside the group compared to their activities with others.

Organized Crime Group Criminality Organized crime group criminality Q_i^t represents a measure for the degree of criminality of crimes committed by the organized crime group members O_i^t .

Organized Crime Group Evolution Trace An evolution trace $E(O_a^t)$ is a sequence of organized crime groups like $O_a^t, O_x^{t+1}, O_x^{t+2}, \dots, O_x^{t+n}$ that shows the trace of evolution of an organized crime group since its inception.

For organized crime group detection, in each time-slice of a co-offending network the following steps are executed: (1) Discover offender groups in the current network; (2) compute the activity and criminality of the detected offender groups in the time period between the current network and the last network; (3) Update the network partitioning for the new network. The following subsections discuss each of these steps in more detail.

A. Organized Crime Group Detection

Community detection in social networks can be defined as a graph minimum cut problem. A cut is a partition of vertices of a graph into two disjoint sets. In the minimum cut problem the goal is to partition the graph in a way that the number of edges between the resulting two node sets is minimized. For most social networks the concept of community is not defined formally. Therefore, having an algorithm that only attempts to find the optimized cut works, regardless of what would be the structure of the detected communities. For example, in the friendship network a good cut can put a person into the most relevant community based friendships that she has. Or, in the co-authorship network the community is mostly related to the authors’ collaboration in their research field. Therefore, just finding the best cuts and assigning authors to the closest cluster makes sense.

The nature of organized crime groups is different from the above types of communities. Organized crime groups are usually well established with group membership being defined explicitly and strictly. Also, relationships among offenders in a community are more systematic and organized to achieve specific goals, unlike in a friendship or co-authorship community. Therefore, detecting organized crime groups calls for a stricter definition of community. On the other hand, although organized crime groups attempt to be distributed enough to escape scrutiny by law enforcement agencies as much as possible, it appears that there is some kind of hierarchy among the members of a group. Another

aspect is that organized crime groups are not completely separated from each other but often have some form of interactions and sometimes even have common members. In this regard, we consider three main aspects of the proposed organized crime detection method: 1) Relationships inside an organized crime group are dense; 2) Members are not at the same level of membership with different types of members in an organized crime group; 3) Groups can overlap and can have common members.

In our opinion, an organized crime group is an offender group which has specific properties: it has sufficiently many members, its activity is continuous, and it is suspected of the commission of serious criminal offences. Therefore, for detecting organized crime groups, we first consider how to detect offenders groups.

In the first step of the proposed method, offender groups are built up from k -cliques. It is assumed that a group is made of adjacent k -cliques, sharing at least $k - 1$ nodes with each other. Since an offender group should have at least three members we assume $k = 3$. Each clique uniquely belongs to one community, but cliques within different communities may share nodes. Hence, we have overlapping groups with common members. For each offender group C_i , these members are assigned as their kernels $K(C_i)$. Kernels are the main members of an offender group and are completely involved in the group activities. In the second step, neighbor nodes connected directly to the kernels are added to the offender groups. These nodes are called *peripheries*. Peripheries of an offender group C_i are denoted by $P(C_i)$.

Activity and criminality of the offenders group are two key characteristics toward understanding the group structure. Below we present how these two measures are computed.

Let's assume i_1, i_2, \dots, i_n are the crime incidents in which members of offender group C_i were involved in timestep t . Activity of C_i in time t is computed as follows:

$$A_t(C_i) = \frac{|R_t(C_i)|}{|R_{t-1}(C_i)|} \quad (4)$$

where $|R_t(C_i)|$ and $|R_{t-1}(C_i)|$ are the number of relationships within offenders group C_i in timesteps t and $t - 1$, respectively. Criminality of C_i in timestep t is defined as:

$$Q_t(C_i) = \sum_{k=1}^{k=n} \frac{S(i_k)}{n} \quad (5)$$

where $0 < S(i_k) \leq 1$ indicates seriousness of the crime incident i_k .

For recognizing whether a detected co-offending group is an organized crime group, activity and criminality measures of the group should be considered. For this purpose we define two thresholds α -activity and β -criminality. A given co-offending group C_i is called α -active, if $A(C_i) > \alpha$, and it is called β -criminal, if $Q(C_i) > \beta$. We consider an

offender group an organized crime group, if it is α -active and β -criminal.

B. Organized Crime Group Evolution Model

Organized crime groups, similar to any other community, evolve over time. An organized crime group may grow by admitting new members, shrink by losing some members, split into two or more groups, or a new group may form by merging two or more existing groups. Therefore, we need to devise a model that allows formulating all these aspects of organized crime group evolution.

The model needs to determine which group at previous time has evolved into which group at current time. Five phenomena can occur for a group in a single snapshot: a community may survive, split, merge, appear or disappear [36]. For this purpose a matching function $match(O_i^t)$ is defined that, for a given group O_i^t , yields the group O_i^{t+1} that has the largest intersection with O_i^t , where this intersection is above a given threshold λ . If there exist no group at time $t + 1$, then $match(O_i^t) = \emptyset$. Intuitively, two groups at consecutive snapshots are matched if their nodes have some high intersection. We use this definition as match value of two organized crime groups

$$match(O, \acute{O}) = \min\left(\left(\frac{O \cap \acute{O}}{O}\right), \left(\frac{O \cap \acute{O}}{\acute{O}}\right)\right) \quad (6)$$

and apply these rules for tracking the evolution of organized crime group as follows:

- O_i^t survives in the next time slot as O_j^{t+1} , if $O_j^{t+1} = match(O_i^t)$ and for each $O_k^t \neq O_i^t$, $O_j^{t+1} \neq match(O_k^t)$.
- O_i^t splits into groups $O_1^{t+1}, O_2^{t+1}, \dots, O_n^{t+1}$, if there is enough overlap between each of these splitted groups and O_i^t , and also $(O_1^{t+1} \cup O_2^{t+1} \cup \dots \cup O_n^{t+1}) \cap O_i^t$, are both above the defined threshold.
- O_i^t merges with some other groups into O_j^{t+1} , if $O_j^{t+1} = match(O_i^t)$ and there exist $O_k^t \neq O_i^t$, $O_j^{t+1} = match(O_k^t)$.
- O_i^t ceases, if none of the above scenarios happened.
- O_j^{t+1} emerges, if $\forall O_i^t, O_j^{t+1} \neq match(O_i^t)$.

These rules are intuitive and easy to observe in the life cycle of groups, but they are not yet rigorous enough. The main problem lies in defining the threshold λ . This threshold should be determined based on either experiences and observations by domain experts or by learning from existing histories for real-world organized crime groups.

VII. CONCLUSIONS

One of the most challenging problems in crime reduction and prevention is investigation and control of organized crime groups and their illegal activities. Applications of co-offending network analysis methods to organized crime do arguably have potential to assist law enforcement agencies

and intelligence agencies, opening up new opportunities by providing novel instruments to derive relevant information from large crime data sets. But research solving the problems in this field by means of advanced computational methods is still in its infancy and does need more coordinated and intensified efforts to gain momentum. One reason for this situation may be the fact that access to real crime data sets for academic research purposes is often problematic and not widely available due to the sensitive nature of such data.

Organized crime has been defined in a variety of ways, although, so far, there is surprisingly little agreement about its meaning—at least not at a level of detail and precision required for defining this meaning in abstract computational terms. The main reason is that, unlike many other types of offenses, organized crime is a conceptual rather than a legal category. The issue of definition is important, because how we define organized directly effects how we attempt to explain, investigate, prevent and control it. We propose here a methodical framework for detecting criminal groups in co-offending networks as a conceptual foundation toward developing advanced computational methods for identifying organized crime structures in co-offending networks.

Our future work concentrates on refining the conceptual foundation in collaboration with leading criminology experts with the goal to amalgamate views across disciplines, in addition to performing more extensive experimental studies with real crime data sets to establish the practicability and identify limitations of the proposed framework.

REFERENCES

- [1] C. Morselli, Inside Criminal Networks. Studies of Organized Crime, Vol. 8, Springer, 2009.
- [2] M. A. Tayebi, L. Bakker, U. Glässer and V. Dabbaghian. Locating Central Actors in Co-offending Networks. Proc. 2011 International Conference on Advances in Social Network Analysis and Mining, Kaohsiung, Taiwan, July 2011.
- [3] Klaus von Lampe, Definitions of Organized Crime. Last visited, August 2011 [Online]. Available: <http://www.organized-crime.de/organizedcrimedefinitions.htm>.
- [4] M. A. Tayebi, M. Jamali, M. Ester, U. Glässer and R. Frank, CrimeWalker: A Recommendation Model for Suspect Investigation. In Proc. ACM RecSys, Chicago, IL, 2011.
- [5] M. B. Short, P. J. Brantingham, A. L. Bertozzi and G. E. Tita, Dissipation and Displacement of Hotspots in Reaction-Diffusion Models of Crime. PNAS. 107:3961-3965, 2010.
- [6] N. Memon, J. D. Farley, D. L. Hicks and T. Rosenorn (eds.), Mathematical Methods in Counterterrorism. Springer, 2009.
- [7] P. L. Brantingham, M. Ester, R. Frank, U. Glässer and M. A. Tayebi, Co-offending Network Mining. In U. Kock Wiil (ed.), Counterterrorism and Open Source Intelligence, Lecture Notes in Social Networks, Vol. 2: 211-239, Springer, 2011.
- [8] P. L. Brantingham, U. Glässer, P. Jackson and M. Vajihollahi, Modeling Criminal Activity in Urban Landscapes. In N. Memon *et al.* (eds.), *Mathematical Methods in Counterterrorism*, Springer, 2009.
- [9] L. Liu and J. Eck (eds.), *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*. IGI Global, 2008.
- [10] D. Kim Rossmo, *Geographic Profiling*. New York: CRC Press, 2000.
- [11] P. L. Brantingham, U. Glässer, P. Jackson, B. Kinney and M. Vajihollahi. Mastermind: Computational Modeling and Simulation of Spatiotemporal Aspects of Crime in Urban Environments. In L. Liu, J. Eck (eds.), *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, IGI Global, 2008.
- [12] D.M.A. Hussain, D. Ortiz-Arroyo. Locating Key Actors in Social Networks Using Bayes' Posterior Probability Framework. LNCS 5376, pp. 2738, 2008.
- [13] S.P. Borgatti, Identifying Sets of Key Players in a Social Network. *Computational and Mathematical Organization Theory*. 12(1):2134, 2006.
- [14] J.J. Xu and H. Chen, CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery. *ACM Transactions on Information Systems*, Vol 23 No 2. pp. 201-226, 2005.
- [15] R. Adderley and P. Musgrove, Modus operandi modelling of group offending: a data-mining case study. *International J. of Police Science and Management*. 5(4): 265-276, 2003.
- [16] A. Malm, G. Bichler, and S. Van de Walle, Comparing the ties that bind criminal networks: Is blood thicker than water?. *Security Journal* 23, 5274. 2010.
- [17] A. J. Reiss, Co-offending and criminal careers. *Crime and Justice: A Review of Research*, 1988.
- [18] A. J. Reiss, and D. P. Farrington, Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males. *Journal of Criminal Law and Criminology* 82 (2), 1991.
- [19] J. M. McGloin et al., Investigating the stability of co-offending and co-offenders among a sample of youthful offenders. *Criminology* 46 (1), 2008.
- [20] R. V. Hauck, H. Atabakhsh, P. Ongvasith, H. Gupta, H. Chen, Using Coplink to analyze criminal-justice data. *IEEE Computer*, Vol. 35, No. 3: 3037, 2002.
- [21] J.J. Xu, and H. Chen, Untangling Criminal Networks: A Case Study. *ISI 2003* pp. 232-248, 2003.
- [22] M. N. Smith, P. J. H. King, Incrementally Visualising Criminal Networks, iv, pp.76, Sixth International Conference on Information Visualisation (IV'02), 2002.
- [23] S. Kaza and H. Chen, Effect of inventor status on intra organizational innovation evolution. *Hawaii Intl. Conference on System Sciences (HICSS-42)*, Big Island, HI, 2009.

- [24] M. K. Sparrow, The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13: 251-274. 1991.
- [25] Alan A. Block, *East SideWest Side: Organizing Crime in New York City, 1930-1950*, 2nd ed., New Brunswick, NJ: Transaction 1994.
- [26] T. Van Der Heijden, Measuring Organized Crime in Western Europe. In Milan, Pagon (eds.) *Policing in Central and Eastern Europe: Comparing First Hand Knowledge with Experience from the West*, Slovenia: College of Police and Security Studies, 1996.
- [27] International Report on Crime Prevention and Community Safety: Trends and Perspectives, 2010. International Centre for the Prevention of Crime, Montreal, Quebec, Canada, 2010.
- [28] C. Fijnaut, F. Bovenkerk, G. Bruinsma and H. van de Bunt, *Organized Crime in the Netherlands*, The Hague: Kluwer Law International, 1998.
- [29] G. Palla, I. Derenyi, I. Farkas, and T. Vicsek, Uncovering the overlapping community structures of complex networks in nature and society, *Nature*, Vol. 435, No. 7043, 2005.
- [30] D. W. Mcmillan and D. M. Chavis. Sense of community: A definition and theory. *Journal of Community Psychology*, 14(1):623, 1986.
- [31] U. Brandes, D. Delling, M. Gaertler, R. Gorke, M. Hoefer, Z. Nikoloski, and D. Wagner. On modularity clustering. *IEEE Trans. on Knowl. and Data Eng.*, 20(2):172-188, 2008.
- [32] M. E. J. Newman. Fast algorithm for detecting community structure in networks, *Phys. Rev. E* 69, 066133, 2004.
- [33] D. Chakrabarti, R. Kumar, and A. Tomkins. Evolutionary clustering. In *Proc. of the 12th ACM SIGKDD Conf.*, 2006.
- [34] Lin, Y.-R., Y. Chi, S. Zhu, H. Sundaram, and B. L. Tseng, FacetNet: A Framework for Analyzing Communities and Their Evolutions in Dynamic Networks. *Proceeding of the 17th International Conference on World Wide Web*, 2008.
- [35] K. Yu, S. Yu, and V. Tresp. Soft clustering on graphs. In *NIPS*, 2005.
- [36] M. Spiliopoulou, I. Ntoutsi, Y. Theodoridis, R. Schult, Monic: modeling and monitoring cluster transitions, in: *Proc. 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, ACM New York, NY, USA, 2006.